

A implementação de programas de compliance para adequação à LGPD

Leandro William Da Silva¹

Victor Pegoraro²

Resumo

Este trabalho analisa a implementação de programas de *compliance* como instrumento jurídico essencial para a adequação das organizações à Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018. Com base em pesquisa qualitativa, bibliográfica e documental, a investigação aborda os fundamentos legais da LGPD, os conceitos de dados pessoais e sensíveis, e os papéis dos agentes responsáveis pelo tratamento — controlador, operador e encarregado (DPO). O estudo também discute o conceito de *compliance* aplicado à proteção de dados, as normas que orientam sua estruturação nas empresas, o papel fiscalizador da Autoridade Nacional de Proteção de Dados (ANPD), as penalidades previstas em caso de descumprimento e como o titular dos dados pode buscar seus direitos em possíveis vazamentos de dados. A pesquisa conclui que os programas de *compliance* são mecanismos indispensáveis para assegurar a conformidade legal, prevenir riscos e garantir a proteção efetiva dos direitos dos titulares, promovendo uma cultura organizacional pautada pela ética, responsabilidade e respeito à privacidade no ambiente digital contemporâneo.

Palavras-chaves: LGPD; *Compliance*; Proteção de dados; ANPD; Responsabilidade jurídica.

Abstract

This study analyzes the implementation of compliance programs as an essential legal instrument for organizations to adapt to the General Data Protection Law (LGPD), Law No. 13,709/2018. Based on qualitative, bibliographic, and documentary research, the investigation addresses the legal foundations of the LGPD, the concepts of personal and sensitive data, and the roles of the data processing agents — controller, processor, and data protection officer (DPO). The study also discusses the concept of compliance as applied to data protection, the regulations that guide its structuring within companies, the supervisory role of the National Data Protection Authority (ANPD), the penalties applicable in cases of non-compliance, and how data subjects can seek their rights in the event of data breaches. The research concludes that compliance programs are

¹ Graduando em Direito, Universidade Santo Amaro.

² Orientador.

indispensable mechanisms to ensure legal conformity, mitigate risks, and effectively protect data subjects' rights, promoting an organizational culture based on ethics, accountability, and respect for privacy in the contemporary digital environment.

Keywords: LGPD; *Compliance*; Data protection; ANPD; Legal accountability.

Introdução

Com o avanço acelerado da tecnologia e a consolidação das relações digitais no cotidiano social, político e econômico, a coleta e o tratamento de dados pessoais tornaram-se práticas recorrentes e indispensáveis para o funcionamento de organizações públicas e privadas. Nesse contexto, a necessidade de proteção da privacidade e da integridade das informações pessoais ganhou especial destaque, culminando na promulgação da Lei nº 13.709/2018, a chamada Lei Geral de Proteção de Dados Pessoais (LGPD).

Inspirada no Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), a LGPD surge como marco legal no ordenamento jurídico brasileiro ao estabelecer regras claras, princípios fundamentais e deveres aos agentes de tratamento de dados, com o objetivo de assegurar direitos como liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Diante da complexidade das disposições da LGPD e da crescente pressão para que as organizações adotem medidas eficazes de conformidade, os programas de *compliance* voltados à proteção de dados passaram a desempenhar um papel estratégico no ambiente corporativo e institucional.

Tais programas, além de promoverem a adaptação normativa, são fundamentais para prevenir sanções administrativas, mitigar riscos legais e preservar a reputação das organizações diante dos titulares de dados e da Autoridade Nacional de Proteção de Dados (ANPD), responsável pela fiscalização do cumprimento da lei.

A presente pesquisa tem por objetivo geral realizar uma análise jurídica sobre a implementação dos programas de *compliance* como ferramenta de adequação à LGPD, investigando como tais mecanismos contribuem para atender às exigências legais, fortalecer a governança de dados nas organizações e compreender de que maneira as penalidades previstas na legislação são aplicadas em casos de descumprimento.

Além disso, busca-se compreender o conceito de *compliance* à luz da LGPD, identificar a legislação e as normas que regulamentam a estruturação desses programas, examinar o papel exercido pela ANPD como ente fiscalizador e estudar as sanções administrativas previstas na LGPD, tanto sob o aspecto preventivo quanto repressivo.

Para alcançar esses objetivos, a metodologia utilizada é de natureza qualitativa, com abordagem exploratória e descritiva, fundamentada em pesquisa bibliográfica e documental. Foram analisadas obras doutrinárias, artigos científicos disponíveis em bases como o Google Acadêmico, bem como a própria legislação aplicável, incluindo a LGPD e os atos normativos expedidos pela ANPD.

A partir dessa abordagem, pretende-se oferecer uma reflexão crítica e técnica sobre os desafios jurídicos e organizacionais da proteção de dados pessoais no Brasil, evidenciando a importância da cultura de conformidade como meio de garantir a segurança jurídica e a efetivação dos direitos fundamentais no ambiente digital.

1. A LGPD e o conceito de compliance

Tendo sido sancionada em 14 de agosto de 2018, em 18 de dezembro de 2020, após o *vacatio legis* de dois anos, a Lei nº 13.709/2018 (BRASIL, 2020), mais conhecida como Lei Geral de Proteção de Dados (LGPD), representou um grande avanço na legislação brasileira, tendo em vista que a presente lei determina e direciona todas as ações no que diz respeito ao tratamento de dados pessoais no âmbito público e privado. (ALMEIDA, 2020).

