CENTRO DE ENSINO SUPERIOR CESREI LTDA

CURSO DE BACHARELADO EM DIREITO

MARCUS VINICIUS LUNA FARIAS JÚNIOR

SEGURANÇA DA INFORMAÇÃO E LGPD: MELHORES PRÁTICAS E TECNOLOGIAS DE PROTEÇÃO DE DADOS À LUZ DO DIREITO BRASILEIRO

Trabalho de Conclusão de Curso em formato de artigo apresentado à Coordenação do Curso de Direito da Cesrei Faculdade como requisito parcial para a obtenção do grau de Bacharel em Direito pela referida instituição.

Orientador: Prof. Esp. Wendley Steffan Ferreira dos Santos, Cesrei Faculdade

1º examinador: Prof. Me. Diego Araújo Coutinho, Cesrei Faculdade

2º examinador: Profª Esp. Sabrina Matias Cavalcante, Cesrei Faculdade

[

CAMPINA GRANDE - PB

2025

SEGURANÇA DA INFORMAÇÃO E LGPD: MELHORES PRÁTICAS E TECNOLOGIAS DE PROTEÇÃO DE DADOS À LUZ DO DIREITO BRASILEIRO

JÚNIOR, Marcus Vinicius Luna Farias[1]
STEFFAN, Wendley[2]

RESUMO

O presente trabalho tem como objetivo analisar os fundamentos jurídicos e práticos da Lei Geral de Proteção de Dados Pessoais (LGPD), destacando as melhores práticas e tecnologias voltadas à proteção de dados em ambientes corporativos. A pesquisa parte da relevância crescente da segurança da informação no contexto da transformação digital e da necessidade de garantir o direito à privacidade, conforme assegurado pela Constituição Federal de 1988. Utilizando-se de uma abordagem qualitativa, de natureza exploratória e bibliográfica, com análise documental de legislações, artigos acadêmicos e materiais doutrinários, o estudo examina como as organizações devem estruturar seus processos internos para alcançar a conformidade legal. Além de abordar os princípios da LGPD, o trabalho discute o papel do encarregado de dados, a importância da governança da informação e a responsabilidade civil das empresas em casos de vazamento ou uso indevido de dados pessoais. Também são destacadas tecnologias de proteção como criptografia, autenticação multifatorial, backups seguros e sistemas de controle de acesso, que, combinadas a uma postura ética e preventiva, compõem o conjunto de medidas necessárias para a segurança jurídica e informacional das instituições. Dessa forma, entende-se que o cumprimento da LGPD vai além da simples adequação normativa, exigindo mudanças culturais, estratégicas e tecnológicas profundas dentro das corporações. Assim, a efetividade da proteção de dados depende diretamente do compromisso institucional com a transparência, a ética e o respeito aos direitos fundamentais dos titulares de dados.

Palavras-chave: LGPD; Proteção de Dados; Segurança da Informação.

ABSTRACT

This paper aims to analyze the legal and practical foundations of the General Law for the Protection of Personal Data (LGPD), highlighting the best practices and technologies aimed at data protection in corporate environments. The research is based on the growing relevance of information security in the context of digital transformation and the need to guarantee the right to privacy, as guaranteed by the Federal Constitution of 1988. Using a qualitative, exploratory and bibliographical approach, with documentary analysis of legislation, academic articles and doctrinal materials, the study examines how organizations should structure their internal processes to achieve legal compliance. In addition to

[1] Concluinte do Curso de Direito da Cesrei Faculdade. Email: vini89luna@gmail.com
[2] Professor, Orientador. do Curso de Direito da Cesrei Faculdade. Email: wendely_789@hotmail.com

addressing the principles of the LGPD, the paper discusses the role of the data controller, the importance of information governance and the civil liability of companies in cases of leakage or misuse of personal data. Protection technologies such as encryption, multifactor authentication, secure backups and access control systems are also highlighted, which, combined with an ethical and preventive stance, make up the set of measures necessary for the legal and informational security of institutions. Therefore, it is understood that compliance with the LGPD goes beyond simple regulatory adaptation, requiring profound cultural, strategic and technological changes within corporations. Thus, the effectiveness of data protection depends directly on the institutional commitment to transparency, ethics and respect for the fundamental rights of data subjects.

Key word: LGPD; Data Protection; Information Security.

1 INTRODUÇÃO

A crescente digitalização das relações econômicas e sociais tem impulsionado um aumento significativo no volume de dados pessoais coletados e processados por empresas e organizações. Esse fenômeno evidencia a necessidade de mecanismos eficazes de proteção dessas informações, uma vez que o uso indevido por terceiros pode resultar em graves violações à privacidade e segurança dos indivíduos.

Nesse contexto, a Lei Geral de Proteção de Dados Pessoais (LGPD), sancionada em 2018, estabelece um marco regulatório fundamental no Brasil, disciplinando o tratamento de dados pessoais e impondo obrigações às entidades envolvidas nesse processo, assegurando direitos fundamentais como a privacidade e a proteção dos dados (Brasil, 2018).

A implementação da LGPD, contudo, enfrenta desafios práticos e tecnológicos, uma vez que muitas empresas ainda carecem de infraestrutura adequada e políticas de segurança da informação eficientes. A assimetria entre grandes corporações e pequenas empresas, no que tange a recursos financeiros e conhecimento técnico-jurídico, também se apresenta como um obstáculo para a plena conformidade com a legislação (Strack, 2024).

Diante desse cenário, torna-se essencial analisar as melhores práticas de segurança da informação e as tecnologias disponíveis que possam contribuir para a proteção de dados pessoais, garantindo o cumprimento das normativas estabelecidas.

A segurança da informação fundamenta-se em pilares como confidencialidade, integridade e disponibilidade, os quais são indispensáveis para garantir a proteção de dados no ambiente digital. Dessa forma, a adoção de soluções como criptografia, anonimização, pseudonimização e sistemas de prevenção de vazamento de dados (DLP) torna-se essencial para a mitigação de riscos. Conforme destaca Schneier (2017), a tecnologia, por si só, não é suficiente para garantir a segurança da informação, sendo necessária sua integração com boas práticas de governança e diretrizes organizacionais claras.

