

**UNIVERSIDADE PRESBITERIANA MACKENZIE**

ABYNER FERREIRA

DIREITO DIGITAL E LGPD: CAMINHOS PARA A HARMONIZAÇÃO ÉTICA NA ERA  
DA TECNOLOGIA

São Paulo

2024

ABYNER FERREIRA

Trabalho de Graduação  
Interdisciplinar apresentado como  
requisito para obtenção do título de  
Bacharel no Curso de Direito da  
Universidade Presbiteriana  
Mackenzie.

ORIENTADOR: PROF. DR. ARMANDO LUIZ ROVAI

São Paulo

2024

ABYNER FERREIRA

DIREITO DIGITAL E LGPD: CAMINHOS PARA A HARMONIZAÇÃO ÉTICA NA ERA  
DA TECNOLOGIA

Trabalho de Graduação  
Interdisciplinar apresentado como  
requisito para obtenção do título de  
Bacharel no Curso de Direito da  
Universidade Presbiteriana  
Mackenzie.

Aprovado em:

BANCA EXAMINADORA

---

Orientador: Armando Luiz Rovai

---

Examinador:

---

Examinador:

## **DIREITO DIGITAL E LGPD: CAMINHOS PARA A HARMONIZAÇÃO ÉTICA NA ERA DA TECNOLOGIA**

**Abyner Ferreira**

**Resumo:** Desde o início dos avanços tecnológicos - que têm constantemente revolucionado a comunicação, a interação e a forma de viver da pessoas -, a tecnologia digital inaugurou um ponto de não-retorno na era contemporânea a partir do qual a humanidade não saberia mais retroceder em suas conquistas de inovação. Neste cenário em que o mundo se mostra cada vez mais virtual e digitalizado e as relações entre as pessoas, por sua vez, cada vez mais cibernéticas, a comunidade legislativa e jurídica, não somente brasileira, mas de todo o mundo, se viu na responsabilidade de produzir um arcabouço regulatório que visasse conter os efeitos prejudiciais de inovações tão disruptivas que se inclinavam para ameaçar direitos e garantias fundamentais no que se refere à privacidade e à intimidade das pessoas e à proteção dos seus dados pessoais. É neste contexto que a presente pesquisa tem como objetivo analisar os caminhos para a harmonização legal na era da tecnologia com o intuito de identificar os meandros nos quais seja possível estabelecer um equilíbrio entre o direito digital regulamentado pela LGPD, a tecnologia da inovação e os direitos fundamentais das pessoas.

**Palavras chaves:** LGPD. Marco Civil da Internet. Tecnologia. Direito digital.

**Abstract:** Since the beginning of technological advances - which have constantly revolutionized communication, interaction and people's way of life - digital technology has inaugurated a point of no return in the contemporary era from which humanity would no longer know how to go back on its innovation achievements. In this scenario in which the world is increasingly virtual and digitized and the relationships between people, in turn, increasingly cybernetic, the legislative and legal community, not only in Brazil, but around the world, saw itself in the responsibility of producing a regulatory framework that aimed to contain the harmful effects of innovations so disruptive that they leaned to threaten fundamental rights and guarantees with regard to privacy and the privacy of individuals and the protection of their personal data. It is in this context that this research aims to analyze the paths to legal harmonization in the age of technology in order to identify the intricacies in which it is possible to establish a balance between the digital law regulated by the LGPD, the technology of innovation and the fundamental rights of people.

**Key words:** LGPD. Brazilian Civil Rights Framework for the Internet. Technology. Digital law.

**Sumário:** 1. Introdução. 2. A evolução do direito digital. 2.1. O Marco Civil da Internet. 3. LGPD: propósito e relevância. 4. Aspectos éticos e sociais da proteção de dados: privacidade, segurança e ética. 4.1. A ética no tratamento de dados pessoais. 4.2. A privacidade como objeto de proteção. 5. Conclusão. 6. Referências.

## 1 INTRODUÇÃO

Na contemporaneidade, a interseção entre o Direito e a tecnologia inaugurou um ponto de não-retorno na história da humanidade, já que, hoje, é impossível pensar o mundo sem os avanços tecnológicos conquistados na última era que revolucionaram a maneira de viver, de pensar e de se comunicar. Não sem razão, a era da tecnologia apresenta um cenário extremamente desafiador para a comunidade jurídica e também para a classe legislativa, que na condição de julgadores e legisladores das demandas sociais, civis, culturais e de toda sorte, precisavam dar respaldo à sociedade diante de tão desafiadores avanços. É nesse sentido em que a harmonização legal no âmbito do direito digital e da LGPD representa o cuidado em equilibrar segurança jurídica, privacidade e tecnologia em um cenário cada vez mais dominado por inovações tremendamente disruptivas.

Diante disso, o direito digital e as suas delimitações de objeto surgem como uma resposta bastante necessária à rápida evolução das tecnologias da informação e da comunicação no mundo moderno, que transformam paulatina e completamente a forma como as pessoas interagem, produzem, consomem e compartilham dados. Nesse contexto, questões legais relacionadas à privacidade, segurança cibernética, proteção de dados pessoais e responsabilidade civil ganham uma importância incontornável, de modo que são justamente sobre essas questões que o direito digital visa legislar no intuito de preservar os direitos do usuário da rede, que acima de tudo é um cidadão, sujeito de direito, e precisa ter suas garantias de privacidade respeitadas conforme preceitua a Constituição Federal.

Nessa toada, conforme se verá em oportuno na presente pesquisa, a LGPD foi inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia e é um marco muito significativo no ordenamento jurídico brasileiro dentro desse contexto de evolução tecnologia digital; a Lei em comento estabelece princípios, direitos e obrigações relacionadas ao

tratamento de dados pessoais por entidades públicas e privadas com o objetivo fundamental (e isso é muito importante) de proteger os direitos fundamentais de privacidade e autodeterminação informativa das pessoas, estabelecendo regras bastante claras para a coleta, uso, armazenamento e compartilhamento de informações pessoais.

Contudo, e conforme se verá adiante, a harmonização legal entre o direito digital e a presente era não é uma tarefa simples: a era da tecnologia impõe desafios únicos que colocam juristas e legisladores a pensar sobre os caminhos desses avanços e que trazem preocupações prementes, como a necessidade de adaptar as leis tradicionais a cenários digitais complexos, como inteligência artificial, *blockchain*, algoritmos, Internet das Coisas e *big data*, por exemplo. Acrescenta ainda à problemática uma dose de complexidade o dinamismo dessas tecnologias, que requerem uma abordagem legal inteligente, clarividente e adaptável, capaz de antecipar conflitos e prever respostas aos impactos éticos, sociais e jurídicos decorrentes de sua utilização.

