152. BOAS PRÁTICAS DA PROTEÇÃO DE DADOS NO ÂMBITO EMPRESARIAL

Mayume Caires Moreira
Mestra, Unicesumar.
Maringá – Paraná – Brasil
https://orcid.org/0000-0002-1333-1891
http://lattes.cnpq.br/7810923422029283
mayume.moreira@unicesumar.edu.br

Caetano Henrique Junqueira
Acadêmico - Unicesumar
Maringá – Paraná - Brasil
https://orcid.org/0009-0008-8913-6575
https://lattes.cnpq.br/9931666313904622
caetanofurlaneto@gmail.com

Matheus Dias Lopes Mantovani
Acadêmico - Unicesumar
Maringá – Paraná - Brasil
https://orcid.org/0009-0006-2297-9055
https://lattes.cnpq.br/6153514485242242
matheusdlm05@gmail.com

Rafael Bueno Fernandes Dias
Acadêmico - Unicesumar
Maringá – Paraná - Brasil
https://orcid.org/0009-0000-4268-4509
http://lattes.cnpq.br/8265737897684570
rafaeldiasnoites5@gmail.com

RESUMO

Este artigo tem como base visar o estudo em profundidade com relação ao avanço da tecnologia, suas formas de proteções, utilizações nas empresas, problemas enfrentados por invasões de hackers e afins. Diante desse cenário, surge a seguinte problemática: como as empresas podem se proteger de forma eficaz contra os riscos de vazamento de dados em um ambiente cada vez mais digital e vulnerável a ataques cibernéticos? Mostraremos e fundamentaremos nossos argumentos com base em artigos, doutrinas e na legislação brasileira que trata do assunto. Além disso, analisaremos como o avanço tecnológico desencadeou muitas novas formas de agir e pensar, agilizando processos que antes demoravam meses ou anos e que hoje podem ser realizados em dias ou até horas. Entretanto, nem tudo é positivo: esse avanço também trouxe diversos problemas, como os riscos de vazamento de dados, o que motivou a criação da LGPD (Lei Geral de Proteção de Dados), além do desenvolvimento de programas de segurança digital, visando impedir o acesso de hackers a arquivos confidenciais. Espera-se, ao final deste estudo, identificar as principais fragilidades enfrentadas pelas empresas quanto à segurança da informação e apontar boas práticas e mecanismos jurídicos e tecnológicos que possam mitigar esses riscos no ambiente corporativo. Este estudo tem como objetivo compreender um tema cada vez mais urgente e complexo: a segurança da informação e a proteção de dados no ambiente digital. Diante de um cenário marcado por transformações tecnológicas e ameaças constantes, é fundamental analisar essa questão sob múltiplos olhares —técnico, jurídico, organizacional e social. A pesquisa começa com um levantamento bibliográfico e documental, reunindo obras acadêmicas, relatórios especializados e legislações. Serão examinados casos reais de empresas que enfrentaram ataques cibernéticos, como vazamentos de dados e sequestros por ransomwares, para entender os efeitos práticos dessas violações — desde prejuízos financeiros até danos à reputação. Especial atenção será dada às dificuldades enfrentadas por pequenas e médias empresas para cumprir as exigências da LGPD, bem como ao papel essencial da ANPD na fiscalização e no incentivo à conformidade. A pesquisa também observa práticas de segurança adotadas por organizações, buscando identificar falhas recorrentes e estratégias eficazes, combinando tecnologia e cultura organizacional. O objetivo é mostrar que proteger dados não é apenas uma exigência legal, mas um diferencial competitivo que fortalece a relação de confiança entre empresas, clientes e a sociedade.

PALAVRAS-CHAVE: Cibersegurança. LGPD. Proteção de dados.