Portanto, o presente estudo tem como objetivo analisar as melhores práticas e tecnologias de proteção de dados no contexto da segurança da informação, considerando a legislação brasileira vigente, em especial a LGPD.

De forma específica, busca-se compreender os princípios e exigências da LGPD, identificar as principais vulnerabilidades de segurança da informação em ambientes corporativos e institucionais, bem como apontar recomendações para o aprimoramento da proteção de dados no Brasil, tendo em vista a crescente sofisticação das ameaças digitais.

A relevância do presente estudo se justifica pelo crescimento exponencial do volume de dados pessoais tratados por empresas e pela necessidade de garantir um ambiente digital seguro e em conformidade com a legislação. Conforme ressalta Doneda (2020), a privacidade e a proteção de dados são direitos fundamentais que devem ser assegurados por meio de mecanismos legais e tecnológicos eficazes. Além disso, Viola (2019) enfatiza que a principal dificuldade das organizações está na integração de políticas de segurança da informação aos seus processos internos, de modo a garantir a proteção dos dados sem comprometer a eficiência operacional.

A metodologia adotada para a condução deste trabalho baseia-se em uma abordagem qualitativa, com revisão bibliográfica e análise documental, além da investigação de casos práticos de empresas que se adequaram à LGPD.

Dessa forma, pretende-se, assim, contribuir para a literatura acerca da segurança da informação no Brasil e fornecer subsídios para a implementação de soluções mais eficazes no campo da proteção de dados pessoais.

2 LEI GERAL DE PROTEÇÃO DE DADOS: BREVE RELATO

2.1 LEI GERAL DE PROTEÇÃO DE DADOS

No mundo atual, com a globalização, os dados são tidos como insumos essenciais para toda e qualquer atividade econômica, como citado por Frazão *et. al* (2019) e acabaram por se tornar, objeto de crescente e pujante mercado.

Os dados podem até ser considerados o novo petróleo, de acordo com estudo de Nick Srnicek (2018) uma economia movida a dados passa-se a ter seu foco na extração e uso de dados pessoais dos indivíduos.

É correto afirmar que, o fenômeno do avanço das tecnologias e da globalização que faz os dados se tornarem tão importantes não se resumem apenas ao setor econômico, mas sim apresenta diversas repercussões nas esferas individuais dos cidadãos.

Com base nisso, os dados ao longo do tempo, sobretudo, atualmente ganharam uma importância maior do que já tiveram em qualquer época, tornando-se "vetores das vidas e liberdades individuais", assim como da sociedade e da democracia como um todo, como mencionado no estudo de Frazão *et. al* (2019).

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n° 13.709/2018, foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade, e a livre formação da personalidade de cada indivíduo. A Lei trata e discorre sobre o tratamento de dados pessoais, que são dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado, englobando um amplo conjunto de operações que podem ocorrer em meios manuais ou digitais, como pode-se ver abaixo:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
>
> Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.

Visto isso, a legislação estabelece uma estrutura legal de direitos dos

cidadãos que são titulares dos dados. Além disso, esses direitos devem ser garantidos durante toda a existência do tratamento dos dados pessoais realizados por órgãos competentes; para isso, a LGPD dispõe um de um conjunto de instrumentos que aprofundam obrigações de se tratar os dados com transparência ativa e passiva, e também criam meios processuais para que possam mobilizar a administração pública.

Como aponta Peck (2018), a regulamentação surgiu para equilibrar o avanço tecnológico e a necessidade de proteção das informações pessoais, promovendo maior transparência e responsabilidade no tratamento de dados. Além disso, ela se tornou um marco no cenário jurídico brasileiro, pois unifica normas dispersas e garante um tratamento uniforme aos dados pessoais.

Antes de sua implementação, dispositivos de proteção de dados estavam fragmentados em legislações como o Código Civil, o Código de Defesa do Consumidor e o Marco Civil da Internet, uma vez que o tratamento de dados pessoais, em particular os advindos no meio digital, é uma atividade que oferece risco e que se concretiza na possibilidade de exposição e utilização indevida ou abusiva de dados pessoais do indivíduo, por isso mesmo com o advento da era digital se amplificam os desafios relacionados à proteção de dados, sobretudo diante da crescente busca por informações pessoais por empresas de tecnologia.

Por conseguinte, com a crescente da dependência dos fluxos internacionais por meio de dados e o modelo de negócios baseado na economia digital intensificaram a necessidade de estabelecer diretrizes cada vez mais claras sobre o uso dessas informações, ou seja, de modo a evitar abusos em ambientes como redes sociais, aplicativos e marketplaces e assegurar a conformidade das empresas com padrões éticos e legais.

O art. 2º da LGPD discorre sobre os seguintes fundamentos: respeito à privacidade, autodeterminação informativa, a liberdade de expressão, de informação, de comunicação e de opinião:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - à inviolabilidade da intimidade, da honra e da imagem;

> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Segundo Oliveira e Novais (2021), esses direitos fundamentais formam a base jurídica e moral para a regulamentação do tratamento de dados pessoais no Brasil, reforçando a necessidade de garantir o controle individual sobre as informações compartilhadas.

Com base no exposto e nos argumentos trazidos por Frazão *et. al* (2019), a LGPD busca regular todas as formas de tratamento de dados pessoais. Ainda nesse sentido, a autora discorre sobre o fato de a Lei servir também como um agente capaz de transformar as técnicas utilizadas pelo capitalismo de vigilância, a fim de conter a extensa extração de dados que ocorrem diariamente sem ao menos os indivíduos se darem conta; e com isso as diversas aplicações e utilizações indevidas que a podem vir a acontecer sem o conhecimento e o consentimento dos usuários.

