# Privacidade digital: análise da lei geral de proteção de dados

Vinícius Pires de Matos, Direito, Centro Universitário Integrado, Brasil, vinicius.pmatos10@gmail.com

Andreia Aparecida de Souza, Professora Orientadora, Curso de direito, Centro universitário Integrado, Brasil, andreia.souza@grupointegrado.br.

## RESUMO

Este trabalho tem como objetivo analisar a proteção de dados pessoais no ambiente digital, com ênfase na aplicação da Lei Geral de Proteção de Dados (LGPD) e os desafios do direito para acompanhar o avanço tecnológico, para tanto, a pesquisa foi desenvolvida utilizando o método dedutivo, abordando conceitos fundamentais do direito digital e da privacidade online demonstrando que, com o crescimento da coleta de dados pelas plataformas digitais, a privacidade dos usuários está constantemente em risco. Diante disso, o estudo pretende analisar a situação abordando conceito e evolução do direito digital, ressaltando as principais legislações sobre o tema, além de abordar a importância dos dados pessoais em virtude da privacidade e do interesse privado neles, desse modo, será analisada a LGPD que se revelou um importante marco legal ao estabelecer regras claras para o tratamento de dados pessoais, trazendo maior segurança jurídica e proteção aos indivíduos, porém, foram identificados desafios práticos para a implementação eficaz da lei, como a adequação das empresas e a conscientização dos usuários. Desse modo, conclui-se, pela importância da legislação para garantir a proteção de dados, entretanto, ressalta-se, a necessidade de ajustes contínuos para acompanhar as inovações tecnológicas e futuras regulamentações.

**Palavras chave:** Proteção de Dados. Privacidade Digital. Lei Geral de Proteção de Dados. Direito Digital.

## ABSTRACT

This work aims to analyze the protection of personal data in the digital environment, with an emphasis on the application of the General Data Protection Law (LGPD) and the challenges of law to keep up with technological advances, to this end, the research was developed using the method deductive, addressing fundamental concepts of digital law and online privacy, demonstrating that, with the growth of data collection by digital platforms, users' privacy is constantly at risk. In view of this, the study intends to analyze the situation by addressing the concept and evolution of digital law, highlighting the main legislation on the subject, in addition to addressing the importance of personal data due to privacy and private interest in them, thus, the LGPD will be analyzed which proved to be an important legal framework by establishing clear rules for the processing of personal data, bringing greater legal certainty and protection to individuals, however, practical challenges were identified for the effective implementation of the law, such as the adequacy of companies and the awareness of users . Therefore, it is concluded that the importance of legislation to ensure data protection is important, however, the need for continuous adjustments to keep up with technological innovations and future regulations is highlighted.

**Keywords:** Data Protection. Digital Privacy. General Data Protection Law. Digital Law.

## INTRODUÇÃO

Com o avanço exponencial da tecnologia e a transformação digital das últimas décadas, o ambiente virtual se tornou um espaço indispensável para a vida moderna, abrangendo diversas atividades do dia a dia, desde o lazer até o comércio e as relações profissionais, portanto, o surgimento e a evolução de tecnologias, como a internet e os dispositivos móveis, proporcionaram um fluxo constante de informações e criaram um novo cenário de interação social, cultural e econômica no ambiente digital.

Nesse contexto, o direito, enquanto instrumento para regular as atividades sociais, teve que enfrentar novos desafios para acompanhar as mudanças geradas pela evolução tecnológica, a crescente exposição de dados pessoais online em plataformas digitais, levantou questões essenciais sobre a privacidade dos indivíduos e a proteção de suas informações, pois diante da facilidade com que dados são coletados, processados e compartilhados por empresas, torna-se clara a necessidade de normas que garantam a segurança e o respeito à privacidade no uso dessas informações.

A relevância desse tema é inegável, visto que, diariamente, surgem relatos de vazamentos de dados, uso indevido de informações e ameaças à privacidade dos usuários. Diante disso, a Lei Geral de Proteção de Dados (LGPD), sancionada em 2018, representa um marco jurídico importante para a proteção dos direitos dos cidadãos no ambiente digital, estabelecendo regras claras sobre o tratamento de dados pessoais.

Assim, o presente trabalho visa discutir a proteção de dados pessoais online, analisando a evolução e o conceito de direito digital, e como ele pode afetar o cotidiano das pessoas, assim observando algumas legislações sobre o assunto, além de ressaltar a importância dos dados pessoas para a privacidade das pessoas e o interesse das instituições privadas nele, observado através de grandes casos de vazamentos. Para tanto, pretendesse analisar como o direito tem acompanhado o avanço tecnológico e os mecanismos previstos na LGPD para assegurar a privacidade dos usuários, e também busca-se refletir sobre a adequação da legislação às exigências do cenário atual, em que a coleta e o uso de dados são práticas rotineiras nas interações digitais, muitas vezes realizadas sem o pleno conhecimento ou consentimento dos titulares.

Desse modo o presente trabalho pretende compreender o papel da LGPD na proteção da privacidade e na segurança de dados, explorando sua aplicação e suas limitações, além de destacar a importância dessa regulamentação para o equilíbrio entre a inovação tecnológica e a preservação dos direitos fundamentais dos indivíduos.

