LUMEN ET VIRTUS
ISSN: 2177-2789

O PAPEL DO ENCARREGADO DE PROTEÇÃO DE DADOS NA ESTRUTURA CORPORATIVA PÓS LGPD

THE ROLE OF THE DATA PROTECTION OFFICER IN THE POST-LGPD CORPORATE STRUCTURE

EL PAPEL DEL RESPONSABLE DE LA PROTECCIÓN DE DATOS EN LA ESTRUCTURA CORPORATIVA TRAS LA LGPD

https://doi.org/10.56238/levv16n55-060

Data de submissão: 12/11/2025 **Data de publicação:** 12/12/2025

Alan Henrique Mota da Rocha
Graduando em Análise e Desenvolvimento de Sistemas
Instituição: Faculdade de Tecnologia de Taquaritinga - Centro Paula Souza
E-mail: alan.hmr@gmail.com

Robson Eduardo Galloppi
Mestrando em Produção de Conteúdo Multiplataformas
Instituição: Faculdade de Tecnologia de Taquaritinga - Centro Paula Souza
E-mail: robsongalloppi@cooperative.com.br

RESUMO

Este artigo realiza uma análise crítica sobre o papel estratégico do Encarregado de Proteção de Dados (Data Protection Officer DPO) na estrutura organizacional das empresas brasileiras após a promulgação da Lei Geral de Proteção de Dados (LGPD), contextualizando historicamente essa legislação e sua relação com o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), evidenciando a influência de padrões internacionais na formulação da norma nacional. Examina-se o impacto da LGPD na governança corporativa, destacando as reestruturações necessárias para garantir conformidade regulatória, transparência e fortalecimento da confiança dos titulares de dados. O estudo apresenta as atribuições do DPO e sua função de interlocutor entre a empresa, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD), abordando as competências técnicas, jurídicas e interpessoais indispensáveis ao exercício desse cargo. Também são discutidos os desafios da integração desse profissional aos processos estratégicos e operacionais das organizações, além das práticas recomendadas de governança da informação, compliance digital e gestão de riscos, com ênfase na importância da cultura organizacional voltada à ética, segurança e proteção de dados pessoais. Conclui-se que o Encarregado de Dados deve ser compreendido não apenas como exigência legal, mas como agente estratégico essencial para a sustentabilidade corporativa e para a consolidação de ambientes empresariais responsáveis e competitivos em um cenário de crescente valorização da privacidade.

Palavras-chave: LGPD. Encarregado de Dados. Proteção de Dados Pessoais. Governança da Informação. Compliance Digital.

ABSTRACT

This article presents a critical analysis of the strategic role of the Data Protection Officer (DPO) within the organizational structure of Brazilian companies following the enactment of the General Data Protection Law (LGPD). It historically contextualizes the legislation and its relationship with the

European Union's General Data Protection Regulation (GDPR), highlighting the influence of international standards on the formulation of the Brazilian law. The impact of the LGPD on corporate governance is examined, emphasizing the structural adjustments necessary to ensure regulatory compliance, transparency, and the strengthening of data subjects' trust. The study outlines the responsibilities of the DPO and their function as an intermediary between the company, data subjects, and the National Data Protection Authority (ANPD), addressing the technical, legal, and interpersonal competencies essential for performing this role. It also discusses the challenges related to integrating this professional into the strategic and operational processes of organizations, as well as recommended practices in information governance, digital compliance, and risk management, with an emphasis on the importance of an organizational culture focused on ethics, security, and the protection of personal data. It concludes that the DPO should not be understood merely as a legal requirement but as a strategic agent essential for corporate sustainability and for the establishment of responsible and competitive business environments in a context of increasing appreciation of privacy.

