Responsabilidade no tratamento de dados: caminhos para a conformidade com a LGPD no contexto empresarial.

Mario Vítor Lazarone Freitas[1]; 0009-0000-5001-8506
Pedro de Oliveira Carreiro[1]; 0009-0005-4004-8329
Lucimeire Cordeiro da Silva[1]; 0000-0001-8166-9803
Ariadne Yurkin Scandiuzzi [1]; 0009-0003-8002-9355
Salete Leone Ferreira[1]; 0000-0002-0937-4899

1 – UniFOA, Centro Universitário de Volta Redonda, Volta Redonda, RJ.
mariajoselazaronexemplo@gmail.com

Resumo: Este artigo analisa o impacto da Lei Geral de Proteção de Dados (LGPD) no contexto empresarial, destacando as implicações para as práticas de coleta, armazenamento, processamento e compartilhamento de informações pessoais. A pesquisa, de natureza qualitativa, descritiva e documental, fundamenta-se em revisão bibliográfica sobre proteção de dados e conformidade legal, com ênfase nos princípios fundamentais da LGPD, como finalidade, adequação, necessidade, transparência e segurança. Os resultados evidenciam que a legislação impõe às empresas responsabilidades que incluem a nomeação de encarregado de dados, a realização de relatórios de impacto, a adoção de medidas técnicas e administrativas e a promoção de uma cultura organizacional voltada à privacidade. Conclui-se que a LGPD representa um marco regulatório relevante, cuja efetiva implementação exige investimentos em tecnologia, capacitação de profissionais e mudança de postura corporativa. Além do cumprimento legal, a conformidade com a lei contribui para fortalecer a confiança dos consumidores e diferenciar competitivamente as organizações em um mercado cada vez mais sensível à proteção das informações pessoais.

.

Palavras-chave: Lei Geral de Proteção de Dados. LGPD. Empresas. Privacidade. Segurança da informação.

INTRODUÇÃO

A proteção de dados tornou-se um tema central no cenário empresarial contemporâneo, impulsionada pelo avanço tecnológico e pela crescente digitalização dos processos organizacionais. A Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), estabelece diretrizes para o tratamento de dados pessoais, com o objetivo de assegurar direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade humana (BRASIL, 2018). Nesse contexto, compreender seus impactos nas práticas empresariais é essencial para a conformidade legal e a manutenção da confiança do consumidor. Portanto o problema de pesquisa pode ser colocado da seguinte forma: Como as empresas podem adequar seus processos de coleta, armazenamento, processamento e compartilhamento de dados pessoais às exigências da LGPD, garantindo conformidade legal e, ao mesmo tempo, fortalecendo a confiança e a segurança dos consumidores?

Para responder ao problema de pesquisa o objetivo geral será examinar o impacto da LGPD no contexto empresarial, destacando as implicações para as práticas de coleta, armazenamento, processamento e compartilhamento de dados pessoais. Como objetivos específicos, tem-se: (i) analisar tecnologias de armazenamento seguro; (ii) avaliar estratégias de implementação de segurança; e (iii) identificar riscos de vazamentos de dados.

O presente estudo traz a recente Lei Geral de proteção de dados, que atualmente é de extrema importância visto que toda pessoa jurídica e física que trate de dados deve estar em conformidade com a mesma. Desta forma é esperado contribuir com esse tema no sentido de explicar de forma clara o que consta e como pode ser feita seu impacto no âmbito das instituições empresariais.

A Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), entrou em vigor em 2020 com o objetivo de proteger os direitos fundamentais de liberdade e privacidade, regulamentando o tratamento de dados pessoais por pessoas físicas ou jurídicas, tanto no setor público quanto privado (BRASIL, 2018). A norma estabelece princípios como finalidade, adequação, necessidade, livre acesso, transparência,

segurança, prevenção e responsabilização, exigindo das organizações a adoção de medidas técnicas e administrativas adequadas.