## MÉTODO

O procedimento adotado será o método dedutivo, através de pesquisa bibliográfica, com pesquisas em fontes bibliográficas e artigos científicos. Para

o desenvolvimento da proposta, primeiramente será contextualizado sobre o direito digital, logo após será debatido quando aos dados digitais e sua importância e por fim será analisado a Lei Geral de Proteção de Dados Pessoais e como o direito tem feito para garantir a segurança online.

## RESULTADOS E DISCUSSÃO

### 1. DIREITO DIGITAL

#### 1.1 CONCEITO E EVOLUÇÃO

A sociedade está em constante transformação, ao longo da história, a humanidade tem evoluído continuamente, introduzindo novos conceitos e redefinindo seu caminho. Segundo Toffler (2008), três grandes ondas caracterizam a evolução da humanidade, sendo a primeira a era agrícola; a segunda, a era da revolução industrial; e a terceira, a era da informação, esta última teve início com as invenções voltadas à comunicação e, com o avanço tecnológico, tem acelerado exponencialmente a transmissão de informações.

A internet surgiu nos Estados Unidos em 1969, quando o Departamento de Defesa criou um sistema de comunicação que interligava centros de pesquisa militar, permitindo a troca de informações. Nos anos 1980, essa tecnologia se expandiu para conectar universidades e outros institutos de pesquisa, viabilizando a comunicação por meio de protocolos de leitura de documentos. Em 1993, com o avanço da tecnologia e o barateamento de equipamentos, a internet tornou-se acessível para empresas e indivíduos, utilizando linhas telefônicas comuns, o que consolidou a "rede mundial de computadores" como meio de interligação global. (Fonseca filho, Clézio, 2007)

Assim, foi criado um novo ambiente para a interação no âmbito digital, desse modo, surgindo junto com ele várias atividades, como operações de compra e venda realizadas online ou por outros sistemas de comunicação e a divulgação de conhecimento. Importante ressaltar que antigamente os negócios eram feitos de forma presencial, porém com o avanço tecnológico, surgiram novas formas de comunicação e a comunicação se tornou incrivelmente mais barata, rápida e praticamente instantânea, permitindo até videoconferências, gravações, e o envio de fotos e documentos.

Assim, como esse novo ambiente estabelecido, houve a possibilidade de realizar negócios jurídicos de formas diferentes além de diversas outras situações que antes o direito não previa, como a possibilidade de crimes cibernéticos e utilização de imagens e divulgações, desse modo o direito deve se atualizar e sofrer variações para estabelecer a ordem, paz, segurança e justiça, como manifesta Nader (2014, p. 53):

> “As instituições jurídicas são inventos humanos, que sofrem variações no tempo e no espaço. Como processo de adaptação social, o direito deve estar sempre se refazendo, em face da mobilidade social. A necessidade de ordem, paz,

> segurança, justiça, que o direito visa a atender, exige procedimentos sempre novos. Se o direito se envelhecer, deixa de ser um processo de adaptação, pois passa a não exercer a função para qual foi criado. Não basta, portanto, o ser do direito na sociedade, é indispensável o ser atuante, o ser atualizado. Os processos de adaptação devem-se renovar, pois somente assim o direito será um instrumento eficaz na garantia do equilíbrio e harmonia social".

Portanto, como o direito é uma criação humana com a função de regulamentar suas atividades, ele se manifesta como um sistema de controle social para garantir a harmonia, desse modo com o novo ambiente digital criado, se fez necessário que diversas adaptações e que mudanças fossem introduzidas para garantir a ordem nesse novo ambiente, assim dando origem ao direito digital, que deve abranger todas as outras áreas do direito, e trazer elas para esse novo ambiente, como estabelecido por Pinheiro (2021, p.49) em sua obra:

> Direito Digital consiste na evolução do próprio Direito, abrangendo todos os princípios fundamentais e institutos que estão vigentes e são aplicadas até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas (Direito Civil, Direito Autoral, Direito Comercial, Direito Contratual, Direito Econômico, Direito Financeiro, Direito Tributário, Direito Penal, Direito Internacional, etc.

Logo, é indispensável uma legislação que contemple questões do Direito Digital em todas as esferas do pensamento jurídico.

## 1.2 NOVAS POSSIBILIDADES E PRINCIPAIS LEGISLAÇÕES

Como estabelece Tarciso Teixeira (2018, p. 179):

> Se antes a interação entre homem e máquina somente era vislumbrada nas obras de ficção científica, hoje podemos afirmar que a vida passou a imitar a arte. Aquilo que antes parecia uma realidade distante, senão impossível, começou a integrar o cotidiano, trazendo situações jurídicas que necessitam de análise cuidadosa, tais como a responsabilidade civil por atos cometidos por sistemas de inteligência artificial autômatos.

Assim é evidente que o ambiente digital tem se tornado cada vez mais presente no cotidiano das pessoas, influenciando e transformando diversos aspectos da vida moderna, desde o trabalho até o lazer, ele desempenha um papel fundamental, tornando-se essencial para o funcionamento e o desenvolvimento da sociedade. Desse modo a digitalização dos processos está não apenas facilitando as interações, mas também redefinindo a forma como

as pessoas se conectam, consomem informações e conduzem suas atividades diárias.

Esse novo ambiente digital abriu diversas possibilidades, como a realização de negócios jurídicos no mundo virtual, seja por meio de redes sociais como Skype, Messenger e WhatsApp, ou através de aplicativos específicos para compra e venda de produtos. Além disso, grandes lojas e empresas oferecem a opção de compra diretamente em seus próprios sites, ampliando ainda mais as oportunidades de comércio online.