De acordo com o art. 6º da LGPD, as atividades de tratamento de dados pessoais deverão observar a boa-fé e uma série de princípios, dentre eles destacam-se:

> 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;.

De acordo com a Declaração Universal dos Direitos Humanos, em seu art. 8º “Toda pessoa tem direito a buscar assistência legal caso seus direitos sejam violados”, isso se conecta à LGPD quando os indivíduos confiam em determinadas empresas e têm seus dados usados, e em piores situações, vazados.

Dessa forma, a LGPD não apenas determina princípios e direitos fundamentais, mas também impõe exigências técnicas e organizacionais que viabilizam uma governança eficaz da segurança da informação, prevenindo incidentes como vazamentos e acessos indevidos.

2.2 EVOLUÇÃO DA LGPD NO CONTEXTO ATUAL BRASILEIRO

Muito se discute a respeito da necessidade de uma legislação específica para proteção de dados no Brasil, essas discussões tiveram início em meados de 2010, quando o Ministério da Justiça promoveu uma consulta pública sobre direitos digitais e regulação da internet. Impulsionado pelo crescente uso da internet e das redes sociais, que eram novidade até então, esse movimento evidenciou o despreparo de normas claras para o tratamento de informações pessoais.

Desde então, começaram a se intensificar os debates acadêmicos, técnicos e jurídicos, que tiveram forte embasamento e influência internacional, principalmente acerca do Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), que viria a servir como um estímulo para a elaboração da legislação brasileira (Brasil, 2018).

Quando foi sancionado em 2014, o Marco Civil (Lei nº 12.965/2014), se tornou mais que uma lei, mas sim um grande primeiro passo para a regulamentação dos direitos fundamentais no ambiente digital que se fazia tão necessária para o país. O Marco determinou princípios importantes como privacidade, segurança e proteção de dados, bem como reforçar a

responsabilidade dos agentes que tratam essas informações. Com a promulgação desta norma, sinalizou-se o compromisso do Estado brasileiro com uma internet livre, mas responsável, segura e com garantia de direitos (Brasil, 2014).

Por volta de 14 de agosto de 2018, mediante amadurecimento das discussões, ocorreu a sanção da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais que viria a ser popularmente conhecida como LGPD. No âmbito do ordenamento jurídico nacional, essa legislação se tornou outro marco importante, por estabelecer normas claras sobre a coleta, uso e o armazenamento e compartilhamento de dados pessoais, seja por entidades públicas ou privadas.

As definições fundamentais como dado pessoal, dado sensível e tratamento de dados que a LGPD trouxe, tornou mais consolidado os direitos dos titulares, os deveres dos controladores e operadores, e as bases legais para o tratamento de informações (Brasil, 2018).

Contudo, para que a LGPD pudesse ser plenamente eficaz, era necessária a criação de um órgão fiscalizador. Nesse contexto, foi editada a Medida Provisória nº 869/2018, posteriormente convertida na Lei nº 13.853/2019, que instituiu a Autoridade Nacional de Proteção de Dados (ANPD).

Dessa forma, a ANPD tornou-se responsável por zelar pela correta aplicação da LGPD, elaborar diretrizes e regulamentos complementares, além de fiscalizar e aplicar sanções em casos de descumprimento da legislação. A criação da ANPD é considerada essencial para garantir a efetividade da proteção de dados no país (Brasil, 2019).

Além disso, a ANPD possui competências amplas que incluem não apenas a fiscalização, mas também a promoção de estudos sobre proteção de dados, a celebração de acordos de cooperação com órgãos nacionais e internacionais, e a realização de consultas públicas para aprimoramento da regulamentação; o órgão tem o poder de aplicar sanções administrativas que variam desde advertências até multas de até 2% do faturamento bruto da empresa no Brasil, limitadas a R$ 50 milhões por infração. A mesma também pode determinar a suspensão parcial ou total do tratamento de dados e até mesmo a eliminação dos dados pessoais objeto da infração.

A ANPD mantém canais de comunicação direta com os cidadãos através de ouvidoria e sistema de denúncias online, permitindo que os titulares de dados

reportem possíveis violações à LGPD, essa estrutura multifacetada demonstra a complexidade das suas atribuições e sua importância como guardiã dos direitos fundamentais de proteção de dados no Brasil.

Por outro lado, a LGPD, ainda que aprovada em 2018, teve sua entrada em vigor postergada, sendo implementada em 18 de setembro de 2020, conforme a Lei nº 14.058/2020. A situação do país naquele momento era crítica, em virtude da pandemia de COVID-19, o que gerou tentativas de novo adiamento.

No entanto, o legislador optou por manter a data original de vigência, pois foi considerada a relevância do tema no contexto da crescente digitalização; ainda mais em um momento que as pessoas estavam em casa, tendo que trabalhar e reorganizar suas rotinas. Após esse marco, empresas e instituições públicas passaram a ser legalmente obrigadas a adequar seus sistemas e políticas ao novo regime jurídico de proteção de dados (Brasil, 2020).

A partir de 1º de agosto de 2021, as sanções administrativas previstas na LGPD começaram a ser aplicadas. Enquanto isso, a ANPD, já parcialmente estruturada, passou a atuar de maneira mais efetiva, no que diz respeito à monitoração do cumprimento da legislação e o início dos processos de fiscalização. Foi a aplicação das sanções que marcou de fato o início da efetiva responsabilização dos agentes de tratamento, reforçando a necessidade de conformidade legal e a proteção dos direitos dos titulares (ANPD, 2021).

Por fim, a estruturação da ANPD foi consolidada em 2022, quando o órgão passou a integrar a Presidência da República com autonomia técnica. Nesse mesmo período, a Emenda Constitucional nº 115/2022 foi promulgada, incluindo a proteção de dados pessoais como direito fundamental no artigo 5º da Constituição Federal.

Desde então, a ANPD tem atuado na produção de normativas complementares e na promoção de campanhas educativas. A consolidação da LGPD reflete o avanço do Brasil na construção de uma cultura de privacidade e segurança da informação, alinhada às melhores práticas internacionais (Brasil, 2022).