Outrossim, a busca pela harmonização legal nesse contexto envolve vários aspectos. Primeiramente, exige a revisão e atualização constante das leis já positivadas para refletir os desafios trazidos pela tecnologia digital, bem como analisar as oportunidades ofertadas por ela para que sejam incorporadas da maneira mais adequada e benéfica possível na vida comum. Isso implica em um diálogo contínuo entre legisladores, comunidade jurídica, especialistas em tecnologia e sociedade civil para garantir que as regulamentações sobre o tema sejam eficazes e que as demandas das pessoas estão sendo contempladas por esse arcabouço regulatório, bem como garantir que sejam proporcionais e alinhadas com os valores fundamentais da democracia.

Além disso, a harmonização legal na era da tecnologia requer cooperação internacional nessa missão, dada a natureza transfronteiriça da internet, da economia digital e da virtualização global das informações e comunicações. A sintonia internacional no sentido de proteção de dados e preservação da privacidade é essencial para facilitar e proteger a interoperabilidade de dados entre diferentes países, estabelecendo padrões de proteção que garantam o fluxo seguro de informações pessoais. Isso sem olvidar da importância do desenvolvimento de capacidades institucionais e técnicas para garantir o cumprimento efetivo da legislação protetiva no âmbito da proteção de dados; isso inclui a capacitação de órgãos reguladores para fiscalizar o cumprimento genuíno das prescrições legislativas e a implementação de mecanismos de supervisão e aplicação eficazes para garantir a conformidade das organizações com as disposições legais, afinal, a lei precisa ser efetivada na conduta e na prática dos seus destinatários, sob pena de se tornar vazia e não obter êxito no seu intento protetivo.

Em suma, a harmonização legal no campo do Direito Digital e da LGPD é uma jornada multidimensional e contínua em direção a um ambiente jurídico mais coeso e adaptado à era da tecnologia; requer um equilíbrio cuidadoso entre a proteção dos direitos individuais, a promoção da inovação tecnológica e a garantia da segurança jurídica. Nesse sentido, a presente pesquisa tem como objetivo descrever os caminhos para a harmonização legal na era da tecnologia por meio do traçado de um panorama sobre a evolução do direito digital e de seu propósito, bem como pela análise dos aspectos éticos e sociais da proteção de dados a fim de demonstrar um equilíbrio entre tecnologia, inovação e proteção que permita a sociedade desfrutar dos benefícios da tecnologia digital de forma ética e responsável.

## 2 A EVOLUÇÃO DO DIREITO DIGITAL

A Internet consolidou-se como um elemento essencial no dia a dia das pessoas, por isso uma sociedade sem acesso a ela é praticamente inimaginável. É essencial reconhecer como a evolução tecnológica, independentemente da sua forma ou fase de desenvolvimento, sempre desempenhou um papel fundamental no progresso coletivo, moldando e remodelando a vida cotidiana humana através das suas conquistas. Neste contexto, a Internet, enquanto epicentro do rápido progresso no mundo digital de hoje, desempenha um papel semelhante ao das revoluções tecnológicas anteriores, influenciando profundamente a sociedade através da conectividade.<sup>1</sup>

A tecnologia está em constante evolução e o campo do direito deve acompanhar estas mudanças para garantir a proteção integral dos direitos fundamentais, sejam eles individuais, sociais, laborais ou quaisquer outros. Não se pode olvidar que ao longo dos anos, a tecnologia foi amplamente integrada na vida cotidiana, dando a todos acesso a uma ampla variedade de recursos através de dispositivos hoje imprescindíveis, como *smartphones*, computadores e *tablets*. Como resultado, o mundo inteiro está conectado.<sup>2</sup>

Nesse sentido, o direito digital opera sob a premissa de que qualquer relação que envolva fornecimento, compartilhamento ou outras operações de dados cria direitos, obrigações, deveres e responsabilidades por parte de quem os trata. Incontinenti, o direito digital utiliza diversos mecanismos, como analogia, costumes e princípios gerais de direito para regular essas relações e mediar os conflitos resultantes dessa manipulação de informações.

---

<sup>1</sup> FERNANDES, R. V. de C.; CARVALHO, A. G. P. **II Congresso Internacional de Direito, Governo e Tecnologia**. Fórum, 2018. Disponível em: <https://search.ebscohost.com/login>. Acesso em: 08 abr. 2024.

<sup>2</sup> Ibidem.

Nesse sentido, a evolução do Direito Digital representa uma jornada histórica que acompanha o desenvolvimento e a expansão da tecnologia da informação e comunicação ao longo das últimas décadas.<sup>3</sup> Esta disciplina surgiu da necessidade de adaptar o arcabouço jurídico tradicional aos desafios e oportunidades trazidos pela era digital, abrangendo questões complexas relacionadas à privacidade, segurança cibernética, propriedade intelectual, liberdade de expressão online e muito mais.<sup>4</sup>

Para compreender a evolução do Direito Digital, é essencial retroceder ao surgimento da internet comercial nas décadas de 1980 e 1990.<sup>5</sup> À medida que a internet se tornou acessível ao público em geral, surgiram novos dilemas legais e os primeiros debates centraram-se em questões como a responsabilidade dos provedores de serviços online por conteúdos gerados por terceiros e a aplicabilidade das leis nacionais a transações realizadas através da rede global.

Nos anos subsequentes, o Direito Digital progrediu rapidamente em resposta ao crescente uso da internet em atividades comerciais, governamentais e pessoais, fazendo com que a proteção de dados pessoais emergisse como uma preocupação central, levando ao desenvolvimento de leis e regulamentações específicas em várias partes do mundo para salvaguardar a privacidade dos indivíduos.

A evolução do Direito Digital também está intimamente ligada ao avanço das tecnologias, como a computação em nuvem, inteligência artificial, *blockchain* e Internet das Coisas, por exemplo. Cada uma dessas tecnologias apresenta desafios únicos em termos de governança legal, levando à necessidade de atualizações constantes nas legislações existentes e à criação de novos princípios legais para regular seu uso ético e seguro.<sup>6</sup>

Um marco significativo na evolução do Direito Digital foi a promulgação de leis de proteção de dados robustas em várias jurisdições. Por exemplo, o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, implementado em 2018, estabeleceu um padrão elevado para o tratamento de dados pessoais e influenciou leis semelhantes em outras partes do mundo, como a já mencionada Lei Geral de Proteção de Dados (LGPD) no Brasil, sendo a lei pátria completamente inspirada na sobredita legislação europeia.<sup>7</sup>

---

<sup>3</sup> SILVEIRA, Ana Cristina de Melo *et al.* **Proteção de dados pessoais na sociedade da informação:** entre dados e danos. 1. ed. Indaiatuba: Foco, 2020. *E-book*. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 07 abr. 2024.

<sup>4</sup> *Ibidem*.