Além disso o ambiente digital facilitou a rápida troca de informações, incluindo mídias protegidas por direitos autorais e o compartilhamento de imagens pessoais, questões que demandam regulamentação adequada para garantir seu uso responsável. Outro avanço significativo foi a criação das criptomoedas, nesse sentido Lorenzetti (2004), ressalta que são intangíveis, herméticas, mutáveis, de modo que são inseridas em um complexo sistema inter-relacional. Também é importante destacar a crescente presença da inteligência artificial nesse contexto digital, adicionando uma nova camada de inovação e complexidade ao ambiente virtual.

Portanto, diante de todas essas inovações foram surgindo leis para regulamentar diversas situações envolvendo o digital, sendo que algumas nascerem somente após acontecer problemas que demonstravam a importância de existir regulamentação nessa área, sendo que algumas das mais importantes são:

### 1.2.1 Lei do Software (Lei 9.609/1998 – 19/02/1998)

A Lei nº 9.609, de 19 de fevereiro de 1998, conhecida como Lei do Software, estabelece normas sobre a proteção da propriedade intelectual de programas de computador no Brasil, equiparando os direitos do software aos direitos autorais, desse modo, a legislação estabelece em seu artigo 2º que o software é considerado propriedade do autor, que possui direitos exclusivos de uso, licenciamento e comercialização.

### 1.2.2 Lei de Acesso à Informação (Lei 12.527/2011 – 18/11/2011)

Conhecida como Lei de Acesso à Informação, garante o direito de qualquer cidadão acessar informações públicas de órgãos e entidades governamentais, promovendo a transparência na administração pública. Para tanto, o artigo 5º estabelece que qualquer cidadão pode solicitar informações de órgãos e entidades públicas, que devem ser fornecidas em prazo razoável e de forma gratuita, além de penalidades para o não cumprimento das normas estabelecidas.

### 1.2.3 Marco Civil da Internet (Lei 12.965/2014 – 24/04/2014)

O Marco Civil da Internet, estabelece princípios e garantias para o uso da internet no Brasil em seu artigo 7° inviolabilidade das comunicações e a confidencialidade das comunicações privadas armazenadas, salvo por ordem judiciaria, assim, a referida lei assegura a proteção da privacidade e dos dados pessoais, a inviolabilidade das comunicações e o direito à liberdade de expressão online. Além disso, o artigo 10º, trata da proteção dos registros e

dados pessoais, permitindo o fornecimento de dados a pedido de um juiz e impondo ao responsável pela guarda dos dados a obrigação de fornecê-los se solicitado judicialmente, e estabelece que o não cumprimento das determinações pode resultar em sanções legais, promovendo um ambiente mais seguro e transparente na internet.

### 1.2.4 Lei de Crimes Cibernéticos (Lei 12.737/2012)

Foi criada após a atriz Carolina Dieckmann, ter suas fotos pessoais vazadas na internet, situação essa que destaca a necessidade de uma legislação mais especifica e robusta para combater crimes virtuais e proteger a privacidade dos usuários. A referida lei estabelece penalidades para crimes praticados no ambiente digital, abrangendo atos como a invasão de dispositivos eletrônicos, a disseminação de vírus e a adulteração de dados. Como exemplo de penalidade o artigo 154-A do Código Penal, introduzido por esta lei, define como crime a invasão não autorizada de dispositivos informáticos, com penas para quem obtiver, adulterar ou destruir dados. Além disso a lei também prevê punições específicas para a criação e a propagação de programas maliciosos, como vírus e worms, visando proteger a integridade e a segurança dos sistemas e dados digitais.

### 1.2.5 LGPD (Lei Geral de Proteção de Dados – Lei 13.709/2018 – 14/08/2018)

Essa lei estabelece regras para a coleta, uso, armazenamento e compartilhamento de dados pessoais no Brasil, visando garantir a privacidade e a proteção das informações dos indivíduos, impondo obrigações às empresas e organizações que lidam com esses dados, ela possui extrema relevância para o tema do trabalho e será abordada mais detalhadamente.

## 2. DADOS PESSOAIS

### 2.1 PRIVACIDADE ONLINE

Com o avanço tecnológico e a criação desse novo ambiente digital, os dados pessoais tornam-se cada vez mais expostos e vulneráveis à coleta. Assim, a crescente dependência da tecnologia na sociedade moderna leva muitos indivíduos a abrir mão de sua privacidade e intimidade, frequentemente sem perceber o alcance das implicações que isso pode ter.

Uma forma encontrada de trazer segurança e regulamentar o ambiente virtual é a monitoração e vigilância para a prevenção de incidentes, e até punições por delitos cometidos nesse meio, porém é evidente que essa segurança encontra uma barreira natural no direito da privacidade e da intimidade do usuário. Para Patrícia Peck Pinheiro (2016), o direito à privacidade constitui um limite natural ao direito à informação, porém, não há lesão ao direito se houver consentimento, mesmo que implícito, na hipótese em que a pessoa demonstra de algum modo interesse em divulgar aspectos da própria vida.