2.2.1 QUESTIONAMENTOS E REFLEXÕES SOBRE A APLICABILIDADE DA LGPD NO BRASIL

Outrossim, apesar do evidente avanço normativo representado pela Lei Geral de Proteção de Dados Pessoais (LGPD), é imperioso que se estabeleça uma análise crítica sobre sua efetiva aplicação no contexto brasileiro; uma vez que a mera existência da lei não garante sua eficácia concreta, sobretudo diante de lacunas institucionais e sociais que comprometem seu pleno funcionamento.

Um dos principais pontos de dúvida diz respeito à atuação da Autoridade Nacional de Proteção de Dados (ANPD), que, embora formalmente instituída, ainda opera de maneira limitada. Segundo análise de Gauer (2024), em seu estudo, ele aponta que a ANPD possui uma estrutura ainda frágil, com independência questionável e recursos limitados, o que impede que exerça seu papel fiscalizador da forma robusta como é necessária. Como aponta o autor, “sem autonomia técnica e orçamentária efetiva, a ANPD permanece como uma promessa institucional ainda não cumprida” (GAUER, 2024).

Todavia, outro ponto importante a se questionar é sobre a responsabilidade civil em casos de vazamentos de dados. Ainda que a LGPD disponha sobre reparação de danos, há incertezas práticas a respeito de como essa responsabilização pode se concretizar. Conforme destaca o *blog* do *Escavador* (2022), a lei oferece diretrizes, porém dá espaço para diferentes interpretações sobre características como nexo de causalidade, a comprovação de dano e a culpa ou dolo dos controladores e operadores. Fato é, uma brecha assim não seria suficiente para criar insegurança tanto para os titulares dos dados quanto para as empresas?

Além disso, é necessário observar e levar em consideração os desafios que empresas brasileiras enfrentam para se adaptar à LGPD. Quando se trata das micro, pequenas e médias empresas (MPMEs), essa adaptação nem sempre é viável financeiramente. Conforme exposto no artigo de Ramos (2020), a LGPD já nasceu cercada de incertezas, e uma das críticas recorrentes é que ela “pode sufocar a inovação entre as *startups* e onerar, de forma desproporcional, as empresas de menor porte”. Diante disso, não é a ausência de diretrizes mais flexíveis para esse público que acaba criando um abismo entre o ideal normativo e a realidade prática?

Ainda segundo o autor, seu texto também expõe que, embora a lei tenha uma função pedagógica e pretenda criar uma cultura de proteção de dados no país, ela ainda não foi plenamente compreendida e assimilada, nem pela

sociedade civil, nem pelas organizações públicas e privadas. Portanto, essas mesmas divergências e incertezas geram um ambiente onde a lei é mais temida do que compreendida, o que consequentemente dificulta a criação de políticas internas nas empresas e corporações que sejam eficazes e alinhadas com seus princípios.

2.3 VULNERABILIDADES DA SEGURANÇA DA INFORMAÇÃO EM AMBIENTES CORPORATIVOS

De acordo com Mello (2020), o Direito à Privacidade não é o único direito envolvido na relação entre empresas e colaboradores, e principalmente para com seus usuários. O autor enfatiza também que, ainda que exista garantia de privacidade na vida real, a “intimidade” virtual também é resguardada pela legislação.

As vulnerabilidades da segurança da informação em ambientes corporativos são ressaltadas na cartilha da Fecomércio MG (2021) como pontos críticos que exigem atenção contínua. A falta de políticas internas claras de proteção de dados é uma das principais fragilidades identificadas, o que gera insegurança para os colaboradores e os clientes. A ausência de normativas internas pode expor a organização a riscos de vazamento de dados, acessos indevidos e responsabilização legal conforme a Lei Geral de Proteção de Dados (LGPD).

De acordo com Magalhães (2020), muitas empresas brasileiras ainda não possuem um planejamento estruturado para lidar com incidentes de segurança, o que as torna suscetíveis a vazamentos e acessos indevidos. A conformidade com a LGPD exige que as organizações adotem medidas proativas, como a criptografia de dados, auditorias regulares e a implementação de um encarregado de proteção de dados (DPO) para monitorar a conformidade com as normas regulatórias.

Nesse sentido, Sydow (2021) observa que “a ausência de uma governança digital clara e efetiva transforma vulnerabilidades técnicas em potenciais violações jurídicas, especialmente diante de um arcabouço normativo como o da LGPD”. O autor destaca que a segurança da informação não pode ser tratada apenas como

uma questão técnica, mas como uma dimensão essencial da responsabilidade corporativa.

Outra vulnerabilidade crítica é a fragilidade das infraestruturas tecnológicas, que muitas vezes operam com sistemas desatualizados e sem mecanismos adequados de defesa. De acordo com estudo de Strack (2024), a ausência de firewalls robustos e sistemas de prevenção contra invasões (IDS/IPS) pode aumentar a exposição das empresas a ameaças como ransomware e ataques de negação de serviço (DDoS). Além disso, a dependência excessiva de soluções terceirizadas sem verificações rigorosas de segurança pode comprometer a integridade dos dados corporativos e dos clientes.

Sydow (2021) reforça que “a terceirização sem critérios de segurança transforma a empresa em corresponsável por incidentes de violação de dados, uma vez que a responsabilidade sobre os dados não se transfere com o serviço, permanecendo com o controlador”. Isso reforça a necessidade de due diligence constante nos contratos com fornecedores e prestadores de serviço que processem dados pessoais.