Keywords: LGPD. Data Protection Officer. Personal Data Protection. Information Governance. Digital Compliance

RESUMEN

Este artículo realiza un análisis crítico sobre el papel estratégico del responsable de la protección de datos (Data Protection Officer, DPO) en la estructura organizativa de las empresas brasileñas tras la promulgación de la Ley General de Protección de Datos (LGPD), contextualizando históricamente esta legislación y su relación con el Reglamento General de Protección de Datos de la Unión Europea (RGPD), poniendo de manifiesto la influencia de las normas internacionales en la formulación de la norma nacional. Se examina el impacto de la LGPD en la gobernanza corporativa, destacando las reestructuraciones necesarias para garantizar el cumplimiento normativo, la transparencia y el fortalecimiento de la confianza de los titulares de los datos. El estudio presenta las atribuciones del DPO y su función de interlocutor entre la empresa, los titulares de datos y la Autoridad Nacional de Protección de Datos (ANPD), abordando las competencias técnicas, jurídicas e interpersonales indispensables para el ejercicio de este cargo. También se discuten los retos de la integración de este profesional en los procesos estratégicos y operativos de las organizaciones, además de las prácticas recomendadas de gobernanza de la información, cumplimiento digital y gestión de riesgos, con énfasis en la importancia de una cultura organizacional orientada a la ética, la seguridad y la protección de los datos personales. Se concluye que el responsable del tratamiento de datos debe entenderse no solo como un requisito legal, sino como un agente estratégico esencial para la sostenibilidad corporativa y para la consolidación de entornos empresariales responsables y competitivos en un contexto de creciente valoración de la privacidad.

Palabras clave: LGPD. Encarregado de Dados. Proteção de Dados Pessoais. Governança da Informação. Compliance Digital.

1 INTRODUÇÃO

A Lei nº 13.709/2018, publicada em 14 de agosto de 2018, representa marco fundamental no processo legislativo brasileiro voltado ao reconhecimento e à proteção de dados pessoais, ao estabelecer um novo modelo normativo de tratamento, uso e segurança das informações pessoais no país, inspirado diretamente no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia. Embora promulgada em 2018, a LGPD passou, inicialmente, por um período de vacância para adequação técnica e institucional, entrando formalmente em vigor em setembro de 2020, quando suas disposições legais começaram a produzir efeitos obrigatórios. Posteriormente, a partir de agosto de 2022, iniciou-se a efetiva aplicação das sanções administrativas pela Autoridade Nacional de Proteção de Dados (ANPD), consolidando a plena operacionalização da lei e o início do regime sancionatório para as empresas e organizações, públicas e privadas, que realizam operações de tratamento de dados pessoais, como coleta, armazenamento, compartilhamento ou processamento.

Além do estabelecimento de padrões técnicos, a LGPD consolida um novo modelo de governança da informação, no qual a proteção da privacidade é reconhecida como direito fundamental e elemento estratégico para as empresas em um mercado cada vez mais competitivo, orientado pela credibilidade e pela sustentabilidade impulsionada por dados. Nesse contexto, destaca-se o papel do Encarregado de Proteção de Dados (Data Protection Officer – DPO), previsto no artigo 41 da Lei nº 13.709/2018, que determina: *"O controlador deverá indicar encarregado para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)"* (BRASIL, 2018). Assim, o DPO assume a função essencial de ponte institucional entre os titulares de dados, os agentes de tratamento e a ANPD, contribuindo para a efetiva implementação dos princípios de transparência, responsabilidade e segurança no tratamento de dados pessoais, conforme preconizado pela legislação.

Seu papel é muito mais do que garantir conformidade — eles se tornam um elemento estratégico dentro da organização, fornecendo informações sobre técnicas de gestão de risco, políticas de segurança de dados, treinamento interno e aconselhando a alta administração sobre questões voltadas à privacidade de dados. Consequentemente, o DPO é uma figura-chave na construção gradual de uma cultura organizacional ética e responsável em relação ao uso de dados pessoais. Nesse sentido, o objetivo deste trabalho é compreender criticamente as funções desempenhadas pelos DPOs nas empresas brasileiras, focando em suas obrigações legais, relevância estratégica e competências necessárias para alcançar uma conformidade efetiva com a LGPD.

Este estudo é relevante não apenas na medida em que garante a conformidade com leis e regulamentos, mas também porque ajuda os brasileiros a avançar na governança da informação, promovendo um ambiente de confiança entre empresas/agências e titulares (pessoas associadas aos dados), aproveitando práticas que promovam o respeito à privacidade e autodeterminação

informacional como estimuladores ou condicionadores do crescimento econômico e desenvolvimento social.