Para Barreto e Faustino (2019), ao abordarem o uso de aplicativos de serviços para a saúde pública e a proteção dos dados pessoais dos usuários, a situação se revela extremamente delicada, pois, em um país como o Brasil,

com uma população tão numerosa, o correto tratamento desses dados é desafiador, o que aumenta o risco de violações à privacidade de uma grande quantidade de usuários, pontificando Barreto e Faustino (2019, n.p.) que:

> A privacidade está ligada a dignidade da pessoa humana, princípio também insculpido na Constituição Federal em seu art. 1o, inciso III e está intimamente ligada com a confidencialidade nos casos envolvendo dados sensíveis relativos à saúde das pessoas, onde no ambiente da internet e das aplicações de internet, a possibilidade da violação da privacidade ganha níveis exponenciais, quer seja pela falta de zelo daqueles que realizam o tratamento dos dados pessoais, quer seja dos próprios usuários, [...]

Importante mencionar que as empresas privadas são grandes interessadas nos dados disponibilizados pelos usuários, que buscam forma de lucrar a partir dessas informações, nesse sentido Pinheiro (2021, p.60) ressalta:

> Se, por um lado, cresce a cada dia o número de empresas que disputam os consumidores da Internet e, consequentemente, a publicidade virtual, com preenchimento de formulários e cadastros, por outro lado, cresce também o nível de conscientização dos consumidores quanto à possibilidade de aplicação do atual Código do Consumidor, que trata da matéria de utilização de informações de consumidores para fins comerciais, trazendo uma série de penalidades para quem as pratica.

Desse modo, é evidente que essa nova realidade da qual dados são constantemente coletados por empresas e plataformas digitais, há uma violação ao disposto no artigo 5º, inciso X, da Constituição Federal (BRASIL, 1988), que garante a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas, assegurando o direito à indenização por danos materiais ou morais decorrentes de sua violação. No contexto do mundo digital em que a sociedade está inserida, esse dispositivo constitucional frequentemente não é respeitado.

Como demonstrado, muitos dos problemas que surgiram com a nova Era Digital estão diretamente relacionados às violações dos princípios estabelecidos pela Constituição Federal, especialmente no que diz respeito ao direito à privacidade das pessoas físicas e, em alguns casos, das pessoas jurídicas. Embora o sigilo de dados, correspondências e comunicações seja garantido tanto pela Constituição brasileira quanto por legislações internacionais de defesa dos Direitos Humanos, o grande desafio da atualidade é encontrar maneiras eficazes de garantir esses direitos em uma sociedade digital, caracterizada pela ausência de fronteiras físicas.

## 2.2 INTERESSE PRIVADO NOS DADOS PESSOAIS

Deve ser ressaltado que a coleta de dados por plataformas digitais criou uma nova realidade para a sociedade, na qual esses dados são comercializados, porém, os dados só adquirem valor quando são processados e convertidos em informações, que, quando alinhadas a um objetivo específico, como a publicidade, geram um valor significativo para as empresas que os utilizam. Isso explica por que a maioria das plataformas digitais são oferecidas gratuitamente, e lucram através da publicidade. Desse modo, para Bioni (2019) é notável que a formatação desse modelo de negócio, onde os serviços são oferecidos de forma gratuita, confirma, portanto, a monetização dos dados pessoais, tornando economicamente viável esse grande volume de produtos e serviços que são “gratuitamente” disponibilizados na internet.

Dessa forma, estabelece-se uma troca: os serviços oferecidos pelas plataformas digitais em troca dos dados pessoais dos usuários, a partir de cada interação, inicia-se a coleta de dados, seja quando o usuário interage em uma rede social, lê um e-mail, ou até mesmo observa por mais tempo uma imagem ou anúncio, sendo que cada movimento é registrado, contribuindo para o acúmulo de informações que podem ser analisadas e utilizadas pelas empresas. Sendo assim Pinheiro (2021, pg. 67) conceitua: “Há uma expressão atual para retratar o modelo de riqueza da web que diz: se o serviço for gratuito, você não é o freguês, você é o produto!”

Deve ser mencionado que para Pinheiro (2021) não há lesão ao direito a privacidade se houver consentimento. Desse modo, o grande ponto desta análise é questionar se os usuários dessas plataformas realmente dão consentimento para que seus dados sejam comercializados, alimentando o mercado de publicidade direcionada, ou se ficam sem alternativa, já que, ao não aceitarem, perdem o acesso aos serviços oferecidos. Assim, essa questão merece uma avaliação cuidadosa, pois, na maioria das plataformas digitais, especialmente nas redes sociais, não há como optar por não permitir a coleta e uso de dados, assim, a possibilidade de oferecer a opção de pagar pelos serviços, estabelecendo uma relação de consumo bilateral, poderia resolver o problema do consentimento, eliminando a obrigatoriedade da coleta de dados como condição de uso.

## 2.3 GRANDES CASOS DE VAZAMENTOS DE DADOS

Como discutido, os dados pessoais contêm informações valiosas para as empresas, além de representarem a privacidade dos usuários. Assim, o vazamento de dados é um incidente de segurança que pode ter consequências graves, pois expõe essas informações de forma não autorizada, tornando-as vulneráveis. Quando isso ocorre, os dados podem ser visualizados, copiados, transmitidos e utilizados sem o consentimento do titular e sem que ele tenha conhecimento da finalidade ou do propósito dessa manipulação, nesse sentido Pinheiro (2021, p.134) ressalta:

> A principal causa para o vazamento de informações são as próprias ações humanas. Com propriedade, o autor Antônio

> Everardo Nunes da Silva destaca que a falha humana é o principal motivo para darmos maior atenção à Segurança da Informação. Mesmo dentro do ambiente corporativo, ou até mesmo dentro da própria residência, é necessário ter cautela com os ativos e informações que são suscetíveis de vazamento. Dessa forma, devemos estar cada vez mais atentos e conscientes de que a informação é a moeda mais preciosa na era do conhecimento.