<sup>5</sup> SARLET, Gabrielle Bezerra Sales; TRINDADE, Manoel Gustavo Neubarth; MELGARÉ, Plínio. **Proteção de dados:** temas controvertidos. 1. ed. Indaiatuba: Foco, 2021. *E-book*. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 07 abr. 2024.

<sup>6</sup> POESEL, Jussara de Oliveira Machado. **Cibersegurança, privacidade e proteção de dados pessoais no Brasil à luz do direito comparado e dos internacionais de regulamentação.** 1. ed. Caxias do Sul, RS: Educs, 2021. *E-book*. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 07 abr. 2024.

<sup>7</sup> *Ibidem*.



Outra área fundamental de desenvolvimento no Direito Digital é o reconhecimento e a regulamentação de novas formas de crimes cibernéticos, como fraudes eletrônicas, invasões de sistemas e ciberataques. Além disso, a evolução do direito digital está moldando as práticas jurídicas e a própria natureza do sistema judicial. A litigação eletrônica, por exemplo, transformou a maneira como os tribunais lidam com processos legais, introduzindo desafios e benefícios únicos, como a gestão eficiente de volumes massivos de dados digitais e a proteção da integridade das evidências digitais.<sup>8</sup>

Destarte, à medida que a humanidade se dirige para o futuro, a evolução do direito digital continuará sendo impulsionada pela inovação tecnológica. Bom também observar que questões emergentes, como a ética da inteligência artificial, a regulamentação da privacidade em ambientes virtuais imersivos (realidade virtual e aumentada) e a governança de algoritmos, estão moldando as discussões acadêmicas e práticas legais.

Em resumo, a evolução do Direito Digital reflete a crescente interdependência entre a tecnologia e o sistema jurídico. É um campo dinâmico e em constante mutação, exigindo adaptação e criatividade por parte dos juristas e legisladores para garantir que os direitos individuais sejam protegidos, os princípios éticos sejam preservados e a inovação tecnológica seja incentivada de maneira responsável e sustentável.

## 2.1 O MARCO CIVIL DA INTERNET

O Marco Civil da Internet foi instituído pela Lei 12.965, de 23 de junho de 2014,<sup>9</sup> que dispõe sobre as diretrizes para o uso da Internet em todo o território do Estado, que incluem garantias, direitos e obrigações em relação à evolução tecnológica. Nos seus artigos 1º e 3º estão indicados princípios e garantias. O artigo 1º da lei estabelece os princípios, garantias, direitos e obrigações para o uso da Internet no Brasil e também define as diretrizes para a atuação da União, dos Estados, do Circuito Federal e dos municípios nesse contexto. Os princípios do uso da Internet no Brasil, de acordo com o artigo 3º, incluem a garantia da liberdade de expressão, comunicação e manifestação de pensamento, a proteção da privacidade, a proteção dos dados pessoais, a preservação e garantia da neutralidade da rede, a preservação da estabilidade, a

---

<sup>8</sup> OLIVEIRA, Pedro de Moura Albuquerque de. **Reconfiguração conceitual da responsabilidade civil pelo direito digital?** Dissertação (Mestrado em Filosofia e Teoria Geral do Direito). São Paulo: Faculdade de Direito da Universidade de São Paulo, 2018.

<sup>9</sup> BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF. Diário Oficial da União. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/ato2011-2014/2014/lei/112965.htm](https://www.planalto.gov.br/ccivil_03/ato2011-2014/2014/lei/112965.htm). Acesso em: 10 abr. 2024.

segurança e a funcionalidade da rede, a responsabilidade dos agentes pelas suas ações, a preservação do carácter participativo da rede e a liberdade dos modelos de negócio promovidos na Internet, desde que não entrem em conflito com outros princípios estabelecidos.

Neste contexto, Daniel Donda<sup>10</sup> manifesta a sua preocupação com a possível restrição da liberdade de expressão ou violação da privacidade dos internautas. O quadro de direitos civis de Donda enfatiza que a garantia destes direitos constitucionais é essencial para o pleno exercício do direito de acesso à rede informática global. A violação destes direitos violaria, portanto, o objetivo da lei como ferramenta para proteger os utilizadores da Internet.

Outrossim, o Marco Civil da Internet foi promulgado para estabelecer restrições ao uso da Internet, garantir os direitos, obrigações e proteções quanto à privacidade e aos dados pessoais dos usuários. Aprovada através da Lei nº 35/2012, originalmente criada pelo Projeto de Lei nº 2.793/2011, com alterações do Projeto de Lei nº 84/99 (Lei Azevedo), a lei foi certificada e publicada pela Lei 12.737/12. Essa legislação, conhecida como “Lei Carolina Dieckmann”, foi a primeira a tratar dos crimes cibernéticos e recebeu esse nome devido ao caso de uma atriz que teve seu computador hackeado e fotos pessoais publicadas.<sup>11</sup> Infelizmente, no entanto, apesar da sua importância no combate aos crimes virtuais, a lei ainda é considerada insuficiente devido ao rápido desenvolvimento tecnológico.

### 3 LGPD: PROPÓSITOS E RELEVÂNCIA

A Lei Geral de Proteção de Dados, Lei nº 13.709, tem como propósito e objetivo principal, conforme explicado em seu artigo 1º, regular o tratamento de dados pessoais, que abrange tanto contextos digitais como não digitais, e que é realizado por pessoas físicas ou jurídicas, sejam elas dentro do setor público ou privado. Essa padronização visa proteger os direitos fundamentais de liberdade e privacidade consagrados na Constituição Federal.<sup>12</sup>

A legislação do artigo 2º estabelece as bases gerais adotadas como critérios para a proteção dos referidos direitos fundamentais. Estes fundamentos incluem o respeito pela privacidade, a autodeterminação afirmativa, a liberdade de expressão, informação,

---

<sup>10</sup> DONDA, Daniel. **Guia prático de implementação da LGPD**. 1. ed. São Paulo: Labrador, 2020. *E- book*. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 1º abr. 2024.

<sup>11</sup> SENADO FERREAL. **Dez anos de vigência da Lei Carolina Dieckmann: a primeira a punir crimes cibernéticos**. Rádio Senado, publicado em 29 mar. 2023. Disponível em: <https://www12.senado.leg.br/radio/1/noticia/2023/03/29/dez-anos-de-vigencia-da-lei-carolina-dieckmann-a-primeira-a-punir-crimes-ciberneticos>. Acesso em: 12 abr. 2024.

<sup>12</sup> BRASIL. **Lei nº 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF. Diário Oficial da União. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/ato2015-2018/2018/lei/113709.htm](https://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/113709.htm). Acesso em: 12 abr. 2024.

comunicação e opinião, a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento económico, tecnológico e a inovação, a livre iniciativa, a livre concorrência e a defesa dos direitos do consumidor, os direitos humanos, livre desenvolvimento da personalidade, dignidade e exercício da cidadania pelas pessoas físicas.