Segundo Alves (2006), o profissional com acesso a dados restritos deve zelar pela integridade das informações, identificando vulnerabilidades e registrando acessos. Machado (2004) acrescenta que a linguagem SQL, ao definir privilégios diferenciados para usuários, auxilia na preservação da integridade e na delimitação das responsabilidades. Para Sêmola (2003), risco é a probabilidade de que ameaças explorem vulnerabilidades, comprometendo a confidencialidade, a integridade e a disponibilidade das informações.

Lemos (2001) destaca que a auditoria em sistemas deve garantir que as medidas de proteção planejadas sejam executadas, assegurando sigilo, discrição e conformidade com normas técnicas. A adoção de normas internacionais, como a ABNT NBR ISO/IEC 27002 (BRASIL, 2005), é recomendada para controle de acessos e boas práticas de governança da informação.

A segurança dos bancos de dados, recurso essencial para organizações, deve prevenir acessos não autorizados, modificações ou destruições indevidas (LEMOS, 2001). Para Elmasri e Navathe (2011), essa proteção deve contemplar os princípios de confidencialidade, integridade e disponibilidade, empregando técnicas de criptografia, autenticação e autorização de usuários.

A LGPD atribui responsabilidades aos agentes de tratamento, que incluem os controladores e operadores. Estes devem indicar um encarregado (Data Protection Officer) e implementar medidas técnicas e administrativas que protejam os dados pessoais de acessos não autorizados ou usos indevidos (BRASIL, 2018).

O descumprimento da lei pode gerar sanções que vão desde advertências até multas de até 2% do faturamento (limitadas a R$ 50 milhões por infração), além de bloqueio ou proibição parcial do tratamento de dados. Para a aplicação das penalidades, a Autoridade Nacional de Proteção de Dados (ANPD) considera critérios como gravidade da infração, boa-fé do infrator, reincidência, grau de cooperação e medidas corretivas adotadas (BRASIL, 2018).

O crescimento das tecnologias digitais aumentou a relevância da proteção de dados. No Brasil, a repercussão internacional do uso inadequado de informações em redes sociais, como o caso do Facebook, impulsionou a criação da LGPD (REGINA, 2021).

A legislação assegura aos titulares de dados direitos como acesso, retificação, anonimização e eliminação de informações desnecessárias (BRASIL, 2018). Além disso, define hipóteses legais para o tratamento, incluindo consentimento explícito, cumprimento de obrigação legal, exercício regular de direitos, proteção da vida, tutela da saúde, interesse legítimo e proteção ao crédito.

O artigo 6º da LGPD estabelece que as atividades de tratamento devem observar a boa-fé, além de princípios como finalidade, adequação, necessidade, livre acesso, transparência e responsabilização (BRASIL, 2018).

O princípio da boa-fé é também reconhecido no Código de Defesa do Consumidor, que considera abusivas cláusulas contratuais que coloquem o consumidor em desvantagem exagerada ou contrariem a equidade (BRASIL, 1990). Andrade (2004) reforça que, nas relações eletrônicas, a boa-fé contratual exige que os contratantes busquem a verdadeira intenção das partes, garantindo equilíbrio e transparência nos contratos digitais.

MÉTODOS

Trata-se de uma pesquisa qualitativa, descritiva e documental. A pesquisa bibliográfica contemplou artigos científicos, livros e legislações pertinentes ao tema, com foco em práticas empresariais de conformidade com a LGPD. A pesquisa documental abrangeu documentos legais, como a Lei nº 13.709/2018, regulamentos complementares e relatórios técnicos. A análise consistiu na organização e categorização temática dos conteúdos, possibilitando a interpretação crítica dos resultados.

RESULTADOS E DISCUSSÃO

Os resultados evidenciam que a LGPD impõe às empresas a adoção de políticas claras e medidas efetivas para a proteção de dados pessoais, contemplando desde a coleta até o armazenamento e compartilhamento. Autores como Regina (2021) e Maia (2020) destacam

a obrigatoriedade do Relatório de Impacto à Proteção de Dados, instrumento fundamental para mapear riscos e garantir a conformidade.