Porém, esses incidentes de vazamento de dados não são raros ou isolados, e cada vez mais relatos de casos surgem ao redor do mundo.

Como exemplo de um grave e catastrófico quadro de vazamentos de dados é o caso da empresa Cambridge Analytica, que, de acordo com o portal de notícias G1, aconteceu em 2018, no qual é uma empresa americana coletou informações pessoais de 50 milhões de usuários, através da rede social Facebook, por meio de um teste psicológico na rede social, e os usuário que participaram acabaram entregando à Cambridge Analytica não apenas suas informações, mas os dados referentes a todos os amigos do perfil.

A empresa Cambridge Analytica, é uma empresa de análise de dados que trabalhou na campanha do republicano Donald Trump nas eleições de 2016, nos Estados Unidos, e também teria sido contratada pelo grupo que promovia a saída do Reino Unido da União Europeia.

Desse modo os dados coletados sem consentimento teriam sido usados para catalogar o perfil das pessoas e, então, direcionar, de forma mais personalizada, materiais pró-Trump e mensagens contrárias à adversária dele, a democrata Hillary Clinton.

O Banco Inter enfrentou uma grave violação de segurança em 2018, quando, de acordo com o portal de notícias G1, dados de cerca de 20 mil clientes, incluindo informações bancárias e senhas, foram expostos. O vazamento ocorreu após uma tentativa de extorsão por hackers, que ameaçaram divulgar os dados. Inicialmente, o banco negou o problema, mas uma investigação do Ministério Público do Distrito Federal e Territórios (MPDFT) confirmou a falha de segurança, levando à abertura de um processo judicial.

Desse modo, o Banco Inter firmou um acordo com o Ministério Público do Distrito Federal e Territórios (MPDFT), pagando R$ 1,5 milhão, o valor foi destinado a iniciativas de combate a crimes cibernéticos e outras instituições de caridade. Esse caso ressalta a crescente preocupação com a proteção de dados no setor financeiro, à medida que ataques cibernéticos se tornam mais sofisticados e frequentes, expondo a vulnerabilidade de sistemas bancários e a necessidade de medidas robustas de segurança para garantir a privacidade dos clientes.

Em dezembro de 2020, de acordo com o portal de notícias G1, uma nova falha do Ministério da Saúde expôs os dados pessoais de 243 milhões de brasileiros na internet, entre os dados vazados estavam informações sensíveis como nomes completos, CPF, endereço e histórico médico. A exposição ocorreu devido a uma configuração inadequada de servidores, permitindo o acesso não autorizado a informações de cidadãos, incluindo até mesmo pessoas falecidas.

Portanto, fica claro que a privacidade das pessoas na internet é algo que se encontra em constante risco, vez que existem diversos casos de vazamentos de dados, como os citados. Desse modo é evidente que o direito deve estar em constante evolução para acompanhar e evitar esses casos, sobre o tema Calaza (2020, p. 181) destaca:

> Na contemporaneidade, os indivíduos se deparam cotidianamente com situações muito mais emblemáticas envolvendo sua privacidade do que as meras publicações jornalísticas invasivas que ocorriam no século XIX. Hoje, é possível se deparar com institutos como: o direito ao esquecimento, data mining, política de cookies, copyright, uso de drones, testamento digital em rede social, vazamentos massivos de dados e muitas outras hipóteses que põe à prova a evolução jurídica do direito à privacidade individual.

Assim é evidenciado que a proteção dos dados pessoais é algo que certamente deve ser feito, vez que a privacidade do usuário deve ser respeitada, além de que, com o vazamento desses dados abre a possibilidade de usos ilegais, como forma de empresas lucrarem em cima, criminosos terem acesso a endereço, CPF e nome de diversas pessoas, sendo possível até afetar a política como mostrado no caso do vazamento do facebook. Desse modo, fica claro a importância de legislações que regulamentem e protejam essa questão.

# 3 LEI GERAL DE PROTEÇÃO DE DADOS

## 3.1 PRINCIPAIS PONTOS

Conforme conceitua Pinheiro em sua obra “Direito digital” (2021, pg.284), que a LGPD é uma Lei que:

> Inaugurou-se um novo marco legal brasileiro para as instituições privadas e públicas. Isso porque a Lei Geral de Proteção de Dados Pessoais, ou LGPD, discorre acerca da proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações que possam ser enquadradas como dados pessoais, ou seja, que estejam relacionadas a uma pessoa natural identificada ou identificável e que sejam tratadas em qualquer meio ou suporte, seja por pessoa jurídica ou por pessoa física.

A Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), introduziu novas regulamentações com o intuito de mitigar os riscos associados ao uso inadequado de dados coletados no âmbito digital. Além disso, busca-se, ao longo do tempo, estabelecer uma base sólida de segurança jurídica sobre o tema.

A regulamentação em questão é amplamente técnica, indo além de meras regras e diretrizes: estabelece princípios, direitos e obrigações relacionados ao uso das bases de dados pessoais, um ativo fundamental e relevante na sociedade contemporânea. O principal objetivo da LGPD é proteger os direitos fundamentais à liberdade, à privacidade e ao livre desenvolvimento da personalidade da pessoa natural, sempre pautada pela premissa da boa-fé em qualquer tratamento de dados pessoais, pontos esses que serão abordados neste capítulo.