O artigo 6º da Lei Geral de Proteção de Dados (LGPD) representa um conjunto de princípios básicos que regem o tratamento de dados pessoais e promovem a proteção adequada e o respeito aos direitos das pessoas físicas. Críticos para o desenvolvimento de um ambiente regulatório consistente, estes princípios são fundamentais para garantir a integridade e a confidencialidade das informações pessoais.

O primeiro princípio estabelecido no artigo 6º é o princípio da finalidade, que afirma que o tratamento dos dados deve ser realizado para fins legítimos, específicos e explícitos, evitando qualquer utilização que não esteja de acordo com os objetivos originalmente estabelecidos. Este princípio visa garantir que os dados pessoais sejam utilizados de forma ética e de acordo com a lei.

O segundo princípio, da proporcionalidade, enfatiza a importância de o tratamento ser compatível com as finalidades previamente estabelecidas e evitar excessos ou desvios da finalidade. Isto significa garantir que apenas os dados necessários para atingir a finalidade proposta são recolhidos e tratados, garantindo que o impacto na privacidade dos indivíduos é minimizado.

O terceiro princípio, a necessidade, complementa o princípio da proporcionalidade, sublinhando que a recolha e o tratamento de dados devem ser limitados ao mínimo necessário para atingir os objetivos declarados. O objetivo desta limitação é evitar a recolha excessiva e desnecessária de dados pessoais e preservar a privacidade e a autonomia dos titulares dos dados.

O quarto princípio, acesso gratuito, sublinha a importância de garantir que os titulares dos dados possam consultar e verificar facilmente o tratamento dos seus dados pessoais. Esse acesso deve ser facilitado para que os indivíduos tenham conhecimento e controle sobre como suas informações são utilizadas.

O quinto princípio, qualidade dos dados, enfatiza a necessidade de garantir precisão, clareza, relevância e atualização dos dados pessoais. Esta política procura garantir que os dados tratados são fiáveis e refletem com exatidão a realidade dos titulares, evitando assim perdas resultantes de informação inexata ou desatualizada.

Os princípios de transparência, segurança, prevenção, não discriminação e responsabilidade complementam o disposto no artigo 6º da LGPD. Estas políticas proporcionam um quadro sólido para a proteção de dados pessoais e apoiam a criação de práticas transparentes,

seguras, preventivas, não discriminatórias e responsáveis no tratamento de tais informações. Juntos, esses princípios formam a base para a efetiva implementação da LGPD, garantindo a proteção da privacidade e a garantia dos direitos individuais no contexto de uma sociedade digital.<sup>13</sup>

A proteção dos direitos fundamentais está claramente definida no artigo 2º da Lei Geral de Proteção de Dados (LGPD), que está em harmonia com o disposto na Constituição Federal Brasileira, em especial com os artigos 5º, incisos X e XII, que tratam da privacidade, problemas relacionados com a honra, imagem das pessoas e sigilo na comunicação.

A LGPD desempenha papel central na preservação e segurança das informações pessoais no contexto digital. O seu objetivo é garantir que os dados pessoais dos indivíduos sejam tratados com a devida privacidade e segurança, em estrita conformidade com os princípios da transparência, consentimento e finalidade. Além disso, estabelece direitos claros para os titulares dos dados e dá-lhes controle sobre os seus dados pessoais.

No cenário atual, o direito à privacidade tornou-se uma questão cara, uma vez que a maioria das pessoas revela as suas vidas pessoais em diversas plataformas de redes sociais, permitindo que inúmeras outras pessoas acompanhem as suas atividades diárias. Além disso, as preocupações com a violação da confidencialidade das comunicações são uma realidade, uma vez que as plataformas de comunicação são frequentemente monitorizadas 24 horas por dia e todos os dados das conversas são armazenados nos servidores da empresa.<sup>14</sup>

As violações destas disposições legais não se limitam às empresas que recolhem, armazenam, processam ou utilizam dados pessoais, mas também incluem hackers que utilizam meios ilegais ou fraudulentos para obter informações que podem ser vendidas a preços inflacionados dependendo da importância dos dados. Mesmo no mundo físico, fora do ambiente online, os direitos à privacidade e à honra podem ser violados, uma vez que os dados pessoais podem ser recolhidos através de documentos escritos ou conversas, ameaçando a privacidade e a reputação das pessoas de quem são recolhidos.<sup>15</sup>

Ressalta-se que a LGPD também se aplica a dados resultantes de relações de consumo que sejam violadas por fornecedores, independentemente de serem pessoas físicas ou jurídicas.

---

<sup>13</sup> GARCIA, Lara Rocha; AGUILERA-FERNANDES, Edson; GONÇALVES, Rafael Augusto Moreno. **Lei geral de proteção de dados (LGPD):** guia de implantação. 1. ed. São Paulo: Blucher, 2020. E-book. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 12 abr. 2024.

<sup>14</sup> GODINHO, A. M. *et al.* **Tutela jurídica do corpo eletrônico:** novos desafios ao direito digital. 1. ed. Indaiatuba: Foco, 2022. E-book. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 12 abr. 2024.

<sup>15</sup> KOHLS, Cleize; WELTER, Sandro; DUTRA, Luiz Henrique. **LGPD:** da teoria a implementação nas empresas. 2. ed. São Paulo: Rideel, 2022. E-book. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 12 abr. 2024.

Garantir o cumprimento destas disposições legais é essencial para proteger os direitos fundamentais dos cidadãos no ambiente digital e físico. Além disso, a Lei enfatiza a importância do consentimento informado dos titulares dos dados antes da coleta e tratamento de seus dados pessoais, promovendo assim a transparência e a autodeterminação. Isto significa que as pessoas têm o direito de saber quais os dados que estão a ser recolhidos, para que finalidade serão utilizados e, em muitos casos, o direito de retirar o seu consentimento a qualquer momento.

Neste sentido, a LGPD é um diploma legal que visa pacificar a problemática que orbita o tratamento de dados pessoais, servindo como norma de padrão e consulta para a disciplina. É nesta lei em que se concentram os institutos próprios da matéria de proteção de dados, portanto, é importante conhecer as particularidades deste normativo para que se entenda quais são os parâmetros a que toda administradora de dados deve se ater.

Considerando os riscos das atividades de tratamento de dados pessoais à privacidade das pessoas, a lei tem um enfoque direcionado à proteção dessa privacidade ao preconizar os direitos desses titulares através de regras de *accountability* que forcem os controladores de dados a prestar contas sobre seu tratamento. Dentre algumas das áreas em que a proteção de dados se mostra pertinente, como na área de direito do consumidor, por exemplo, o direito à privacidade parece ser a mais relevante, daí a forte imbricação desses institutos e a ressonância entre eles, que inclusive sugere certa ambivalência quando da utilização destes dois termos, a privacidade e a proteção de dados.