A engenharia social também se mostra como um fator de risco relevante. Muitos ataques bem-sucedidos de hackers e invasores ocorrem devido à manipulação psicológica de funcionários para obtenção de credenciais e acessos privilegiados. Ainda segundo Magalhães (2020), a falta de treinamentos recorrentes em boas práticas de segurança faz com que os próprios colaboradores das empresas se tornem elos fracos na proteção dos dados dos clientes, facilitando ataques de “phishing” (técnica de fraude que visa obter informações pessoais ou financeiras de usuários da internet) e outras fraudes eletrônicas. A mitigação desses riscos exige a implementação de uma cultura organizacional focada na segurança da informação, com treinamentos periódicos e conscientização sobre ameaças digitais.

Segundo Sydow (2021), “a segurança da informação deve ser uma cultura empresarial, e não um conjunto isolado de ferramentas técnicas. A maior ameaça às empresas não é o hacker sofisticado, mas o colaborador despreparado”. Assim, a prevenção é um fator fundamental para mitigar riscos operacionais e

legais no tratamento de dados pessoais.

Com base no exposto do capítulo anterior deste estudo, os princípios fundamentais da LGPD representam os pilares sobre os quais a proteção da privacidade e a gestão responsável de dados pessoais no Brasil são construídos. De acordo com a JRQ Master (2022), a aplicação da LGPD nas empresas exige mudanças estruturais nos processos internos para garantir a proteção de dados pessoais, uma vez que os ambientes corporativos, empresas e organizações são guiados por esses princípios para que possam usar as informações pessoais dos usuários de maneira ética e dentro da lei.

Diante disso, destacam-se os princípios da "Finalidade", que promove a transparência nas práticas de coleta, a "Adequação", que evita a obtenção excessiva de informações e, por último, mas não menos importante, o "Consentimento", garantindo que a coleta seja feita com permissão explícita e informada.

Além disso, no cenário brasileiro atual, a Lei Geral de Proteção de Dados (LGPD) é aplicável para todas as operações de dados, de acordo com estudo de Micheletti et al. (2021), o que está relacionado ao fato de que, no ambiente corporativo, as empresas devem ter medidas firmes para evitar violações de segurança, que podem vir de diversas formas, seja por negligência, imprudência ou até mesmo por má-fé.

Sydow (2021) ressalta, ainda, que a aplicação dos princípios da LGPD exige das organizações um “comprometimento ético com o tratamento de dados pessoais, que vá além da letra fria da lei, abraçando o espírito da proteção da dignidade da pessoa humana”.

No entanto, com base no artigo de Mello (2020), o autor expõe que o direito à privacidade não é o único direito envolvido na relação entre empresas e colaboradores quanto ao monitoramento dos computadores. O autor explica que empresas e corporações têm a propriedade da estação de trabalho, do acesso à Internet e do e-mail corporativo (ex:*seunome@nomedaempresa.com.br*). Por isso, também entende-se que quem oferece os meios para de trabalhar com essas informações, também tem direitos.

A Constituição Federal (1988), em seu art. 5º, inciso XXII, estabelece que é garantido às empresas também, o direito de propriedade:

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

Ademais, nos termos do art. 1.228 do Código Civil, que discorre acerca do direito de propriedade "o proprietário tem a faculdade de usar, gozar e dispor da coisa, e o direito de reavê-la do poder de quem quer que injustamente a possua ou detenha".

Porém isso vai em contrapartida do que também diz o art. 5º em seu inciso X onde se tem que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.”

A luz do cenário atual brasileiro, com a tecnologia estando a frente de grande parte das áreas do mercado de trabalho, a Internet e outros meios eletrônicos de comunicação se tornaram e hoje são imprescindíveis, exímias ferramentas de trabalho, algumas vezes pessoais dos funcionários, outras fornecidas pela própria empresa aos seus funcionários, o que permite maior eficiência na comunicação, bem como otimização das rotinas de trabalho.

Porém, para Mello (2020), quando esta ferramenta é mal utilizada, compromete não apenas a imagem e segurança da empresa como também o desempenho das tarefas, o que corrobora os fatos elencados na cartilha da Fecomércio MG (2021): a ausência de boas práticas internas contribui para o aumento das vulnerabilidades corporativas.

Logo, a gestão da segurança da informação deve ir além da simples instalação de antivírus ou firewalls, exigindo ações estruturadas de governança de dados, políticas internas bem definidas, treinamentos regulares e o monitoramento de condutas, como exposto na cartilha da Fecomércio MG (2021). Nesse sentido, a LGPD obriga os controladores e operadores de dados a adotarem não apenas medidas técnicas, mas também administrativas para

proteger os dados pessoais sob sua responsabilidade.

Outro ponto relevante é a fragilidade humana, considerada uma das maiores fontes de risco. A cartilha da Fecomércio MG (2021) destaca que funcionários não treinados ou mal orientados tendem a cometer falhas como o uso de senhas fracas, o compartilhamento indevido de informações ou o clique em links maliciosos.

Essa dimensão humana da vulnerabilidade exige das empresas investimentos constantes em educação e conscientização sobre segurança digital, incorporando boas práticas no cotidiano corporativo e enfatiza a importância de políticas de privacidade acessíveis, compreensíveis e divulgadas a todos os colaboradores.

Conforme orienta a Cartilha da Fecomércio MG (2021), qualquer organização que colete, armazene ou trate dados pessoais — inclusive nome, CPF, e-mail ou até dados sensíveis — está sujeita às obrigações legais da LGPD. Isso inclui empresas de pequeno porte, comércios locais e prestadores de serviço.

O texto legal não diferencia empresas pelo porte, mas sim pela atividade de tratamento de dados. Por isso, o texto da cartilha alerta para a necessidade de uma atuação proporcional, conforme a realidade de cada empresa, sempre observando os princípios da LGPD, como a finalidade, necessidade, adequação e transparência.

Segundo a Flowti (2024), a adequação à LGPD exige planejamento e envolvimento de todos os setores da empresa, além disso, muitas empresas, especialmente de pequeno e médio porte, não possuem infraestrutura tecnológica adequada para garantir a proteção dos dados pessoais. A falta de sistemas de proteção atualizados, backups seguros e controle de acesso a informações sensíveis torna essas organizações alvos fáceis de ataques cibernéticos.