2 A LEI GERAL DE PROTEÇÃO DE DADOS: FUNDAMENTOS E PRINCIPIOS

A Lei nº 13.709/2018 elevou a proteção de dados pessoais ao patamar de direito fundamental, vinculando-a aos valores constitucionais da dignidade da pessoa humana, do livre desenvolvimento da personalidade e da cidadania. A partir dessa perspectiva, a LGPD não apenas resguarda a privacidade e a autodeterminação informacional, mas também busca harmonizar esses direitos com a liberdade econômica, a inovação e os legítimos interesses das atividades empresariais, garantindo segurança jurídica, previsibilidade e responsabilidade no tratamento de dados.

Nesse cenário, a legislação determina que o uso de dados pessoais deve ocorrer de forma ética e transparente, observando princípios que orientam a conduta das organizações, como a finalidade específica, a adequação entre o tratamento e o contexto em que os dados foram coletados, a limitação ao necessário, bem como a segurança, a prevenção de danos e a responsabilização. Esses princípios, previstos no artigo 6º da LGPD, funcionam como diretrizes obrigatórias para que o tratamento de dados ocorra em conformidade com a boa-fé e com os direitos dos titulares (BRASIL, 2018).

A LGPD passou a tratar a privacidade como um direito autônomo, dotado de dimensão coletiva e intrinsecamente conectado à proteção de dados pessoais e ao livre desenvolvimento da personalidade, superando a visão meramente individual e patrimonial desse direito. Além disso, observa-se que a construção normativa brasileira recebeu forte influência do modelo europeu, especialmente ao incorporar o dever de conformidade preventiva e a adoção de práticas proativas por parte das organizações, reforçando a responsabilidade no tratamento de dados e a mudança cultural necessária à proteção efetiva dos titulares (DONEDA, 2021; BIONI, 2020).

Nesse contexto, a LGPD não deve ser compreendida apenas como um mecanismo restritivo às atividades empresariais, mas também como um instrumento capaz de impulsionar a inovação, fortalecer a competitividade e criar um ambiente econômico mais seguro e equilibrado. Sob essa perspectiva, destaca-se que a legislação contribui para a consolidação da segurança jurídica e posiciona o Brasil em alinhamento com os padrões internacionais mais avançados, beneficiando tanto os consumidores quanto o desenvolvimento de um cenário favorável aos negócios (PECK, 2021).

3 INFLUÊNCIAS DO GDPR NA LGPD

O Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, em vigor desde 2018, consolidou-se como a principal referência legal global e teve impacto direto na LGPD do Brasil. Seu escopo extraterritorial demonstrou um novo paradigma de governança informacional: a União Europeia (UE) passou a regular entidades que processam dados de residentes europeus globalmente.

Aspectos da LGPD, como princípios, bases legais e DPO, foram influenciados pelo modelo europeu. Nessa direção, (BIONI, 2020) destaca que tal aproximação não se limitou apenas a questões jurídicas, mas também objetivou inserir o Brasil em um cenário global mais competitivo, favorecendo a integração econômica e tecnológica com mercados internacionais.

Direitos de titulares de dados, a necessidade de bases legais lícitas, responsabilidade e avaliações de impacto são apenas algumas áreas onde existe consenso junto ao estabelecimento do DPO. Conforme destaca Doneda (2021), a elaboração da LGPD não representou mera transposição do GDPR, mas sim um processo de adaptação normativa que considerou as necessidades e características do contexto brasileiro, preservando a proteção de direitos fundamentais sem inviabilizar a inovação e o desenvolvimento econômico. (MONTEIRO & OLIVEIRA, 2020) argumentam que a proximidade com o modelo europeu trouxe maior segurança jurídica nas transações internacionais.

No entanto, existem grandes distinções: o GDPR possui multas de até 4% do faturamento global total, enquanto a LGPD possui penalidades mais leves e a ANPD ainda está se consolidando, ao contrário das autoridades europeias que já foram criadas. De fato, como enfatiza (PECK, 2021), o efeito do GDPR foi determinante para a LGPD e posicionou o Brasil em um ecossistema internacional de proteção de dados, promovendo a confiança em seu mercado digital.