Em suma, a LGPD desempenha um papel extremamente importante na proteção de dados pessoais no ambiente digital, garantindo a privacidade e a segurança das informações pessoais dos cidadãos, ao mesmo tempo que impõe obrigações claras às organizações que tratam desses dados. O seu objetivo é promover um ambiente digital mais seguro e transparente, onde os direitos de privacidade dos indivíduos sejam respeitados e protegidos. Estes princípios são de suma importância num mundo cada vez mais digital e conectado.

#### **4 ASPECTOS ÉTICOS E SOCIAIS DA PROTEÇÃO DE DADOS: PRIVACIDADE, SEGURANÇA E ÉTICA**

Pode-se aprender muito sobre um determinado período da história da humanidade apenas se analisando as agruras e preocupações típicas de cada época. Houve um tempo em que as preocupações típicas das pessoas era saber se a carta que elas haviam escrito de próprio punho e enviado por mensageiros à cavalo haviam chegado ao destino. Em outro momento, precisavam aprender Código Morse para enviarem mensagens por telégrafo utilizando-se de

corrente elétrica por meio de um emaranhado de fios.

Hoje não há qualquer preocupação ou necessidade de esforço desmedido para conversar com qualquer pessoa, por mais distante que ela esteja, nem mesmo se ela estiver em outro continente: a comunicação está, literalmente, na palma das mãos e a milésimos de segundos de distância. Em contrapartida, as preocupações continuam presentes, só mudaram um pouquinho de feição. Agora a humanidade se preocupa com a própria segurança cibernética e a privacidade dos seus dados pessoais, que assim como as suas mensagens, podem estar em qualquer lugar do mundo em questão de segundos.

Com efeito, é neste cenário marcado pelos avanços mais tecnológicos já experienciados pela humanidade que a importância da proteção de dados pessoais se agiganta, mostrando-se fundamental justamente devido à crescente digitalização da sociedade, da virtualização dos meios de comunicação e da expansão das tecnologias de coleta, processamento e compartilhamento de informações. Não obstante os inúmeros benefícios e avanços tecnológicos que esse contexto tenha proporcionado, ele também tem levantado preocupações muito relevantes em relação à privacidade e à segurança dos dados pessoais das pessoas usuárias da tecnologia da comunicação e informação.

Nesse diapasão, a proteção de dados pessoais é essencial por várias razões. Primeiramente porque incluem informações muito particulares sobre as pessoas, inclusive, por esse motivo, são chamados de dados sensíveis,<sup>16</sup> como nomes, endereços, números de telefone, históricos médicos, preferências de compra e até dados biométricos, para se ter uma ideia da extensão das informações particulares que se deixa em rede ao criar uma simples conta em sites na internet, de forma que o problema reside no fato de que esses dados, quando coletados e utilizados de maneira inadequada ou não autorizada, podem ser usados para violações de direitos relacionados à privacidade, intimidade e imagem, não raro podendo inclusive causar danos emocionais, financeiros e até físicos para o titular das informações.<sup>17</sup> Não à toa se discute hoje tão intensamente a importância da proteção de dados pessoais para garantir a confiança e a transparência nas interações digitais entre empresas, governos e pessoas.<sup>18</sup>

Ainda, a importância da proteção de dados está diretamente ligada à preservação dos direitos humanos. Primeiramente, a proteção de dados está diretamente relacionada à liberdade

---

<sup>16</sup> PINHEIRO, Patricia Peck. **Proteção de dados pessoais**: comentários à lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva, 2020. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9788553613625/>. Acesso em: 16 mar. 2024.

<sup>17</sup> Ibidem.

<sup>18</sup> LOPES, Juliana Joppert et al. Lei Geral de Proteção de Dados Pessoais (LGPD). **Swisscam Brasil**, 15 set. 2021. Disponível em: <https://swisscam.com.br/publicacao/doing-business-in-brazil/33-lei-geral-de-protecao-de-dados-pessoais-lgpd/>. Acesso em: 16 mar. 2024.

de expressão,<sup>19</sup> pois influencia na sensação de segurança das pessoas de se expressarem livremente sem medo de censura ou vigilância, independentemente da sua opinião, já que, em um mundo onde os dados pessoais são coletados em massa, existe o risco de que informações sensíveis sejam utilizadas para monitorar e controlar as atividades dos indivíduos, inibindo sua liberdade de expressão. Por exemplo, se as comunicações online são monitoradas e analisadas de maneira invasiva, isso pode gerar um ambiente de autocensura, onde as pessoas evitam expressar opiniões controversas ou desafiadoras por receio de represálias ou discriminação.<sup>20</sup>

Além disso, a proteção de dados é essencial para garantir o direito à privacidade, que por sua vez é um pilar fundamental dos direitos humanos, conforme se verá mais adiante. Trata-se de um direito corolário para a dignidade humana, para a autonomia e o desenvolvimento individual das pessoas, que precisam ter segurança de saber que a sua privacidade está resguardada e, assim, não se acanharem na expressividade das suas relações com o mundo, afinal, sem proteção adequada de dado, as pessoas perdem o controle sobre suas informações pessoais, ficando expostas a práticas invasivas de vigilância ou manipulação que colocam em risco a sua intimidade.<sup>21</sup>

Além disso, pode-se considerar também que a conexão entre proteção de dados e direitos humanos está relacionada ao princípio da igualdade e não discriminação. Isso porque a coleta e o uso indiscriminado de dados pessoais podem levar à discriminação algorítmica, onde algoritmos automatizados tomam decisões com base em dados sensíveis ao traçar um perfilamento dos usuários, resultando em tratamento diferenciado ou injusto para certos grupos sociais, violando, assim, os princípios de justiça e equidade.<sup>22</sup>

Nesse sentido, não se pode olvidar nem um instante que em um mundo digitalizado, onde os dados são a nova moeda de ouro, objeto de mercado, informações pessoais são frequentemente utilizadas com fins econômicos e de exploração capitalista e que por isso mesmo é essencial garantir que o processo de tratamento dessas informações seja transparente. Em suma, a importância da proteção de dados pessoais na atualidade é inegável, posto que ela não apenas protege a privacidade e os direitos individuais, mas também promove a confiança digital, a segurança cibernética e a transparência nas relações entre indivíduos e instituições que

---

<sup>19</sup> LIMA, Lindamaria. A Lei Geral de Proteção de Dados Pessoais e o Privacy by Design e Privacy by Default. **Tripla**, 23 jun. 2021. LGPD. Disponível em: <https://triplait.com/a-lei-geral-de-protecao-de-dados-pessoais-e-o-privacy-by-design-e-privacy-by-default/>. Acesso em: 25 mar. 2024.