ABSTRACT

This article aims to conduct an in-depth study regarding the advancement of technology, its protective measures, applications in companies, and the problems arising from hacker attacks and related threats. In this context, the central research question is: how can companies effectively protect themselves against the risks of data leaks in an increasingly digital environment vulnerable to cyberattacks? Arguments will be supported based on articles, doctrines, and Brazilian legislation addressing the subject. Additionally, the study will analyze how technological advancements have triggered new ways of acting and thinking, accelerating processes that previously took months or years to now be completed in days or even hours. However, not all consequences are positive: this advancement has also brought numerous challenges, such as data leak risks, which motivated the creation of the LGPD (General Data Protection Law), as well as the development of digital security programs aimed at preventing hackers from accessing confidential files. At the end of this study, the goal is to identify the main vulnerabilities faced by companies regarding information security and to highlight best practices and legal and technological mechanisms that can mitigate these risks in the corporate environment. The study seeks to understand an increasingly urgent and complex topic: information security and data protection in the digital environment. In a scenario marked by technological transformations and constant threats, it is essential to analyze this issue from multiple perspectives—technical, legal, organizational, and social. The research begins with a bibliographic and documentary review, gathering academic works, specialized reports, and legislation. Real cases of companies that faced cyberattacks, such as data breaches and ransomware incidents, will be examined to understand the practical effects of these violations—from financial losses to reputational damage. Special attention will be given to the challenges faced by small and medium-sized enterprises in complying with LGPD requirements, as well as the essential role of the ANPD in oversight and promoting compliance. The study also observes security practices adopted by organizations, aiming to identify recurring failures and effective strategies that combine technology and organizational culture. The objective is to demonstrate that data protection is not only a legal requirement but also a competitive advantage that strengthens the trust relationship between companies, clients, and society.

KEYWORDS: Cybersecurity; LGPD; Data Protection.

1 INTRODUÇÃO

Nas últimas décadas, a tecnologia tem avançado em um ritmo impressionante, mudando profundamente a forma como vivemos, nos comunicamos, trabalhamos e nos conectamos com o mundo ao nosso redor. Inovações como a inteligência artificial, a internet das coisas, os avanços em biotecnologia, a computação quântica e a automação industrial vêm moldando uma nova realidade mais dinâmica, mais interligada e, ao mesmo tempo, mais desafiadora, portanto, com alguns assuntos que devem ser olhados com muita cautela, sendo uma delas a segurança virtual.

Essas transformações trouxeram inúmeros benefícios. Hoje, a inteligência artificial já é usada para ajudar médicos a diagnosticar doenças com mais precisão, personalizar experiências online, tornar fábricas mais eficientes e até prever catástrofes naturais com antecedência. A chamada internet das coisas conecta desde eletrodomésticos até cidades inteiras, otimizando recursos e facilitando nossas rotinas. Na biotecnologia, a edição genética – como a técnica CRISPR – abre caminhos para tratar doenças genéticas, melhorar a produção de alimentos e contribuir para a conservação do meio ambiente.

Mas, por mais fascinante que tudo isso pareça, é impossível ignorar as perguntas e preocupações que esse progresso desperta. À medida que máquinas e algoritmos

assumem tarefas que antes eram feitas por pessoas, começamos a nos questionar: como será o futuro do trabalho? já vemos algumas profissões desaparecerem e outras surgirem, exigindo conhecimentos técnicos que nem sempre estão ao alcance de todos. Isso coloca uma pressão enorme sobre escolas, universidades e programas de formação profissional, que precisam se adaptar rapidamente para preparar as pessoas para esse novo cenário.

E as mudanças não param por aí. Elas nos obrigam a refletir sobre temas sensíveis como ética, privacidade, segurança e desigualdade social. Quem realmente se beneficia dessas tecnologias? Quem está ficando para trás? Como garantir que os dados de milhões de pessoas não sejam explorados de forma indevida? E mais: como criar inteligências artificiais justas, que respeitem os direitos humanos e não reproduzam preconceitos?

A privacidade, em especial, tornou-se uma grande preocupação no mundo digital. Com tantos aplicativos, redes sociais e dispositivos conectados, a quantidade de informações pessoais sendo coletadas todos os dias é gigantesca. E muitas vezes, sem que a pessoa sequer perceba. Estamos sendo vigiados de perto, e isso nos leva a refletir sobre os limites do que é aceitável em nome da inovação.

Além disso, não dá para ignorar os impactos da tecnologia no nosso bem-estar. A conexão constante, o uso excessivo de telas e a dependência de redes sociais têm afetado a saúde mental de muita gente. Ansiedade, estresse, sensação de isolamento, tudo isso se intensificou nos últimos anos. Por isso, é urgente pensar não só em como usar a tecnologia, mas como viver bem com ela.

Este texto tem como propósito justamente olhar para esse cenário com atenção, sem exageros, mas também sem ingenuidade. Queremos refletir sobre os avanços mais relevantes do nosso tempo, e demostrar os perigos de não ter segurança em questões de privacidade virtual, tanto no âmbito empresarial, quanto na vida de pessoas em nossa vida rotineira.