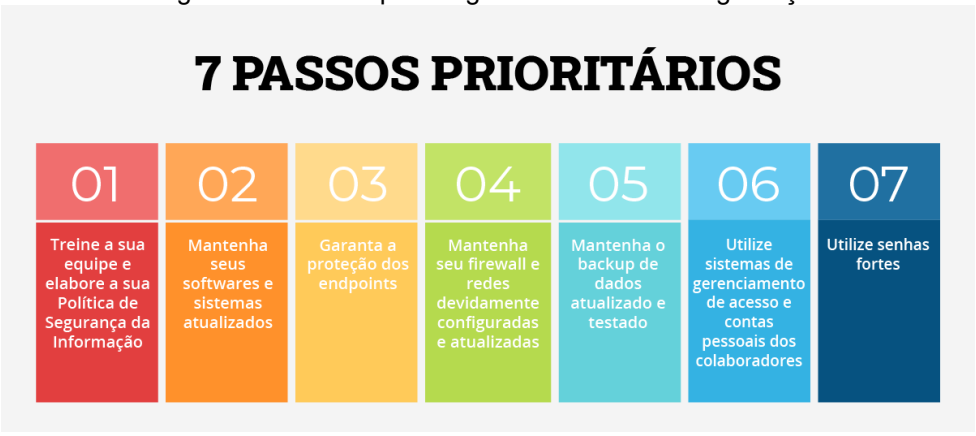
Ezra et al. (2021) ressaltam a importância de tecnologias como VPNs, associadas ao uso de firewalls e sistemas de criptografia, para garantir conexões seguras. No entanto, como defendem Noticebored (2022) e o Government Communications Security Bureau (2017), a tecnologia isolada não é suficiente: a capacitação contínua de colaboradores é indispensável para a prevenção de incidentes.

Martins et al. (2019) enfatizam que os dados podem ser coletados de forma ativa ou passiva, ampliando a necessidade de legislações como a LGPD para assegurar a privacidade. Almeida et al. (2020) reforçam que a conformidade legal exige integração entre infraestrutura, tecnologia e recursos humanos qualificados.

A proteção de dados pessoas devem ser de responsabilidade conjunta entre tecnologia, infraestrutura e recursos humanos qualificados. Não é possível assegurar que dados dos titulares serão tratados de maneira lícita, justa e responsável, conforme exigido pela legislação. Porém, a conformidade com as leis de proteção de dados não é apenas uma questão legal, mas também operacional e estratégica, exigindo a integração das diversas áreas dentro da organização.

Os passos mencionados na figura 1 são fundamentais para proteger os dados pessoais dos clientes e prevenir vazamentos de informações:

Figura 1 - Passos que integram ambiente de segurança.



Fonte: Rotta (disponível no site gepcompliance)

Esses passos integram um ambiente de segurança robusto, com várias camadas de proteção, defendendo de ameaças externas até a conscientização dos funcionários. Ajudando a garantir a conformidade com as leis de proteção de dados.

CONCLUSÕES

O objetivo dessa pesquisa foi examinar o impacto da LGPD no contexto empresarial, destacando as implicações para as práticas de coleta, armazenamento, processamento e compartilhamento de dados pessoais, observou-se que tem um impacto significativo no contexto empresarial. A legislação visa proteger a privacidade dos indivíduos e estabelecer diretrizes claras para o tratamento de dados pessoais pelas empresas. No entanto, sua implementação e conformidade apresentam desafios para as organizações, especialmente as de menor porte, que possuem recursos limitados.

Um dos principais desafios é a criação de uma cultura de proteção de dados, tanto dentro das empresas quanto na sociedade em geral. É necessário sensibilizar os trabalhadores e as partes interessadas sobre a importância da privacidade e segurança dos dados pessoais, promovendo uma mudança de mentalidade e comportamento em relação ao tratamento dessas informações.

Além disso, as empresas enfrentam a necessidade de se adequarem às novas obrigações legais, como a nomeação de um encarregado de proteção de dados, a realização de avaliações de impacto de privacidade e a implementação de medidas técnicas e organizacionais para garantir a segurança dos dados pessoais. Essas adaptações exigem investimentos em recursos humanos, tecnológicos e processuais, o que pode ser um desafio para empresas com recursos limitados.