4 O ENCARREGADO DE DADOS: ATRIBUIÇÕES E RESPONSABILIDADES

O artigo 41 da Lei nº 13.709/2018 fortalece a estrutura de governança em proteção de dados ao exigir que o controlador designe um encarregado pelo tratamento de dados pessoais, conhecido como Data Protection Officer (DPO). Esse profissional exerce papel estratégico por atuar como canal de interlocução entre os titulares, o controlador e a Autoridade Nacional de Proteção de Dados (ANPD), devendo ter sua identidade e meios de contato amplamente divulgados. Entre suas atribuições, estão o recebimento de reclamações e comunicações dos titulares, a orientação interna quanto às práticas adequadas de proteção de dados e a adoção de providências diante de solicitações da ANPD. A legislação também autoriza que a própria autoridade reguladora defina normas complementares e até mesmo estabeleça hipóteses de dispensa de indicação do encarregado. Dessa forma, a previsão legal contribui para consolidar o DPO como agente institucional fundamental, promovendo transparência, conformidade normativa e responsabilidade organizacional no tratamento de dados pessoais (BRASIL, 2018).

A LGPD determina que o DPO seja responsável por, entre outras coisas: receber reclamações e comunicações de titulares de dados; esclarecer dúvidas quando necessário; tomar medidas visando orientar os empregados e contratados do controlador sobre boas práticas de proteção de dados pessoais (BRASIL, 2018) e qualquer outro ato estabelecido pelas regras complementares da ANPD ou acordado pelo controlador.

O DPO deve ser concebido como um agente de governança, encarregado de garantir que a organização não apenas cumpra a lei vigente, mas também desenvolva uma cultura de proteção de dados incorporada em todos os processos (BIONI, 2020). Nesse sentido, o DPO não se limita a atender solicitações isoladas, mas desempenha um papel ativo na implementação de mecanismos contínuos de monitoramento, avaliação e melhoria dos processos de tratamento de dados pessoais, garantindo alinhamento permanente com os princípios da LGPD e com as boas práticas de governança da informação.

Segundo (PECK, 2021), ela enfatiza que o DPO deve ter autonomia e independência para sua funcionalidade, embora possa estar hierarquicamente subordinado a alguma parte da empresa. Isso porque eles são eficazes apenas na medida em que são capazes de monitorar os processos internos e comunicar-se com a alta administração sem grandes obstáculos. Portanto, a confiança e a legitimidade do DPO dependem exclusivamente da sua independência.

Em termos práticos, o DPO desempenha um papel híbrido:

- Operacionalmente: supervisionando fluxos de dados e utilizando avaliações de impacto, educando equipes;
- Estrategicamente: inserindo a proteção de dados no planejamento da organização e auxiliando a tomada de decisões com base em fundamentos éticos e legais (CAVALCANTI, 2022).

Para (MONTEIRO & OLIVEIRA, 2020) também apontam que o DPO deve se comportar como um elo de confiança entre outros setores da organização como departamentos jurídicos, equipes de gestão de recursos humanos, unidades de serviços de Tecnologia da informação e gestores de conformidade. Essa intermediação é necessária para construir um ambiente cooperativo em torno da responsabilidade compartilhada pela proteção dos dados.

Finalmente, é notado que o DPO não tem um papel puramente burocrático, mas também ético e educacional, a saber: sensibilizar outros na organização para respeitar a privacidade e a autodeterminação informacional como valores sociais. Nesse processo, o Encarregado de Proteção de Dados surge como um ator da mudança institucional que é eficaz não apenas pelas habilidades técnicas e legais, mas também pelas suas capacidades de comunicação, negociação e liderança (DONEDA, 2021).

5 ESTRUTURA CORPORATIVA E ADEQUAÇÃO À LGPD

A adequação à Lei Geral de Proteção de Dados (LGPD) implica mudanças nas empresas brasileiras que superam a mera mudança técnica em modelos e procedimentos de negócios, exigindo uma governança corporativa com proteção de dados. A conformidade não deve ser vista apenas como uma obrigação unilateral, mas também como estratégica para construir confiança entre clientes,

parceiros e investidores e fortalecer a credibilidade das empresas (MONTEIRO & OLIVEIRA, 2020). Isso consiste em observar fluxos e políticas internas, contratos, o envolvimento de várias áreas: legal com conformidade documental, processamento de dados com controles de segurança e monitoramento; conformidade com auditorias e relatórios periódicos, recursos humanos para treinamento e despertar.