Um exemplo prático de falha recorrente é o envio de documentos em formato PDF que mantêm metadados rastreáveis, como nome do autor, localização, data de criação, e até versões anteriores do conteúdo. Em muitos casos, esses arquivos são compartilhados com clientes, fornecedores ou até publicados em sites institucionais sem a devida sanitização. Essas informações ocultas podem ser exploradas por cibercriminosos para obtenção de dados sensíveis ou engenharia social, o que configura clara vulnerabilidade à luz da LGPD. Além do

risco técnico, esse tipo de descuido pode acarretar responsabilização legal por exposição indevida de dados pessoais e corporativos, conforme previsto na legislação.

Nesse sentido, a adoção de medidas preventivas, como o mapeamento de dados e a revisão de processos internos, é apontada como essencial para reduzir tais vulnerabilidades e promover a cultura da segurança da informação.

3 DISCUSSÕES ACERCA DA ÉTICA E LEGISLAÇÃO

No contexto jurídico e ético contemporâneo, a proteção de dados pessoais se consolida como uma exigência fundamental da sociedade digital. Esta proteção não pode ser concebida apenas como um conjunto de normas técnicas, mas como um imperativo ético que reflete valores essenciais de respeito à privacidade e à autodeterminação informativa dos indivíduos.

A ética no âmbito da segurança da informação está intrinsecamente relacionada ao compromisso das instituições públicas e privadas em garantir a integridade, confidencialidade e transparência no tratamento dos dados pessoais

A Lei Geral de Proteção de Dados (LGPD) consagra esses princípios e alinha-se aos fundamentos constitucionais da dignidade da pessoa humana, conforme estabelecido pela Emenda Constitucional nº 115/2022, que elevou a proteção de dados pessoais à categoria de direito fundamental (BRASIL, 2022). Entretanto, como observado no capítulo anterior, existe um descompasso entre o avanço normativo representado pela LGPD e sua efetiva implementação no contexto brasileiro, o que suscita importantes reflexões éticas e jurídicas

Segundo Oliveira (2021), em estudo publicado na Revista Brasileira de Ensino e Pesquisa em Administração Pública, a ética da informação deve ser entendida como um conjunto de práticas orientadas pela responsabilidade e pelo dever de não causar danos aos titulares dos dados. Essa perspectiva complementa o aparato normativo da LGPD, pois transcende a mera obrigação legal e alcança uma dimensão moral que deve nortear a conduta das organizações.

Nesse sentido, é preocupante constatar, como aponta Gauer (2024), que a Autoridade Nacional de Proteção de Dados (ANPD) ainda opera com estrutura limitada e recursos insuficientes, comprometendo sua capacidade fiscalizadora e

criando um vácuo institucional que pode fragilizar a efetividade da proteção de dados no Brasil, revelando uma contradição ética: embora o país disponha de uma legislação avançada, carece de mecanismos práticos para sua plena aplicação.

A questão da responsabilidade civil em casos de vazamentos de dados, conforme destacado pelo *blog* do *Escavador* (2022), também evidencia lacunas interpretativas que podem gerar insegurança jurídica tanto para os titulares dos dados quanto para as organizações; a ausência de parâmetros claros compromete a dimensão restaurativa da justiça.

Outro aspecto ético relevante diz respeito às desigualdades no processo de adequação à LGPD. Conforme exposto por Ramos (2020), a lei pode onerar desproporcionalmente as micro, pequenas e médias empresas (MPMEs), que muitas vezes não dispõem de recursos financeiros ou técnicos para implementar as medidas necessárias.

Esta realidade evidencia um dilema ético: como assegurar a proteção de dados sem inviabilizar a atividade econômica de empresas menores? A ausência de diretrizes mais flexíveis ou programas de apoio à adequação para este segmento pode resultar em um cenário de exclusão digital ou, pior, de conformidade meramente formal sem efetiva proteção.

A LGPD exige a observância de princípios como finalidade, necessidade e adequação, os quais possuem não apenas valor jurídico, mas também ético, por evitarem a coleta indiscriminada e abusiva de informações (FRAZÃO et al., 2019). Contudo, a implementação prática desses princípios esbarra em obstáculos culturais e organizacionais. Como evidenciado pela cartilha da Fecomércio MG (2021), muitas empresas brasileiras ainda não possuem políticas internas claras de proteção de dados, o que gera insegurança para colaboradores e clientes.

No plano institucional, embora a criação da ANPD represente um avanço jurídico importante, sua efetividade permanece comprometida pela ausência de independência técnica e orçamentária plena, como destacado por Gauer (2024). Quando coloca-se o cenário brasileiro em contraste com a experiência europeia, onde as autoridades de proteção de dados desfrutam de maior autonomia e poder de aplicação fica ainda mais perceptível a fragilidade institucional da ANPD, o que se torna um desafio ético e jurídico para a consolidação de uma cultura de proteção de dados no Brasil.

Mais adiante, conforme evidencia Strack (2024), a ética corporativa em segurança da informação também exige que as organizações invistam em tecnologias como criptografia, *backups* seguros e mecanismos de monitoramento de acessos, sem desconsiderar o fator humano. O autor destaca que muitos vazamentos de dados ocorrem por falhas humanas, o que exige treinamentos constantes e uma cultura organizacional baseada na proteção de dados. Esta abordagem é corroborada pela cartilha da Fecomércio MG (2021), que enfatiza o papel da ética na construção de políticas internas claras e efetivas.

Na esfera do serviço público, o estudo de Freitas e Lima (2018) ressalta que a ética na gestão de dados sensíveis da população deve observar o princípio da transparência ativa, especialmente em serviços de saúde e assistência social. A coleta de dados sem consentimento ou sem finalidades definidas pode gerar exclusão social, discriminação e violação de direitos. Assim, a responsabilidade ética na administração pública está diretamente ligada à função social dos dados e ao respeito à privacidade do cidadão.