Fundamentos da LGPD (BRASIL, 2018) estão previstos em seu artigo 2° sendo eles: respeito à privacidade; autodeterminação informativa; liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico, tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Ao examinar os fundamentos previstos neste artigo, torna-se claro que a principal preocupação da lei é proteger o titular dos dados, pois a maioria dos fundamentos está diretamente relacionada a ele, uma vez que o uso de seus dados só é permitido mediante seu consentimento. Dessa forma, o titular assume um papel ativo no processo, consolidando seu controle sobre suas informações pessoais.

Já os princípios da LGPD (BRASIL,2018) estão contidos em seu artigo 6°, sendo eles: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas. Todos esses princípios devem ser respeitados quando do tratamento de dados e nesse sentido percebe-se que o uso de dados deve ser feito de forma consciente e limitando-se a um fim específico, não sendo, portanto, permitido a partir da entrada em vigor da referida legislação que o uso exacerbado e irrestrito de dados pessoais permaneça.

Em seu artigo 5° a Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018) traz alguns conceitos que são abordados por ela e necessários para sua compreensão, sendo alguns mais importantes:

> *I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;*
>
> *II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato*

> *ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;*
>
> *III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;*
>
> *IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;*
>
> *V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;*
>
> *VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;*
>
> *VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;*
>
> *VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);*
>
> *IX - agentes de tratamento: o controlador e o operador;*
>
> *X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;*

Em síntese, a Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018) estabelece um marco regulatório fundamental para a proteção dos dados pessoais no Brasil, visando assegurar os direitos de privacidade e autodeterminação informativa. Com seus princípios, fundamentos e conceitos claramente delineados, a LGPD confere maior controle ao titular sobre suas informações e impõe responsabilidades às entidades que tratam esses dados. Pinheiro (2021, pg.284) conceitua: “Importante destacar que o objetivo da LGPD é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”, de modo que a referida lei visa favorecer o titular dos dados pessoais.

## 3.2 RESPONSABILIDADE CIVIL PELA LGPD E SANÇÕES

Como já mencionado, vivemos em uma era em que o digital está cada vez mais integrado ao nosso cotidiano. A tecnologia tornou-se parte essencial da vida das pessoas, o que torna indispensável a regulamentação desse espaço, como exemplificado pela Lei Geral de Proteção de Dados (BRASIL, 2018). Assim, aspectos como a responsabilidade civil no tratamento de dados e

as sanções aplicáveis devem ser abordados de forma clara e objetiva pela legislação.

Desse modo a Lei Geral de Proteção de Dados (BRASIL, 2018) define quem seriam os agentes de tratamento responsáveis pela coleta, tratamento, armazenamento e exclusão de dados pessoais, portanto, se a coleta não for realizada de maneira correta e prevista na lei, podem ser responsabilizados por eventuais prejuízos civilmente. Assim, quanto a responsabilidade a obrigação de reparar Sílvio de Salvo Venosa (2023, pg. 22) esclarece:

> Por vezes, a vontade não atua no sentido precípuo de criar uma obrigação, mas no de ocasionar intencionalmente um dano, com consequente prejuízo. Nasce a obrigação de reparar o dano, de pagar indenização. Também pode ocorrer que a vontade não atue diretamente a fim de criar um dever de indenizar, mas a conduta do agente, decorrente de negligência, imprudência ou imperícia, culpa no sentido estrito, ocasiona um dano indenizável no patrimônio alheio.

Desse modo, a Lei Geral de Proteção de Dados (BRASIL, 2018), em sua sessão III, esclarece sobre a responsabilidade dos agentes de tratamento, de modo que o artigo 42 dispõe:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
>
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
>
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
>
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.
>
> § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
>
> § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.

> § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Assim é evidente que o controlador ou o operador, ao realizar o tratamento de dados, é responsável por eventuais danos que possa causar ao usuário, que podem ser consumidores, de modo que existe a responsabilidade solidaria na situação descrita. Sobre isso Pinheiro (2021, pg. 288) esclarece:

> Já o Operador pressupõe uma nova relação, que é estabelecida com o Controlador e não com o Titular, normalmente por meio de subcontratação, terceirização ou transferência de atividade. Sua atuação é dependente do Controlador e traz responsabilidades específicas que irão recair sobre ele diretamente, inclusive por solidariedade (conforme o art. 42).

Além disso, como a maioria das relações de tratamento de dados os titulares dos dados são consumidores, algumas hipóteses do código de defesa do consumidor podem ser aplicadas ao caso, como por exemplo no artigo 42, § 2º, onde a lei permite que o juiz no processo, possa inverter o ônus da prova a favor do titular de dados, algo semelhante ao que ocorre no Código de Defesa do Consumidor (BRASIL, 1990) - a inversão do ônus probatório a favor do consumidor.

Desse modo é perceptível que os agentes de tratamento de dados possuem responsabilidade pelos dados que estão tratando, de modo que o artigo 52 da LGPD (BRASIL, 2018) prevê algumas sanções para infrações cometidas contra as normas estabelecidas na lei, como advertências, multas, e até suspensão das atividades.