Dessa forma, (BIONI, 2020) enfatiza que a governança de dados não funciona se não for feita de forma coletiva, transcendendo as regras internas e alcançando a cultura organizacional. Outro eixo crucial é a implementação de programas de governança de privacidade com base no que a Autoridade Nacional de Proteção de Dados (ANPD) sugere. Tais iniciativas podem variar desde políticas de privacidade compreensíveis, RIPD (Relatório de Impacto à Proteção de Dados) ou planos de gestão de incidentes.

(CAVALCANTI, 2022) destaca que a adoção dessas medidas deve estar alinhada aos padrões internacionais de gestão da privacidade, como a ISO/IEC 27701, que avalia a capacidade da organização de implementar um sistema estruturado de proteção de dados pessoais, contemplando governança, gestão de riscos, segurança da informação e conformidade normativa, o que amplia a credibilidade empresarial em um contexto global. Nesse mesmo sentido, (PECK, 2021) enfatiza que a segurança de dados deve ser compreendida não apenas como exigência técnica, mas como valor ético e estratégico, demandando o engajamento da alta administração, a definição clara de responsabilidades e a incorporação da privacidade como princípio organizacional.

Dito isso, a conformidade com a LGPD deve ser o resultado de um fortalecimento do ecossistema interno de governança da informação — no qual cada segmento desempenha sua missão e o Encarregado de Proteção de Dados cumpre seu papel no meio de todos os atores. Segundo (DONENA, 2021), a eficácia desse modelo assenta em encontrar equilíbrio entre privacidade e inovação, segundo o qual as empresas podem crescer de forma saudável dentro de uma sociedade baseada em dados.

6 FUNÇÕES ESTRATÉGICAS E OPERACIONAIS DO ENCARREGADO

O Encarregado de Proteção de Dados (DPO) atua em duas capacidades: uma é operacional e a outra é estratégica. Seu papel principal não é apenas garantir que uma empresa cumpra a lei em relação à proteção de dados, mas também, ao incorporar e apoiar a proteção de dados nos objetivos da organização, agir como "motores de mudança" dentro das organizações.

No nível operacional, ele supervisiona o processamento de dados e auditorias, treina o pessoal e implanta ferramentas de supervisão e gestão de risco para garantir que as políticas de privacidade sejam implementadas na prática.

No nível estratégico, ele está envolvido nas decisões do conselho, no planejamento de produtos e parcerias e na defesa do privacy-by-design e privacy-by-default. Eles também contribuem para a

responsabilidade, aumentam a reputação corporativa e consolidam a confiança dos titulares de dados. Exige também autonomia, recursos para agir e independência funcional para que os programas de conformidade digital funcionem.

Por fim, o DPO também desempenha um papel educacional que permite a conscientização ética e cria uma cultura organizacional orientada para a proteção de dados. Assim, seu papel se desenvolve em duas áreas complementares: operacional - relacionada à gestão cotidiana - e estratégica - mais relacionada ao planejamento e à cultura corporativa -, estabelecendo-se como um gestor transversal dentro da corporação.

7 COMPLIANCE DIGITAL E GOVERNANÇA DE DADOS

No contexto da proteção de dados pessoais, **compliance digital** pode ser compreendido como o conjunto de políticas, procedimentos e práticas adotadas pelas organizações para assegurar que o uso de tecnologias, sistemas informacionais e fluxos de dados esteja em conformidade com a legislação vigente, com normas técnicas e com princípios éticos. Mais do que um simples atendimento a regras, envolve a implementação de critérios de transparência, registro de evidências, definição de responsabilidades internas e criação de mecanismos de controle e auditoria que permitam comprovar a aderência às exigências legais e regulatórias, como a LGPD, o Marco Civil da Internet e normas ISO relacionadas à gestão da informação.

Por sua vez, a **governança de dados** refere-se à estrutura organizacional responsável por planejar, supervisionar e orientar o ciclo de vida dos dados dentro da instituição — desde sua coleta e classificação até o armazenamento, compartilhamento, retenção e descarte. Essa governança inclui a definição de papéis (como controlador, operador e encarregado), critérios de acesso, políticas de minimização, mecanismos de segurança, gestão de riscos e controle de incidentes. Trata-se de uma abordagem estratégica que assegura integridade, confiabilidade e disponibilidade das informações, permitindo que os dados sejam utilizados de forma segura e responsável, com respeito aos direitos dos titulares e em alinhamento aos objetivos institucionais.