<sup>20</sup> LOPES, Juliana Joppert et al. Lei Geral de Proteção de Dados Pessoais (LGPD). **Swisscam Brasil**, 15 set. 2021. Disponível em: <https://swisscam.com.br/publicacao/doing-business-in-brazil/33-lei-geral-de-protecao-de-dados-pessoais-lgpd/>. Acesso em: 25 mar. 2024.

<sup>21</sup> GET PRIVACY. Dados sensíveis na LGPD: riscos, bases legais e cuidados. **Get Privacy**, 2021. Disponível em: <https://getprivacy.com.br/dados-sensiveis-lgpd/>. Acesso em: 27 mar. 2024.

<sup>22</sup> Ibidem.

recolhem, armazenam e usam esses dados. Destarte, investir em práticas eficazes de proteção de dados é essencial para construir um ambiente digital seguro e ético, conforme se passa a analisar.

#### 4.1 A ÉTICA NO TRATAMENTO DE DADOS PESSOAIS

Diante do exposto anteriormente, ficou evidente que a questão da proteção dos dados pessoais é premente no contexto da comunicação moderna, em que o tempo todo as informações sensíveis das pessoas são coletadas e armazenadas para as mais diversas finalidades. Nesse sentido, a ética na coleta de dados pessoais é fundamental para estabelecer uma relação saudável entre as organizações que tratam esses dados e os indivíduos titulares dessas informações, pois sem padrões éticos sólidos, os riscos de abuso, exploração e violação da privacidade dos usuários aumentam significativamente.

No tocante a esse ponto, a ética no tratamento de dados pessoais se refere à conduta, ao comportamento das organizações em posse desses dados quanto ao que farão com eles e, sobretudo, como o farão. Compreende-se que da maneira como a comunicação e as relações estão organizadas hoje, haverá a retenção e a utilização de dados pessoais por parte das empresas que, de algum modo, interagem com as pessoas fornecendo-lhes algum tipo de produto, serviço ou informação. No entanto, o que se espera é o comportamento ético nesse procedimento, que se refere à lisura, à boa intenção e à dignidade no tratamento desses dados, de modo que o cumprimento de padrões éticos na coleta de dados pode inclusive promover a inovação responsável, o desenvolvimento sustentável e a proteção dos direitos individuais na era digital.

Nessa toada, mais do que a proteção dos dados pessoais, mas a importância da ética no tratamento desses dados é tema de grande relevância na era digital presente, onde a quantidade e a sensibilidade das informações coletadas sobre indivíduos têm aumentado exponencialmente. Não obstante, a ética nesse contexto não apenas diz respeito aos princípios morais envolvidos na coleta e no uso de dados, mas também aborda questões fundamentais relacionadas à privacidade, à autonomia individual e à confiança nas instituições que lidam com informações pessoais de milhares de pessoas, muitas delas sem noção de tudo o que é possível fazer com essas informações ou o quanto elas valem.

Isso porque, em um mundo cada vez mais interconectado como este, empresas, governos e tantas outras entidades têm acesso a uma quantidade exorbitante de dados sobre comportamentos, preferências e características das pessoas, dados estes que podem ser



utilizados com várias finalidades, algumas bem intencionadas, outras nem tanto, como personalizar experiências online ou influenciar a tomada de decisões do usuário com fins escusos.<sup>23</sup> Justamente por isso, a coleta e o uso ético dessas informações são essenciais por diversas razões.

Primeiramente, como já mencionado brevemente antes, a ética na coleta de dados pessoais está intrinsecamente ligada à proteção da privacidade e da autonomia, direitos humanos fundamentais que dão aos indivíduos a prerrogativa de decidir quem pode controlar e quem tem acesso às suas informações pessoais e como essas informações serão utilizadas. O drama é que sem uma abordagem ética, os dados pessoais podem ser explorados de maneira invasiva ou lesiva, resultando na violação desses direitos.

Além disso, a ética no tratamento de dados é essencial para promover a confiança e a transparência nas relações entre instituições e público, pois quando as organizações tratam os dados pessoais de forma ética e responsável, constrói-se um ambiente de confiança mútua,<sup>24</sup> onde os indivíduos se sentem mais seguros em compartilhar informações necessárias para a prestação de serviços mais assertivos e mais personalizados sabendo que não estão trazendo sobre si uma ameaça em potencial.

Diante dessas considerações, é fundamental estabelecer e aplicar princípios éticos sólidos na coleta e no uso de dados pessoais. Isso inclui garantir o consentimento informado e voluntário dos indivíduos, respeitar os princípios de propósito específico e minimização de dados, garantir a segurança e a proteção adequadas dos dados e promover a boa conduta em todas as etapas do processo de tratamento.

Para tanto, é fundamental considerar princípios éticos ao lidar com dados pessoais. Um dos mais importantes é o consentimento informado. Este princípio preceitua que os indivíduos devem ser plenamente informados sobre quais dados estão sendo coletados, como serão utilizados e quem terá acesso a eles. Uma vez em posse dessas informações, o consentimento deve ser dado de forma livre, específica e inequívoca pelo titular, frisando-se, inclusive, que este consentimento é revogável a qualquer momento.

Outro aspecto ético crucial é garantir que a coleta de informações pessoais seja realizada apenas para fins legítimos e específicos,<sup>25</sup> ou seja, os dados devem ser utilizados somente para os propósitos declarados e não devem ser compartilhados ou processados de maneira

---

<sup>23</sup> PINHEIRO, Patricia Peck. **Proteção de dados pessoais**. São Paulo: Saraiva, 2020.

<sup>24</sup> BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2020.

<sup>25</sup> Ibidem.

incompatível com os propósitos originais estabelecidos com os quais o titular havia concordado. Ainda, o princípio da minimização dos dados é um dos mais fundamentais: significa coletar apenas as informações pessoais necessárias para alcançar os objetivos específicos da coleta, evitando a coleta excessiva ou desnecessária de dados e descartando completamente aqueles que não serão utilizados. Além disso, tal princípio também preceitua a precisão dos dados coletados, de modo a coletar não apenas o mínimo de dados possível.

Desta feita, é inconteste que a ética na coleta de informações pessoais também envolve a responsabilidade de garantir a segurança e a proteção adequadas dos dados. É considerando essa responsabilidade civil, penal e administrativa que as organizações têm o dever ético de implementar medidas de segurança robustas aptas a proteger os dados pessoais contra acesso não autorizado, uso indevido, divulgação ou alteração que prejudique o seu titular, o que vai exigir, incontornavelmente, investimento em tecnologia de criptografia, controle de acesso e procedimentos de segurança cibernética eficazes.

Por fim, a ética na coleta de informações pessoais exige o cumprimento de padrões elevados de transparência, consentimento informado, minimização de dados e segurança em um mundo cada vez mais orientado por dados, promovendo uma cultura de respeito à privacidade e responsabilidade no tratamento das informações pessoais, o que demonstra que a ética no tratamento de dados pessoais é essencial para garantir que os avanços tecnológicos beneficiem a sociedade, e não a controlem, violem ou prejudiquem-nas em seus direitos individuais, respeitando a dignidade de todos, uma vez que, ainda que inseridos neste novo ecossistema digital, ainda são sujeitos de direitos.