O debate sobre a ética na proteção de dados também se estende às questões de equidade social. Conforme apontam pesquisadores da Universidade Federal de Santa Catarina (UFSC) (2023), a automação de decisões baseada em dados, como em sistemas de crédito ou seleção de currículos, pode reproduzir preconceitos ou discriminar populações vulneráveis, ferindo tanto a LGPD quanto princípios constitucionais como a igualdade.

Outro ponto de tensão ética reside no equilíbrio entre o direito à privacidade e o direito de propriedade das empresas sobre suas ferramentas de trabalho. Como observa Mello (2020), as empresas possuem legitimidade para monitorar computadores, acessos à internet e e-mails corporativos, com base no direito de propriedade garantido pelo art. 5º, inciso XXII da Constituição Federal e pelo art. 1.228 do Código Civil. Contudo, este monitoramento deve respeitar limites, a fim de não violar o direito à intimidade assegurado pelo art. 5º, inciso X da Constituição. Diante disso, o aparente conflito normativo revela a necessidade de uma interpretação sistemática e ponderada do ordenamento jurídico, orientada por princípios éticos de proporcionalidade e respeito à dignidade humana.

A cultura organizacional também representa um fator decisivo para a efetividade da proteção de dados. Conforme destacado por Magalhães (2020), muitas empresas brasileiras ainda não possuem um planejamento estruturado

para lidar com incidentes de segurança, o que as torna suscetíveis a vazamentos e acessos indevidos.

Ademais, como apontado por Ramos (2020), a LGPD ainda não foi plenamente compreendida pela sociedade e pelas organizações. Esta percepção negativa dificulta a criação de uma cultura de proteção de dados baseada em valores éticos compartilhados, em vez de mero cumprimento formal de obrigações legais por temor de sanções.

No contexto das tecnologias emergentes, como a inteligência artificial e o *big data*, os desafios éticos tornam-se ainda mais complexos. A LGPD, embora abrangente, não contempla especificidades dessas tecnologias, o que pode gerar lacunas normativas em áreas como decisões automatizadas, perfilamento e inferência de dados sensíveis a partir de dados aparentemente neutros.

A ética e a legislação devem caminhar juntas para consolidar um ambiente digital mais seguro, justo e transparente. A construção de uma verdadeira cultura de proteção de dados no Brasil requer, assim, não apenas o aprimoramento dos mecanismos institucionais de fiscalização e aplicação da lei, mas também um esforço educacional e cultural para disseminar valores éticos relacionados à privacidade e à segurança da informação.

Portanto, feito isso, será possível superar o abismo entre a teoria e a prática, mencionado por Micheletti et al. (2021), e assegurar que a proteção de dados seja compreendida não como uma mera exigência legal, mas como um imperativo ético que assegura a confiança, a cidadania digital e os direitos fundamentais no século XXI.

4 CONSIDERAÇÕES FINAIS

O presente estudo evidenciou que a segurança da informação e a proteção de dados pessoais constituem pilares fundamentais para o cumprimento efetivo da Lei Geral de Proteção de Dados no Brasil. A análise das tecnologias e práticas de proteção revelou que, para além da conformidade legal, é essencial o desenvolvimento de uma cultura organizacional baseada na valorização da privacidade.

Constatou-se que as tecnologias de proteção de dados, como criptografia, anonimização e sistemas DLP (*Data Loss Prevention*), são ferramentas

necessárias, porém insuficientes quando dissociadas de políticas internas bem estruturadas e do engajamento dos colaboradores. As vulnerabilidades identificadas em ambientes corporativos brasileiros demonstram que o fator humano permanece como elemento crítico na cadeia de segurança da informação.

No âmbito jurídico, verificou-se que a LGPD estabeleceu um novo paradigma para o tratamento de dados pessoais no Brasil, harmonizando-se com tendências internacionais de proteção à privacidade. Contudo, a plena efetividade da legislação ainda enfrenta desafios estruturais, como a consolidação da ANPD como órgão fiscalizador independente e a necessidade de parâmetros mais claros sobre responsabilidade civil em casos de violações, que combine aspectos técnicos, organizacionais e jurídicos

Por fim, entende-se que o alinhamento entre segurança da informação e exigências legais da LGPD não representa apenas uma obrigação normativa, mas uma vantagem competitiva para organizações que buscam construir relações de confiança em um contexto onde dados pessoais são ativos cada vez mais valiosos. O investimento em proteção de dados transcende, portanto, a simples adequação legal, configurando-se como estratégia essencial de sustentabilidade e responsabilidade corporativa no cenário digital brasileiro.

REFERÊNCIAS

ANPD – Autoridade Nacional de Proteção de Dados. Portal institucional. Disponível em: https://www.gov.br/anpd Acesso em: 14 abr. 2025.

BRASIL. Código Civil. **Lei nº 10.406, de 10 de janeiro de 2002.** Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, p. 1, 11 jan. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm . Acesso em: 9 abr. 2025.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988.** Diário Oficial da União, Brasília, DF, 5 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm . Acesso em: 9 abr. 2025.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022.** Altera a Constituição Federal para incluir a proteção de dados pessoais como direito fundamental. Disponível em:

https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm . Acesso em: 15 abr. 2025.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Marco Civil da Internet. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 15 abr. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br Acesso em: 31 mar. 2025.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019.** Altera a LGPD e cria a Autoridade Nacional de Proteção de Dados (ANPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13853.htm Acesso em: 12 abr. 2025.

BRASIL. **Lei nº 14.058, de 17 de setembro de 2020.** Dispõe sobre a entrada em vigor da LGPD. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14058.htm . Acesso em: 12 abr. 2025.

DONEDA, D. **Proteção de dados pessoais:** a função e os limites do consentimento. São Paulo: Atlas, 2020.

ESCAVADOR. **Entenda as discussões relativas à responsabilidade civil na LGPD.** Escavador Blog, 2022. Disponível em: https://blog.escavador.com/entenda-as-discussoes-relativas-a-responsabilidade-civil-na-lgpd. Acesso em: 07 maio 2025.