2 REFERENCIAL TEÓRICO

Com o avanço acelerado da transformação digital, o uso da internet e de ambientes online se tornou essencial para a realização de atividades empresariais, operacionais e estratégicas. Empresas de todos os portes passaram a depender de sistemas conectados para armazenar dados, gerenciar informações sensíveis e se comunicar com clientes e parceiros, esse fato por si só já impulsiona a relevância do tema proteção de dados uma vez que sua relevância está diretamente correlacionada a Ascensão digital

(Schneier,2023). No entanto, esse cenário também trouxe um aumento significativo nas ameaças digitais, como ataques cibernéticos, vazamentos de dados e invasões de sistemas. Diante desse contexto, discutir mecanismos de proteção de dados se torna não apenas relevante, mas necessário, pois a segurança da informação é hoje um dos pilares para a continuidade e credibilidade das companhias.

A negligência de diversas empresas na implementação de mecanismos eficazes de proteção de dados tem custado caro ao meio corporativo. O relatório Data Breach Report da IBM (2024), evidencia que o custo médio global de uma violação chegou a US$ 4,88 milhões, uma alta de 10% em relação ao ano passado, ou seja, organizações com sistemas deficitários e falta de preparo para lidar com ataques enfrentam custos significativamente mais altos. Esse cenário significa que a escolha de não investir em cibersegurança é um risco estratégico que a empresa está correndo.

Diante disso, é essencial reconhecer que a proteção de dados pessoais deve ser compreendida não apenas como um dever legal, mas como um diferencial competitivo e um elemento de confiança nas relações empresariais (Doneda,2016). Reforçando o papel da segurança da informação como fator crucial na credibilidade das empresas.

Para maximizar a segurança de dados, as empresas devem adotar uma abordagem multifacetada que combine aspectos técnicos e aspectos culturais. A implementação de políticas claras de governança, acesso limitado a informações sensíveis da empresa, aliada ao uso de ferramentas com 2 ou mais backups criptografados, firewalls atualizados, autenticação multifator e monitoramento contínuo, forma a base da proteção técnica. No entanto, a eficácia desses mecanismos depende também de uma cultura organizacional voltada para o meio, o que inclui a capacitação de colaboradores por meio de treinamentos periódicos e campanhas internas de conscientização. Além disso, é indispensável que as companhias se mantenham antenadas a quaisquer mudanças legislativas e regulatórias relacionadas ao tema, ainda mais tendo em vista que o cenário jurídico está em constante evolução, impulsionado pelo avanço tecnológico em ascensão.

O método do criminoso digital, em diversos casos, não visa propriamente o comércio aberto dos dados furtados, mas sim a exploração direta da dependência que a própria companhia tem dessas informações. Por meio de ataques como o ransomwares, os criminosos sequestram dados estratégicos, sensíveis e operacionais, bloqueando o acesso e exigindo pagamentos vultosos para a devolução ou desbloqueio das informações. Essa conduta evidencia que, muitas vezes, o valor econômico dos dados não está em sua

utilidade para terceiros, mas na importância exclusiva que possuem para a vítima, ou seja. O criminoso monetiza em valor econômico os dados ao transformar a urgência e a necessidade da empresa em lucro, utilizando a informação como moeda de troca. Como destaca a seguinte literatura:

> […] As variantes de ransomware operam removendo o acesso do sistema do usuário, seja bloqueando o sistema ou criptografando alguns ou todos os dados e, subsequentemente, exigindo pagamento ou resgate em troca do retorno do acesso ao sistema ou do fornecimento de uma chave de descriptografia para a vítima. (Abarghouei; Bonner; Mcgough, 2019, p. 1).

Além da necessidade de investir em tecnologia, as empresas precisam ter em mente que proteger dados não é só instalar um bom antivírus ou adotar uma ferramenta de backup. A verdadeira proteção de dados começa nas pessoas — na forma como os colaboradores lidam com informações, na clareza dos processos internos e na cultura que a empresa constrói em torno da privacidade.