## 4.2 A PRIVACIDADE COMO OBJETO DE PROTEÇÃO

A privacidade como objeto de proteção num mundo moderno regido pela ordem digital é um tema de grande relevância e também complexidade, especialmente diante dos avanços tecnológicos e das mudanças na maneira como as pessoas interagem e compartilham informações. Nesse cenário, a privacidade é um direito que se torna cada vez mais desafiador exercer e preservar em um contexto no qual dados pessoais são coletados, armazenados e utilizados em larga escala e para quase tudo.

Com efeito, a proteção da privacidade é essencial por várias razões. Em primeiro lugar, é fundamental para garantir a autonomia e a liberdade individual, que devolvem (ou deveriam devolver) ao titular dos dados o controle sobre suas informações pessoais para que ele decida com quem e como deseja compartilhá-las. A ausência de privacidade adequada, portanto, leva

as pessoas a sentirem-se coagidas ou monitoradas, afetando sua capacidade de se expressar livremente e de tomar decisões sem que tenham sido sorrateiramente influenciadas.<sup>26</sup>

A Inteligência Artificial é um dos instrumentos mais utilizados nesse processo: algoritmos de aprendizado de máquina são usados para analisar esses dados e extrair *insights*, estabelecer padrões e identificar comportamentos e preferências dos usuários, levantando pautas, inclusive, sobre o quanto dessas preferências e comportamentos são, de fato, legítimos, genuínos, já que através da Inteligência Artificial se pode influenciar os gostos, as percepções e os interesses das pessoas.

Segundo Vieira:

Importa salientar, de toda sorte, que a privacidade ainda que em franca reconfiguração no sistema jurídico e na vida cotidiana, pode ser dividida em diferentes categorias: (a) privacidade física – proteção contra procedimentos invasivos não autorizados como exames genéticos ou testes de drogas; (b) privacidade do domicílio –é aquela prevista no artigo 5º, inciso XI da Constituição Federal que dispõe: “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”; (c) privacidade das comunicações – também encontra respaldo constitucional (art. 5, XII); (d) privacidade decisional ou direito à autodeterminação – consiste no poder de decisão do indivíduo. E, por fim, (e) privacidade informacional ou autodeterminação informativa. (...) A esfera das informações pessoais toca diretamente no direito à autodeterminação informativa e, portanto, na privacidade informacional. No que diz respeito à ideia de soberania dos dados pessoais, não se deve olvidar que o âmbito da propriedade pessoal está vinculado às questões como propriedade (privada), posse, disposição do bem e outros aspectos dos direitos das coisas.<sup>27</sup>

No excerto, o autor explora diferentes categorias de privacidade e destaca a importância dessa diversidade na compreensão dos direitos individuais, especialmente no contexto jurídico e na vida cotidiana. Ele faz um adendo para a ideia de soberania dos dados pessoais, levantando questões importantes sobre a propriedade e o controle dos dados em um contexto digital.

Isso é importante porque, ao se falar na privacidade como objeto de proteção, é necessário compreender que o conceito de privacidade informacional está interligado com a capacidade de possuir, controlar e dispor de bens, incluindo informações pessoais. No contexto da privacidade, portanto, a soberania dos dados pessoais refere-se ao direito do indivíduo de ter controle sobre suas próprias informações e decidir como esses dados são utilizados por

<sup>26</sup> BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Grupo GEN, 2020.

<sup>27</sup> VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação, efetividade desse direito fundamental diante dos avanços da tecnologia da informação**. Porto Alegre: Fabris, 2007 p. 33.

terceiros.

Essa análise crítica ressalta a complexidade da privacidade em um mundo digital em constante evolução, onde os avanços tecnológicos levantam novos desafios para a proteção dos direitos individuais. Fato incontestável é que, no Brasil, previsto tanto na Constituição quanto na legislação infraconstitucional, mais especificamente na LGPD, o direito à privacidade é considerado um direito fundamental e um dos direitos da personalidade, e por isso mesmo é de inteira relevância que o sistema jurídico e as práticas cotidianas evoluam para garantir que a privacidade seja adequadamente protegida em todas essas dimensões, respeitando a autonomia e a dignidade dos indivíduos em relação aos seus dados pessoais, o que é o mesmo que dizer em respeito à sua privacidade; privacidade informacional.

## 5 CONCLUSÃO

Na era da informação digitalizada, a proteção de dados emergiu como um dos temas mais relevantes e complexos da atualidade. A coleta, processamento e uso de dados pessoais tornaram-se parte integrante da vida cotidiana, com implicações éticas e sociais significativas que precisam ser cuidadosamente consideradas e regulamentadas.

Nessa toada e à luz dos fatos expostos, ficou evidenciado que a ética na proteção de dados está diretamente relacionada à satisfação dos princípios fundamentais que orientam a maneira como os dados devem ser tratados em um ambiente digital. No cerne dessa questão está o respeito aos direitos individuais, à privacidade e à autonomia do titular em relação às suas informações pessoais.

É bem verdade que, na era da comunicação de um mundo digitalizado, os avanços tecnológicos permitem a coleta massiva e o processamento incansável de dados e que é forçoso compreender que isso passou a fazer parte do estado atual das coisas e de como a sociedade passou a ser organizada, contudo, essa realidade não pode se opor aos princípios constitucionais nem aos direitos fundamentais que ela preconiza, de forma que o tratamento de dados pessoais não deve, tampouco pode, ser feito sem o pleno consentimento ou conhecimento dos indivíduos afetados.

Além das considerações éticas, foi possível concluir também que o Direito Digital, sobretudo por meio da LGPD, causou um impacto profundo na estrutura social e nas relações de poder no que se refere ao tratamento de informações pessoais ao se colocar entre o titular dos dados – cidadão e sujeito de dinheiro – e o poderio informacional e tecnológico das organizações detentoras dos dados, estabelecendo limites ao tratamento e impondo regras

quanto a esse procedimento. Essa incitativa legislativa, não se pode olvidar, contribuiu muito para a segurança dos internautas e usuários das redes, embora haja muito ainda a ser aprimorado nesse cenário complexo.

Ainda, ficou evidente também que a privacidade é um componente essencial no exercício pleno da liberdade individual e da autodeterminação da pessoa, garantindo que elas possam agir, pensar e se expressar sem medo de vigilância ou manipulação indevida.