Importante ressaltar que o parágrafo primeiro do artigo referido esclarece que as sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios previstos na lei. Além disso as sanções não devem substituir as sanções administrativas.

Em resumo, todas as pessoas e instituições que manuseiam dados pessoais de terceiros com fins econômicos devem seguir os princípios estabelecidos pela Lei Geral de Proteção de Dados Pessoais, assegurando que todas as operações sejam orientadas por interesses lícitos e permitidos pela legislação, pois podem responder civilmente por eventuais prejuízos causado aos titulares dos dados, além de poderem incorrer em sanções prevista na Lei Geral de Proteção de Dados (BRASIL, 2018).

## 3.3 IMPACTOS DA LGPD

A Lei Geral de Proteção de Dados entrou em vigor em 18 de setembro de 2020, e como abordado ela visa proteger os dados dos usuários, visando defender o seu direito a privacidade.

Importante ressaltar que a LGPD (BRASIL, 2018) não proíbe o tratamento de dados, mas estabelece um conjunto de proteções para essa atividade, com princípios que legitimam sua realização. Assim, a referida lei determina que o tratamento de dados pessoais só pode ocorrer quando observados o princípio primordial da boa-fé, além de outros princípios descritos no artigo 6º a Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018), sendo eles:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Diante desse modo, a coleta e também o tratamento de dados devem ter uma finalidade explícita para o usuário, sendo essa compatível, necessária, de livre acesso e transparente. Importante mencionar que antes da Lei Geral de Proteção de Dados, a legislação brasileira contava apenas com artigos perdidos sobre o tema, de modo que a LGPD (BRASIL, 2018) demostra um

grande avanço para a sociedade brasileira, proporcionando uma proteção significativa aos direitos dos cidadãos, que desde o surgimento e desenvolvimento da internet estavam vulneráveis ao tratamento inadequado de seus dados.

Como abordado para regular o ambiente digital, além de estabelecer regras e diretrizes, a Lei Geral de Proteção de Dados (BRASIL, 2018) traz sanções com o fim de regulamentar o ambiente digital e punir infrações além de responsabilizar civilmente os operadores dos dados por eventuais danos causados aos clientes, de modo que assim o ambiente digital não se torna um local caótico e seguro para os usuários.

Importante ressaltar que nessa lei foi criada a Autoridade Nacional de Proteção de Dados, a ANPD, que ficará responsável por fazer as devidas fiscalizações e para garantir que a lei tenha a devida aplicação. Como diz Patrícia Peck Pinheiro (2021, pg.285):

> Vale lembrar que a ANPD617 foi elaborada para ajudar a proteger o mercado e a implementar a proteção de dados, numa atuação de garantir o cumprimento e o melhor proveito da regulamentação, seja por meio de normas complementares e pareceres técnicos, seja por procedimentos de inspeção.

Importante mencionar que o artigo 4 estabelece casos em que a Lei Geral de Proteção de dados (BRASIL, 2018) não poderá ser aplicada, a fim de proteger os direitos fundamentais a privacidade e intimidade pessoal, de modo que a lei dispõe o seguinte:

> 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.

Dessa forma, Basan (2024, pg. 90) destaca:

> Com efeito, o legislador foi cauteloso ao traçar limites de aplicação da LGPD, notadamente buscando o equilíbrio entre direitos fundamentais que, em determinadas situações, podem entrar em conflito, como a vida privada, o sigilo de comunicações, a liberdade de expressão, de informação, religiosa e cultural; além da ordem pública, evidenciada no tratamento de dados, pelo poder público, envolvendo investigação, segurança e defesa.

Dessa forma é evidente que a LGPD (BRASIL, 2018) traçou limites para sua aplicação, levando em conta diversos princípios como citado, mas é evidente que isso pode trazer brechas para fugir da regulamentação dessa lei.

Observa-se que no caso do inciso I do artigo 4° da LGPD (BRASIL, 2018) onde prevê que a lei não se aplica ao tratamento de dados realizado por pessoa natural para fins exclusivamente particulares e não econômicos, Basan (2024, pg. 91) esclarece:

> A não aplicação da LGPD, nessas situações, encontra fundamento na finalidade principal da norma, qual seja, regular o uso de dados pessoais com a finalidade econômica, capaz de interferir na vida privada e promover a indevida vigilância das pessoas humanas", Em virtude dessa limitação imposta pela LGPD, percebe-se que ela não abarca todas as situações em que a privacidade ou intimidade de um cidadão pode ser violada, como no caso de vídeos, fotos ou áudios armazenados e compartilhados sem autorização por pessoas naturais.

Desse modo, a LGPD (BRASIL, 2018) representa um avanço significativo no cenário jurídico brasileiro, promovendo uma cultura de respeito à privacidade e proteção de dados pessoais, mesmo sendo inegável que a aplicação dessa lei ainda enfrenta desafios, especialmente em um ambiente digital dinâmico e em constante evolução.

## CONSIDERAÇÕES FINAIS

O presente trabalho visou compreender como o direito, por meio de normas como a Lei Geral de Proteção de Dados (LGPD), tem se adequado às rápidas transformações tecnológicas, buscando assegurar a privacidade e a proteção de dados pessoais no ambiente digital. Desse modo, a pesquisa permitiu analisar como o avanço da tecnologia, especialmente no que tange à coleta e uso de dados pelos mais diversos atores no meio digital, trouxe novos desafios para o direito, exigindo uma atualização das normas e a criação de mecanismos eficazes de proteção.