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº13.709, de 14 de agosto de 2018, tem por objetivo assegurar a proteção dos dados de pessoas físicas, responsabilizando as empresas que não respeitarem suas diretrizes. Em um contexto em que informações particulares são comumente reveladas sem consentimento, a legislação visa assegurar segurança jurídica e respeito pela privacidade. A ação da Autoridade Nacional de Proteção de Dados (ANPD) é fundamental para regularizar, fiscalizar e impor multas e penas, e apesar de a LGPD prever sanções predominantemente civis, a responsabilidade criminal pode ser imputada com base em normas afins, como o Código Penal. A conformidade com a LGPD não é apenas um dever legal, mas um comando ético e estratégico para as organizações empresariais.

3 METODOLOGIA

Este estudo adota uma abordagem qualitativa, com caráter exploratório e descritivo, justamente por tratar de um tema complexo e multifacetado: a segurança da informação e a proteção de dados no ambiente digital. Como o assunto envolve aspectos técnicos, jurídicos, organizacionais e sociais, é necessário analisá-lo com profundidade e a partir de diferentes perspectivas.

A primeira etapa da pesquisa consiste em um levantamento bibliográfico e documental. Foram consultados livros, artigos científicos, relatórios técnicos e documentos

legais que abordam a segurança digital. Entre os materiais de destaque, está o Data Breach Report 2024, produzido pela IBM, que traz dados atualizados sobre os custos das violações de dados ao redor do mundo. Além disso, foram utilizadas contribuições teóricas de autores reconhecidos por suas reflexões sobre privacidade, riscos tecnológicos e regulação de dados. Também serão analisadas legislações pertinentes, com especial atenção à Lei Geral de Proteção de Dados Pessoais (LGPD) e às diretrizes da Autoridade Nacional de Proteção de Dados (ANPD).

A pesquisa será enriquecida com a análise de casos concretos de empresas que sofreram ataques cibernéticos, principalmente aqueles que envolveram o uso de ransomwares e o vazamento de informações sensíveis. O objetivo aqui é observar, na prática, os impactos dessas falhas de segurança, considerando as consequências financeiras, a perda de reputação e os danos operacionais que esses incidentes causam às organizações.

Outro ponto importante será a análise crítica da aplicação da LGPD no contexto corporativo, especialmente entre pequenas e médias empresas, que muitas vezes enfrentam dificuldades para se adaptar à legislação. A atuação da ANPD será avaliada como peça-chave no processo de fiscalização, aplicação de sanções e promoção da conformidade legal.

Ao longo da pesquisa, serão observadas práticas de segurança adotadas por diferentes organizações, com o intuito de identificar padrões, erros frequentes e soluções eficazes. A proposta é reunir boas práticas que combinem o uso de tecnologias — como backups criptografados, autenticação multifator e monitoramento contínuo — com a criação de uma cultura organizacional que valorize a proteção de dados, por meio de treinamentos, campanhas internas e políticas claras.

Por fim, espera-se que o estudo contribua para fortalecer a cultura de proteção de dados no Brasil, mostrando que a segurança da informação não deve ser vista apenas como uma obrigação legal, mas como um diferencial estratégico que reforça a confiança e a credibilidade das empresas diante de seus clientes, parceiros e da sociedade.

4 RESULTADOS ESPERADOS

Espera-se que, ao final deste estudo, seja possível identificar de forma clara e fundamentada as principais fragilidades enfrentadas pelas empresas no que diz respeito à proteção de dados e à segurança da informação no ambiente digital. A análise crítica de

artigos, doutrinas e legislações — em especial a Lei Geral de Proteção de Dados (LGPD) deve fornecer subsídios teóricos e práticos para compreender como os ataques cibernéticos ocorrem, quais são suas motivações e os impactos reais nas operações empresariais e na economia do país, tanto financeiros quanto reputacionais.

Dentre os principais resultados esperados está a elaboração de um panorama atualizado sobre os riscos mais recorrentes associados ao ambiente digital corporativo, como o uso de ransomwares, vazamentos de dados pessoais e a exploração de vulnerabilidades técnicas e humanas nos sistemas empresariais. Além disso, espera-se identificar os erros mais comuns cometidos por empresas em relação à governança de dados, destacando a negligência quanto a treinamentos internos, ausência de políticas de segurança e falhas na adoção de ferramentas de proteção digital.

Outro resultado previsto é a definição de um conjunto de boas práticas que unam tecnologia e cultura organizacional, demonstrando que a eficácia da cibersegurança depende não apenas de investimentos em infraestrutura, mas principalmente da conscientização e capacitação contínua dos colaboradores. Pretende-se reforçar que a segurança da informação deve ser compreendida como um ativo estratégico, e não apenas uma obrigação legal, sendo fundamental para garantir a continuidade do negócio e a confiança dos stakeholders.