Com o progresso da transformação digital, há novas demandas para a proteção de privacidade, forçando a conformidade digital a ser uma parte crucial na organização moderna. Em termos da Lei Geral de Proteção de Dados (LGPD), conformidade não significa meramente obedecer a uma série de regras; é o alinhamento com uma estratégia integrada de governança pública que proporciona segurança jurídica, eficácia operacional e credibilidade institucional.

A Autoridade Nacional de Proteção de Dados (ANPD), por exemplo, indicou que os programas de governança de privacidade devem incluir políticas de proteção de dados definidas, processos de monitoramento e regras de avaliação de risco e resposta a incidentes, bem como a realização de Avaliações de Impacto sobre a Privacidade de Dados (DPIA). Estas são medidas não apenas

preventivas (ou seja, ajudam a prevenir violações), mas também garantem a responsabilização, ou seja, a entidade terá um meio de demonstrar que cumpriu suas obrigações de proteção de dados para indivíduos e autoridades.

Segundo (BIONI, 2020), conformidade digital significa organizações "adotando um comportamento proativo, para quem a proteção de dados pessoais é integrada à sua cultura organizacional e vai além da mera obrigação legal." Nesse sentido, (CAVALCANTI, 2022) destaca a importância de associar a LGPD aos padrões internacionais de segurança de dados, como a ISO 27701, para estabelecer parâmetros para sistemas de governança de dados pessoais.

Peck (2021) argumenta que os programas de conformidade digital são efetivos quando estruturados como processos contínuos, apoiados por mecanismos claros de governança e alinhados às estratégias organizacionais. A independência do DPO, o suporte da alta administração e a conscientização dos funcionários configuram fatores-chave para o sucesso em um ambiente de conformidade digital. Nesse sentido, a cultura organizacional desempenha papel decisivo, pois a efetividade das políticas de proteção de dados depende da adesão prática e do comprometimento de todos os envolvidos no ciclo de tratamento das informações. Além disso, (MONTEIRO & OLIVEIRA, 2020) destacam que a conformidade digital deve ser considerada como um elemento de governança corporativa se estiver alinhada aos objetivos estratégicos da empresa. Desta forma, a empresa transforma sua exigência regulatória em uma oportunidade de vantagem competitiva, aprimoramento reputacional e até mesmo de valorização de mercado.

Por fim, (DONEDA, 2021) descreve que a governança de dados não pode ser considerada apenas como um dispositivo de controle, mas corrigida para uma expressão de responsabilidade social, uma vez que envolve a salvaguarda de direitos fundamentais em um contexto de crescente dependência digital. A conformidade digital, portanto, confirma-se como um instrumento necessário, não apenas para prevenir sanções, mas também para garantir confiança, transparência e legitimidade por parte das organizações.

8 PERFIL PROFISSIONAL DO ENCARREGADO DE PROTEÇÃO DE DADOS NO BRASIL

Com o advento do status de Data Protection Officer (DPO) no Brasil, tornou-se necessário estabelecer um perfil profissional multidisciplinar capaz de conciliar conhecimentos jurídicos, técnicos e de gestão. A LGPD não estipula requisitos formais de certificação ou treinamento para o papel, exceto a capacidade de tal profissional de conduzir e apoiar o tratamento de dados pessoais em conformidade com a lei (BRASIL, 2018).

O DPO deve ser competente em toda a legislação nacional de proteção de dados e padrões internacionais, bem como ter um firme entendimento sobre segurança da informação, devido ao fato de que muitas violações de privacidade ocorrem devido a falhas tecnológicas (PECK, 2021). Isso é

corroborado por (CAVALCANTI, 2022), ao destacar que o profissional responsável pela proteção de dados precisa possuir, ainda que em grau inicial, familiaridade com normas técnicas internacionalmente reconhecidas, como a ISO/IEC 27001, que estabelece requisitos para a implementação de um Sistema de Gestão de Segurança da Informação (SGSI), e a ISO/IEC 27701, que complementa a primeira ao introduzir controles específicos voltados à proteção da privacidade, por meio de um Sistema de Gestão da Informação de Privacidade (PIMS – Privacy Information Management System), promovendo a integração entre segurança da informação e proteção de dados pessoais.