Deve ser ressaltado que a LGPD foi destacada como um marco regulatório fundamental no Brasil, estabelecendo regras claras para o tratamento de dados e impondo responsabilidades tanto para empresas quanto

para órgãos públicos, desse modo a análise dessa legislação evidenciou que o Brasil deu um passo importante em direção à proteção da privacidade online, ao garantir ao cidadão maior controle sobre suas informações e assegurar que essas sejam utilizadas de forma consciente e transparente.

Contudo, algumas limitações ficaram evidentes ao longo do trabalho, sendo que, a recente implementação da LGPD ainda traz desafios práticos, levando em conta a complexidade do ambiente digital, com inovações constantes, como a inteligência artificial e as criptomoedas, demanda uma atualização contínua do direito, o que pode gerar uma necessidade de novas regulamentações complementares.

Outro fator que limita a plena eficácia da LGPD é a conscientização do próprio usuário, que muitas vezes não tem ciência de seus direitos ou de como seus dados estão sendo utilizados, de modo que o fortalecimento de campanhas educativas e uma atuação mais robusta da Autoridade Nacional de Proteção de Dados (ANPD) são essenciais para consolidar os avanços propostos pela legislação. Além disso, existem situações em que LGPD não pode ser aplicada, de modo que brechas podem ser geradas para fugir de sanções e punições.

Desse modo, é evidente a necessidade de estudos que aprofundem temas como o impacto da inteligência artificial na privacidade, a regulamentação de novas tecnologias que surgem no ambiente digital, e a responsabilidade internacional no tratamento de dados em um mundo cada vez mais conectado, para tanto, deve-se investigar como outros países estão lidando com esses desafios e compará-los com o cenário brasileiro pode contribuir significativamente para aprimorar a proteção de dados no Brasil.

Assim, conclui-se que, embora tenha sido possível atingir os objetivos propostos neste trabalho, o campo do direito digital permanece em constante evolução, exigindo um acompanhamento atento para que o equilíbrio entre inovação e proteção de direitos fundamentais seja mantido.

## REFERÊNCIAS


BARRETO JUNIOR, Irineu Francisco; FAUSTINO, André. **Aplicativos de serviços de saúde e proteção dos dados pessoais dos usuários**, 2019. Disponível em: https://revista.unicuritiba.edu.br/index.php/RevJur/article/view/3311/371371803. Acesso em 13 set. 2024.

BASAN, Arthur Pinheiro. et al. **Comentários a lei geral de proteção de dados pessoais**. 2. ed. Indaiatuba, SP: Editora Foco, 2024.

BIONI, Bruno Ricardo. **Proteção de dados pessoais a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2019.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. **Diário Oficial da União**: Seção 1, Brasília, DF, p. 1, 05 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 14 nov. 2024.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. **Diário Oficial da União**: seção 1, Brasília, DF, p. 1, 18 nov. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 14 nov. 2024.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. **Diário Oficial da União**: seção 1, Brasília, DF, p. 1, 3 dez. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 14 nov. 2024.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**: seção 1, Brasília, DF, p. 1, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 14 nov. 2024.

BRASIL**.** Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). **Diário Oficial da União**: seção 1, Brasília, DF, p. 1, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 nov. 2024.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Diário Oficial da União**: seção 1, Brasília, DF, p. 1, 12 set. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 14 nov. 2024.

BRASIL. Lei nº 9.609, de 19 de fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no país, e dá outras providências. **Diário Oficial da União**: seção 1, Brasília, DF, p. 1, 20 fev. 1998. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9609.htm. Acesso em: 14 nov. 2024.

CALAZA, Tales. et al. **Fundamentos do direito digital**. Uberlândia: LAECC, 2020.

FONSECA FILHO, Cléuzio. **História da computação**: O Caminho do Pensamento e da Tecnologia. – Porto Alegre : EDIPUCRS, 2007.

G1. **MP do DF pede indenização de R$ 10 milhões ao Banco Inter por vazamento de dados de clientes**. G1, 2018. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/2018/07/31/mp-do-df-pede-indenizacao-de-r-10-milhoes-ao-banco-inter-por-vazamento-de-dados-de-clientes.ghtml. Acesso em: 25 out. 2024.

G1. **Nova falha do Ministério da Saúde expõe dados de 243 milhões de brasileiros na internet, diz jornal**. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-dados-de-243-milhoes-de-brasileiros-na-internet-diz-jornal.ghtml. Acesso em: 07 dez. 2024.

LORENZETTI, Ricardo L. **Comércio Eletrônico**. São Paulo: Revista dos Tribunais, 2004.

NADER, Paulo. **Introdução ao estudo do direito**. 36. Ed. Rio de Janeiro: interEditora Forense, 2018

PINHEIRO, **Patrícia Peck. Direito Digital**. 6. ed. São Paulo: Saraiva. São Paulo, 2016.

TEIXEIRA, Tarcisio. **Direito digital e processo eletrônico**. 6. ed. São Paulo: SaraivaJur, 2022.

THOMPSON, Stuart. **Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades**. G1, 2018. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml. Acesso em: 25 out. 2024.

TOFFLER, Alvin. **The third wave**. New York: Bantam Books, 1980

VENOSA, Sílvio de Salvo. **Direito civil obrigações e responsabilidade civil**. 23. ed. Rio de Janeiro: Atlas, 2023.