No plano jurídico, espera-se demonstrar que a LGPD é um marco regulatório essencial, mas que sua aplicação ainda encontra desafios, tanto na fiscalização quanto na adesão pelas pequenas e médias empresas. A atuação da Autoridade Nacional de Proteção de Dados (ANPD) será analisada como elemento central na aplicação de sanções e estímulo à conformidade, para que não comprometa diretos fundamentais como a honra, privacidade e direito a imagem.

A partir da sistematização dessas informações, pretende-se contribuir para o desenvolvimento de uma cultura de proteção de dados mais sólida no Brasil, bem como fornecer subsídios teóricos e práticos para gestores, profissionais de TI e advogados corporativos. Espera-se ainda que os resultados obtidos sirvam de base para novos estudos que aprofundem o entendimento sobre a integração entre tecnologia, direito e governança empresarial, favorecendo a formulação de políticas públicas e estratégias empresariais mais eficazes no combate às ameaças cibernéticas.

Adicionalmente, pretende-se demonstrar, com base nos dados analisados, que a antecipação de riscos e a implementação preventiva de medidas de segurança são

significativamente mais eficazes e menos custosas do que respostas reativas após incidentes. O estudo espera comprovar que empresas que integram a proteção de dados em sua estratégia de gestão corporativa não apenas reduzem os impactos financeiros de ataques, como também constroem uma imagem de responsabilidade e comprometimento ético diante de seus clientes e parceiros. Isso reforça a ideia de que a proteção de dados não deve ser tratada apenas como um setor técnico, mas como uma responsabilidade transversal. Por fim, espera-se que o trabalho incentive uma mentalidade preventiva e integrada sobre cibersegurança, promovendo a adaptação contínua das empresas frente às inovações tecnológicas e aos novos desafios digitais.

REFERÊNCIAS

Atapour-Abarghouei, S. Bonner and A. S. McGough, Volenti non fit injuria: Ransomware and its Victims, 2019. IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 2019, disponivel em: https://ieeexplore.ieee.org/document/9006298. Acesso em: 04 abr. 2025.

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, ano 155, 15 ago. 2018. Disponível em:. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 8 de maio. 2025

DE OLIVEIRA FORNASIER, Mateus; SPINATO, Tiago Protti; RIBEIRO, Fernanda Lencina. Ransomware e cibersegurança: a informação ameaçada por ataques a dados. Revista Thesis Juris, v. 9, n. 1, p. 208-236, 2020.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 3. ed. São Paulo: Revista dos Tribunais, 2021.

IBM. Data Breach Report. Nova York, 2024. Disponível em: https://www.ibm.com/downloads/documents/br-pt/107a02e94948f4ec. Acesso em: 02 de abr 2024.

LIMA, Victtor Henrique. LGPD: análise dos impactos da implementação em ambientes corporativos: estudo de caso. [S.l.]: [s.n.], 2020.MALDONADO, Laura Braga; SOTERO, Andrea Luiza Escarabelo. APLICABILIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS LEI 13.709/18 — SANÇÕES ADMINISTRATIVAS E CRIMINAIS. Revista Ibero-Americana de Humanidades, Ciências e Educação, [S. l.], v. 7, n. 3, p. 221–229, 2021. DOI: 10.51891/rease. v7i3.771. Disponível em: https://periodicorease.pro.br/rease/article/view/771. Acesso em: 12 maio. 2025.

MELLO, A. P..; MIRAMONTES, G. C. . LGPD: agentes De Tratamento, Resposável E ANPD. Cadernos Jurídicos da Faculdade de Direito de Sorocaba, [S. l.], v. 3, n. 1, p. 73–80, 2022. Disponível em:

https://www.fadi.br/revista/index.php/cadernosjuridicos/article/view/88. Acesso em: 11 maio. 2025.

SCHNEIER, Bruce. Entrevista ao canal Valor Econômico. [Vídeo]. YouTube: Valor Econômico, 2023. 10 min. Disponível em: https://www.youtube.com/watch?v=VDhprrn5vho. Acesso em: 04 abr. 2025.

SCHNEIER, Bruce. A Hacker's Mind: How the Powerful Bend Society's Rules, and How to Bend them Back. 1. ed. New York: W. W. Norton & Company, 2023.