Na dimensão jurídica, (DONEDA, 2021) apontou que o DPO deve de alguma forma considerar e aplicar elementos como propósito, necessidade e proporcionalidade, equilibrando-se em uma abordagem baseada em direitos humanos, respeitando os direitos fundamentais das partes com os interesses legítimos das organizações. É esse papel de mediação que é fundamental para que o DPO seja visto como uma figura confiável pelos titulares de dados e reguladores.

De acordo com (MONTEIRO & OLIVEIRA, 2020), além do conhecimento técnico-jurídico, o DPO deve também ter uma série de habilidades interpessoais essenciais, que incluem comunicação clara, habilidades de negociação, empatia e liderança. Isso ocorre porque eles atuam como uma ponte entre diferentes departamentos dentro de suas empresas (jurídico, TI, RH, conformidade) e entre a própria empresa e os pedidos dos titulares de dados que podem surgir em circunstâncias de conflito.

Outra consideração é o aumento da demanda por treinamentos e certificações especializadas. Bootcamps nacionais e internacionais realizam cursos focados na atuação do DPO, promovendo padronização de habilidades e conscientização deste mercado em desenvolvimento. O empoderamento desta profissão está diretamente ligado à consolidação de uma cultura organizacional de proteção de dados no Brasil (Bioni, 2020).

Portanto, considerando o perfil perfeito do DPO brasileiro, ele deve combinar:

- Habilidades jurídicas – interpretação e aplicação da LGPD, GDPR e regulamentos setoriais;
- Técnicas – segurança da informação, controle de riscos e técnicos;
- Habilidades de comunicação, negociação e liderança interpessoais;
- Capacidade estratégica – Participar dos processos de governança e planejamento corporativo.

O DPO brasileiro:

Em síntese, o Encarregado de Proteção de Dados no Brasil assume uma natureza profissional híbrida, articulando conhecimentos jurídicos, competências tecnológicas e sensibilidade para lidar com aspectos humanos e organizacionais. Seu papel vai além do mero cumprimento de exigências legais, abrangendo a promoção de uma cultura institucional baseada na confiança, responsabilidade e proteção

efetiva dos dados pessoais, contribuindo para a consolidação da privacidade como valor estratégico e estruturante nas organizações brasileiras.

9 PROCEDIMENTOS METODOLÓGICOS

A natureza desta pesquisa é qualitativa, exploratória e descritiva, adequada ao tema estudado, uma vez que esses métodos permitem compreender fenômenos complexos, como o papel do Data Protection Officer (DPO) nas organizações brasileiras, a partir da análise de suas múltiplas dimensões jurídicas, tecnológicas, institucionais e humanas. Essa escolha metodológica permite a análise não apenas das dimensões legais e técnicas da LGPD, mas também de aspectos estratégicos e culturais que decorrem de sua implementação na prática dentro das organizações.

A análise é guiada pelo método dedutivo, que começa com os elementos teóricos e normativos da Lei Geral de Proteção de Dados (LGPD) e do Regulamento Geral de Proteção de Dados (GDPR) e prossegue para considerar os seus efeitos sobre os negócios. Isso faz com que o plano normativo se transponha para um plano organizacional, ao ver como os conceitos presentes na legislação se manifestam na prática das corporações.

Houve duas abordagens metodológicas principais nos estudos:

1. Revisão de literatura - levantamento e análise de livros, artigos científicos, relatórios e outras publicações que fornecem bibliografia contínua sobre o tópico de proteção de dados, bem como sobre o DPO. Esta etapa serviu como base para a compreensão crítica e fundamentação teórica do fenômeno estudado.
2. Pesquisa documental - A análise de legislações, normas, declarações e manuais emitidos por órgãos reguladores, mas também documentos institucionais emanados de instituições que já implementaram programas de conformidade voltados para a proteção de dados. Este processo enriqueceu a identificação de melhores práticas e dificuldades encontradas na realidade dos negócios.