FECOMÉRCIO MG. **Cartilha LGPD:** boas práticas de proteção de dados pessoais nas empresas. Belo Horizonte: Fecomércio MG, 2021. Disponível em: https://www.fecomerciomg.org.br/wp-content/uploads/2021/05/Cartilha-LGPD.pdf. Acesso em: 14 abr. 2025.

FLOWTI. **LGPD na prática:** o que a sua empresa precisa saber. [S. l.]: Flowti, 2024. Disponível em: https://flowti.com.br/blog/lgpd-na-pratica-o-que-a-sua-empresa-precisa-saber. Acesso em: 14 abr. 2025.

FRAZÃO, Ana; OLIVA, Milena Donato; TEPEDINO, Gustavo. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro.** Thomson Reuters Brasil, 2019.

FREITAS, Carolina Souza; LIMA, Everson. **A privacidade do dado como condição de dignidade humana.** In: 15 Conferência Nacional de Saúde. 2018. Disponível em: http://conferencia2018.redeunida.org.br/ocs2/index.php/15CRU/15CRU/paper/view/16139 Acesso em: 19 abr. 2025.

GAUER, Marcelo. **Com a ANPD só no papel, como fica a aplicação da LGPD no Brasil?** Sindiregis, 2024. Disponível em: https://sindiregis.com.br/artigo-com-a-anpd-so-no-papel-como-fica-a-aplicacao-da-lgpd-no-brasil/. Acesso em: 07

maio 2025.

JRQ MASTER. **LGPD no ambiente corporativo.** 2022. Disponível em: https://www.jrqmaster.com.br/lgpd-no-ambiente-corporativo/. Acesso em: 9 abr. 2025

LEFOSSE Advogados. **A evolução da Lei LGPD.** Disponível em: https://lefosse.com/noticias/a-evolucao-da-lei-lgpd/ . Acesso em: 15 abr. 2025.

MAGALHÃES, Filipa Matias; PEREIRA, Maria Leitão. **Regulamento Geral de Proteção de Dados:** manual prático. 3 Edição Revista e Ampliada. Vida Econômica Editorial, 2020.

MELLO, Rafael. **Segurança da informação e monitoramento corporativo em tempos de LGPD.** Jusbrasil, 2020. Disponível em: https://www.jusbrasil.com.br/artigos/seguranca-da-informacao-e-monitoramento-corporativo-em-tempos-de-lgpd/865706666. Acesso em: 9 abr. 2025.
MENEGHINI, José Ricardo da Silva. **Ética e LGPD no uso de dados em serviços públicos:** desafios e caminhos. Repositório UFSC, 2023. Disponível em: https://repositorio.ufsc.br/handle/123456789/243525 Acesso em: 20 abr. 2025.

MICHELETTI, Miquéias. **Lei Geral de Proteção de Dados:** O abismo entre a teoria e a prática. Disponível em: https://cdljundiai.com.br/wp-content/uploads/2021/09/LGPD-O-ABISMO-ENTRE-A-TEORIA-E-A-PRATICA_202102231600.pdf Acesso em: 6 abr. 2025.

OLIVEIRA, Larissa de Jesus; NOVAIS, Thyara Gonçalves. **Lei Geral de Proteção de Dados Pessoais:** responsabilidade civil no vazamento de informações. Revista de Direito Civil Contemporâneo, v. 31, p. 27–49, 2021. Disponível em: https://repositorio.ufsc.br/handle/123456789/243525. Acesso em: 5 maio 2025.

OLIVEIRA, Thiago Nogueira de. **A ética no uso de dados pessoais e a LGPD:** entre o dever jurídico e o imperativo moral. Revista Brasileira de Ensino e Pesquisa em Administração Pública, v. 7, n. 1, 2021. Disponível em: https://pos.direito.ufmg.br/rbep/index.php/rbep/article/view/894 Acesso em: 19 abr. 2025.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Declaração Universal dos Direitos Humanos**, 1949. Disponível em: Declaração Universal dos Direitos Humanos: como surgiu e o que propõe? - Desinstitute. Acesso em: 19 abri. 2025.

RAMOS, Pedro Henrique. **O otimismo com a LGPD pode ser ilusório:** entenda por que a nova lei de proteção de dados já começa cercada de incertezas. Projeto Draft, 16 set. 2020. Disponível em: https://www.projetodraft.com/por-que-a-lgpd-ja-comeca-cercada-de-incertezas/. Acesso em: 07 maio 2025.

SCHNEIER, B. **Data and Goliath:** The Hidden Battles to Collect Your Data and

Control Your World. New York: W.W. Norton & Company, 2017.

SRNICEK, Nick. **Platform capitalism.** Cambridge: Polity Press, 2018. p. 39.

STRACK, Anderson Antônio. **Segurança da informação:** estudo de caso sobre a adequação à LGPD em uma empresa de tecnologia da informação. 2024. 47 f. Trabalho de Conclusão de Curso (Graduação em Gestão da Tecnologia da Informação) – Universidade Tecnológica Federal do Paraná, Curitiba, 2024.

SYDOW, Spencer Toth. **LGPD:** Lei Geral de Proteção de Dados Pessoais: Lei n.º 13.709/2018 comentada artigo por artigo. 2. ed. São Paulo: Revista dos Tribunais, 2021.

TRIBUNAL DE CONTAS DO ESTADO DE SÃO PAULO. **Passos mínimos para adequação à LGPD pelos Tribunais de Contas.** São Paulo: TCE/SP, 2022. Disponível em: https://www.tce.sp.gov.br/sites/default/files/portal/Passos%20mínimos%20para%20adequação%20à%20LGPD%20pelos%20TCs.pdf Acesso em: 20 abr. 2025.

VIOLA, M. Segurança da informação e desafios empresariais na era digital. **Revista Brasileira de Direito Digital**, v. 5, n. 2, p. 45-67, 2019.