No entanto, a conformidade com a LGPD não é apenas uma questão de cumprir as obrigações legais, mas também de proteger a reputação e a confiança dos clientes. Violações da lei podem resultar em sanções administrativas, multas e danos à imagem da empresa. Portanto, é fundamental que as organizações compreendam a importância da proteção de dados como um diferencial competitivo e adotem medidas proativas para garantir a conformidade e a segurança das informações pessoais dos usuários.

Conclui-se que a LGPD constitui um marco regulatório essencial para a proteção de dados pessoais no contexto empresarial. Sua efetiva implementação demanda investimentos em tecnologia, treinamento e mudança cultural, especialmente nas organizações de menor porte. Mais do que cumprir exigências legais, a conformidade com a LGPD fortalece a confiança dos consumidores e representa diferencial competitivo. Nesse sentido, a adequação à lei deve ser compreendida como estratégia de governança e sustentabilidade empresarial.

NOTA DE TRANSPARÊNCIA/DECLARAÇÃO DE USO DE IA

Algumas partes deste artigo foram reestruturadas com o auxílio da ferramenta de Inteligência Artificial ChatGPT, utilizada apenas para fins de resumo e adequação ao limite de páginas estabelecido, sob revisão crítica e aprovação dos autores.

REFERÊNCIAS

ALMEIDA, Bethania de Araujo et al. Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. Ciência & Saúde Coletiva, v.25, p.2487-2492, 2020.

ANDRADE, Ronaldo Alves de. Contratos eletrônicos e o princípio da boa-fé. Revista da Faculdade de Direito de Campos, v.5, n.5, p.153-171, 2004.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Senado Federal, 1988.

BRASIL. Código de Defesa do Consumidor: Lei n. 8.078, de 11 de setembro de 1990. Brasília, DF: Presidência da República, 1990.

BRASIL. Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27002: Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação. Rio de Janeiro: ABNT, 2005.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais. Diário Oficial da União, Brasília, DF, 15 ago. 2018.

ELMASRI, R.; NAVATHE, S. B. Sistemas de Banco de Dados. 6. ed. São Paulo: Pearson Addison Wesley, 2011.

EZRA, P. et al. Secured Communication Using Virtual Private Network (VPN). Lecture Notes on Data Engineering and Communications Technologies, p.309-319, 2021.

GEPCOMPLIANCE. Mapa da Governança de Dados – LGPD. Disponível em: https://www.gepcompliance.com/. Acesso em: 2 set. 2025.

GCSB – Government Communications Security Bureau. New Zealand Information Security Manual. 2017. Disponível em: https://www.gcsb.govt.nz/about-us/legislation/. Acesso em: 14 fev. 2023.

GCSB – Government Communications Security Bureau. New Zealand Information Security Manual. 2023. Disponível em: https://nzism.gcsb.govt.nz/ism-document/. Acesso em: 14 fev. 2023.

LEMOS, A. C. Auditoria de sistemas de informação. Rio de Janeiro: Ciência Moderna, 2001.

MACHADO, F. N. Segurança de dados em bancos de dados relacionais. São Paulo: Futura, 2004.

MAIA, Rafael. Lei Geral de Proteção de Dados Comentada. 2. ed. São Paulo: Revista dos Tribunais, 2020.

MARTINS, Marcelo Guerra et al. Big data e a proteção do direito à privacidade no contexto da sociedade da informação. Revista Jurídica Cesumar, v.19, n.3, p.705-725, 2019.

NOTICEBORED. Information Security 101: back to basics. 2022. Disponível em: <https://www.noticebored.com/html/infosec_101.html>. Acesso em: 12 fev. 2023.

REGINA, Luiza. Impactos da Lei Geral de Proteção de Dados (LGPD) no contexto empresarial. Revista de Direito Digital, v.3, n.2, p.45-62, 2021.

SÊMOLA, Marcos. Gestão da segurança da informação: uma visão executiva. Rio de Janeiro: Elsevier, 2003.