Não foram realizados estudos de casos empíricos porque o trabalho foi em grande parte teórico e normativo em natureza. O objetivo é apresentar uma visão integrada e crítica sobre a posição do Data Protection Officer, sintetizando literatura com documentos oficiais. Por esse motivo, a metodologia adotada é planejada para manter a coerência e a objetividade em profundidade ao longo da análise, o que torna um estudo que pode contribuir tanto com o debate acadêmico quanto com a prática profissional relacionada à aplicação da Lei de Proteção de Dados à governança corporativa.

10 RESULTADOS E DISCUSSÃO

De acordo com a pesquisa, mostra-se que o oficial de proteção de dados (DPO) faz parte da centralização da LGPD no Brasil, sendo considerado não apenas uma obrigação legal, mas também um elemento estratégico para a governança corporativa. Sua atuação se desdobra em três dimensões interdependentes. No âmbito operacional, o DPO contribui para a segurança da informação, mitigação de riscos e conformidade processual por meio de avaliações de impacto, auditorias e implementação de políticas de proteção de dados. Na dimensão estratégica, participa da tomada de decisões e promove a integração entre proteção de dados e objetivos organizacionais, fortalecendo a confiança institucional e aprimorando as relações internas e externas. Sob a perspectiva cultural, impulsiona ações de capacitação e conscientização, consolidando a ética da privacidade como valor corporativo e promovendo uma cultura organizacional orientada à responsabilidade e ao uso adequado das informações.

Em conclusão, o DPO deve ser concebido como um elemento sistêmico de governança da informação, cujos efeitos transcendem a conformidade legal e são projetados para a sustentabilidade das organizações em uma economia movida por dados.

11 CONCLUSÃO

A análise realizada evidencia que o Encarregado de Dados (DPO) é peça estratégica e indispensável diante das exigências da LGPD. Mais que obrigação legal, sua função estabelece confiança entre empresas, titulares de dados e a ANPD, consolidando uma cultura de ética, transparência e responsabilidade no uso da informação.

O estudo mostrou que o DPO atua tanto no âmbito operacional garantindo a conformidade diária e coordenando planos de prevenção quanto no estratégico, assessorando a alta gestão e integrando a proteção de dados ao planejamento corporativo. Essa dupla atuação fortalece a governança da informação e amplia a credibilidade organizacional.

Além disso, a presença do DPO favorece a conscientização interna e a formação de uma cultura de proteção de dados, transformando a adequação à LGPD em diferencial competitivo. Seu perfil multidisciplinar exige atualização constante e capacidade de diálogo com diversas áreas, consolidando-o como gestor transversal.

Conclui-se, portanto, que o DPO transcende o caráter regulatório, atuando como agente transformador essencial para um ecossistema corporativo baseado em confiança, inovação responsável e respeito à privacidade.

REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018**.** ***Lei Geral de Proteção de Dados Pessoais (LGPD)***. Diário Oficial da União, Brasília, DF, 15 ago. 2018.

BIONI, Bruno Ricardo. ***Proteção de dados pessoais: a função e os limites da autodeterminação informativa no Brasil***. 2. ed. São Paulo: Revista dos Tribunais, 2020.

DONEDA, Danilo. ***Da privacidade à proteção de dados pessoais.*** Rio de Janeiro: Forense, 2021.

MONTEIRO, Fabrício da Mota Alves; OLIVEIRA, Renato Leite Monteiro. ***Manual de proteção de dados: a LGPD na prática.*** São Paulo: Revista dos Tribunais, 2020.

PECK, Patrícia. ***LGPD Comentada: Lei Geral de Proteção de Dados Pessoais.*** 2. ed. São Paulo: Thomson Reuters Brasil, 2021.

CAVALCANTI, Maurício. ***Governança da informação: LGPD, ISO 27701 e boas práticas.*** São Paulo: Senac, 2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). ***Guias, recomendações e orientações técnicas.*** Disponível em: https://www.gov.br/anpd/. Acesso em: maio 2025.

GIL, Antônio Carlos. ***Métodos e técnicas de pesquisa social.*** 7. ed. São Paulo: Atlas, 2019.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). ***ISO/IEC 27001:2013 – Information security management systems.*** Geneva: ISO, 2013.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). ***ISO/IEC 27701:2019 – Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management.*** Geneva: ISO, 2019.