Com efeito, os desafios na proteção de dados são muitos. Com a rápida evolução da tecnologia, incluindo inteligência artificial e internet das coisas, é certo que ela apresentará constantes novos desafios à privacidade e à segurança dos dados. Não à toa, o futuro da tutela informacional dependerá de abordagens que incorporem considerações legais, tecnológicas e sociais para a plena harmonia ética na tecnologia. Isso inclui o desenvolvimento de marcos regulatórios robustos, investimentos em pesquisa ética e educação pública sobre direitos de privacidade. As organizações e governos também devem adotar uma abordagem proativa para enfrentar os desafios emergentes, como a ética da inteligência artificial e o uso responsável de dados biométricos.

Em resumo, os aspectos éticos e sociais da proteção de dados representam um dos dilemas centrais da sociedade digital contemporânea, de modo que, garantir a proteção da privacidade e promover a justiça social requer um compromisso coletivo com a ética e a responsabilidade dos operadores de dados pessoais. À medida que se navega pelos meandros desse novo território virtual, ainda não totalmente desbravado, deve-se permanecer vigilante na defesa dos direitos individuais e na construção de um ambiente digital que seja justo, inclusivo e respeitoso com a dignidade humana. Assim, a ética na coleta de dados pessoais é essencial para proteger a privacidade, a autonomia e os direitos individuais em um mundo cada vez mais digital, bem como a aplicação de princípios éticos sólidos que não apenas fortaleça a confiança entre instituições e titulares de dados, mas também promova uma sociedade mais justa, transparente e respeitosa no contexto da era da informação.

## 6 REFERÊNCIAS

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF. Diário Oficial da União. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/112965.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm). Acesso em: 10 abr. 2024.

BRASIL. **Lei nº 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF. Diário Oficial da União. Disponível em:

[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm). Acesso em: 12 abr. 2024.

BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2020.

BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Grupo GEN, 2020.

DONDA, Daniel. **Guia prático de implementação da LGPD**. 1. ed. São Paulo: Labrador, 2020. *E-book*. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 1ª abr. 2024.

FERNANDES, R. V. de C.; CARVALHO, A. G. P. **II Congresso Internacional de Direito, Governo e Tecnologia**. Fórum, 2018. Disponível em: <https://search.ebscohost.com/login>. Acesso em: 08 abr. 2024.

GARCIA, Lara Rocha; AGUILERA-FERNANDES, Edson; GONÇALVES, Rafael Augusto Moreno. **Lei geral de proteção de dados (LGPD): guia de implantação**. 1. ed. São Paulo: Blucher, 2020. *E-book*. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 12 abr. 2024.

GET PRIVACY. **Dados sensíveis na LGPD: riscos, bases legais e cuidados**. *Get Privacy*, 2021. Disponível em: <https://getprivacy.com.br/dados-sensiveis-lgpd/>. Acesso em: 27 mar. 2024.

GODINHO, A. M. *et al.* **Tutela jurídica do corpo eletrônico: novos desafios ao direito digital**. 1. ed. Indaiatuba: Foco, 2022. *E-book*. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 12 abr. 2024.

KOHL, Cleize; WELTER, Sandro; DUTRA, Luiz Henrique. **LGPD: da teoria a implementação nas empresas**. 2. ed. São Paulo: Rideel, 2022. *E-book*. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 12 abr. 2024.

LIMA, Lindamaria. **A Lei Geral de Proteção de Dados Pessoais e o Privacy by Design e Privacy by Default**. *Tripla*, 23 jun. 2021. LGPD. Disponível em: <https://triplait.com/a-lei-geral-de-protecao-de-dados-pessoais-e-o-privacy-by-design-e-privacy-by-default/>. Acesso em: 25 mar. 2024.

LOPES, Juliana Joppert et al. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. *Swisscam Brasil*, 15 set. 2021. Disponível em: <https://swisscam.com.br/publicacao/doing-business-in-brazil/33-lei-geral-de-protecao-de-dados-pessoais-lgpd/>. Acesso em: 16 mar. 2024.

MELGARÉ, Plínio. **Proteção de dados: temas controvertidos**. 1. ed. Indaiatuba: Foco, 2021. *E-book*. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 07 abr. 2024.

OLIVEIRA, Pedro de Moura Albuquerque de. **Reconfiguração conceitual da responsabilidade civil pelo direito digital?** Dissertação (Mestrado em Filosofia e Teoria Geral do Direito). São Paulo: Faculdade de Direito da Universidade de São Paulo, 2018.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais**. São Paulo: Saraiva, 2020.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à lei n. 13.709/2018 (LGPD)**. 2. ed. São Paulo: Saraiva, 2020. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9788553613625/>. Acesso em: 16 mar. 2024.

POLESEL, Jussara de Oliveira Machado. **Cibersegurança, privacidade e proteção de dados pessoais no Brasil à luz do direito comparado e dos internacionais de regulamentação**. 1. ed. Caxias do Sul, RS: Educs, 2021. *E-book*. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 07 abr. 2024.

SARLET, Gabrielle Bezerra Sales; TRINDADE, Manoel Gustavo Neubarth;

SENADO FEREAL. **Dez anos de vigência da Lei Carolina Dieckmann: a primeira a punir crimes cibernéticos**. Rádio Senado, publicado em 29 mar. 2023. Disponível em: <https://www12.senado.leg.br/radio/1/noticia/2023/03/29/dez-anos-de-vigencia-da-lei-carolina-dieckmann-a-primeira-a-punir-crimes-ciberneticos>. Acesso em: 12 abr. 2024.

SILVEIRA, Ana Cristina de Melo *et al.* **Proteção de dados pessoais na sociedade da informação: entre dados e danos**. 1. ed. Indaiatuba: Foco, 2020. *E-book*. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 07 abr. 2024.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação, efetividade desse direito fundamental diante dos avanços da tecnologia da informação**. Porto Alegre: Fabris, 2007.



---

## TERMO DE AUTENTICIDADE DO TRABALHO DE CONCLUSÃO DE CURSO

Eu, Abyner Ferreira

discente regularmente matriculado(a) na disciplina TCC II, da 10ª etapa do curso de Direito, matrícula nº 31848028 período matutino, turma 9D, tendo realizado o TCC com o título: Direito Digital e LGPD: Caminhos para a Harmonização Ética na Era da Tecnologia sob a orientação do(a) Professor(a) Armando Luiz Rovai

declaro para os devidos fins que tenho pleno conhecimento das regras metodológicas para confecção do Trabalho de Conclusão de Curso (TCC), informando que o realizei sem plágio de obras literárias ou a utilização de qualquer meio irregular.

Declaro ainda que, estou ciente que caso sejam detectadas irregularidades referentes às citações das fontes e/ou desrespeito às normas técnicas próprias relativas aos direitos autorais de obras utilizadas na confecção do trabalho, serão aplicáveis as sanções legais de natureza civil, penal e administrativa, além da reprovação automática, impedindo a conclusão do curso.

São Paulo, 10 de Maio de 2024.

---

Assinatura do discente