Ante a consolidação das tecnologias digitais e a necessidade intrínseca de seu uso nas mais diversas áreas da vida do brasileiro, tais contextos desembocaram na massiva coleta de informações pessoais dos usuários. Com isso, torna-se impossível não fazer menção ao caso envolvendo a Crambridge Analytica, empresa que realizou o uso indevido de dados de usuários do Facebook, reforçando a importância da garantia de privacidade e segurança das informações pessoais dos usuários. (G1, 2018)

Não obstante, além do contexto apresentado, a LGPD sofreu grande influência da legislação europeia sobre dados pessoais, a Regulamento Geral sobre Proteção de Dados (*General Data Protection Regulation – GDPR*), estabelecendo rigorosamente a padronização e diretrizes para o tratamento de dados pessoais nos países da União Europeia, sendo a base sob a qual se funda a legislação nacional (LEMOS apud PINHEIRO, 2020).

Antes do advento da LGPD, inexistia qualquer legislação em âmbito nacional que regulamentasse a proteção dos dados pessoais. Existiam leis esparsas, como o Marco Civil da Internet (Lei 12.965/2014), Carolina Dieckman (Lei 12.737/2012) e do Cadastro Positivo (Lei 12.414/2011), que ainda deixavam lacunas quanto a questão do tratamento dos dados pessoais.

Com isso, a ausência de normas claras e coesas resultava em enorme insegurança jurídica aos titulares dos dados, bem como para as organizações que realizava seu tratamento. Diante desse contexto, a LGPD não só supriu a necessidade latente de atender as demandas concernentes ao tratamento dos dados, firmando princípios e obrigações no que tange tal temática (SCIMAGO, 2023).

Ademais, no que tange as obrigações, a LGPD define que as pessoas jurídicas de direito público e privado ajam com transparência em todos os atos que envolvam o tratamento dos dados pessoais de qualquer indivíduo, visando conceder maior controle sobre suas informações (CAETANO e BIFF, 2024)

Não obstante, será melhor explicitado adiante, mas a LGPD prevê a necessidade do consentimento do titular para o tratamento dos dados, o fornecimento do acesso às informações a qualquer momento seja para corrigir ou apenas ser informado sobre como se dá o tratamento de seus dados, além de obrigar a forja de meios mais seguros para proteção dos dados contra acessos não autorizados (CAETANO e BIFF, 2024).

Em seguida, quanto a finalidade da LGPD, o Art. 1º dispõe o seguinte:

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 (BRASIL, 2018).

Conforme se vê, o objetivo principal reside na necessidade de expressão do ser humano quanto a sua liberdade, honra, intimidade, privacidade e o livre desenvolvimento da pessoa humana, zelando pelas diretrizes previstas no Art. 5º, inciso X da Carta Magna de 1988 (BRASIL, 1988)

Além do mais, conforme já mencionado anteriormente, o advento da LGPD está atrelado a necessidade de instauração de segurança jurídica referente ao tratamento dos dados pessoais; padronizando os processos e implicando no desenvolvimento tecnológico e econômico do país, garantindo que as inovações tecnológicas estejam alinhadas com a segurança dos direitos dos indivíduos que tem suas informações tratadas pelas diversas instituições que os tratam.

Em razão disso, a LGPD prevê a criação da Agência Nacional de Proteção de Dados (ANPD), sendo uma das finalidades da lei, à fim de que seja o órgão responsável por fiscalizar o cumprimento das obrigações previstas na legislação, além de velar pela proteção dos dados pessoais (BRASIL, 2018).

1.1 Conceito de compliance

Em primeiro lugar, antes de se conceituar o que é o *compliance*, é necessário esmiuçar a palavra em si. O termo é uma derivação de “*comply*”, que significa “cumprir” ou “estar em conformidade” (GOOGLE, 2025), ou seja, no que tange o contexto empresarial, trata-se das ações tomadas pelas organizações para assegurar o cumprimento da legislação vigente, alinhando procedimentos internos e externos, agindo de forma ética, visando garantir que as atividades desempenhadas pelas organizações estejam em conformidade (LOUZADA et AL, 2020).

No mesmo sentido, o *compliance* abarca diversas áreas dentro de uma organização, tais como a implementação de políticas internas, códigos de conduta, capacitação dos colaboradores, canais de denúncia, auditorias internas e externas, bem como mecanismos para monitoramento e controle, sendo esses os elementos que garantem a prevenção, detecção e combate ao descumprimento de qualquer das diretrizes estabelecidas (LOUZADA et AL, 2020).

Não apenas isso, mas a finalidade do compliance é o gerenciamento de riscos, de forma a permitir a aplicação dos princípios estabelecidos por cada organização, observando sua visão, missão e os valores que a regem (LOUZADA et AL, 2020).

Com isso, o compliance se tornou uma ferramenta indispensável, sendo adotado como uma necessidade estratégica no âmbito organizacional, não somente para que se adeque a legislação, mas além disso, auxilia no fortalecimento das organizações, influenciando em sua reputação, pois mitiga riscos em todas as áreas da organização, mas sua implementação e seus mecanismos garantem a conformidade das organizações privadas e públicas a mitigação da corrupção e da

fraude nos recursos (CARARETTO, 2021).

Sua aplicação ganhou força através da promulgação da Lei 12.486/2013 (Lei Anticorrupção), que responsabiliza empresas por atos lesivos contra a administração pública, nacional ou estrangeira, fomentando a criação e adoção de integridade à fim de prevenir e identificar irregularidades (BRASIL, 2013) (CARARETTO, 2021).

Além disso, é necessário pontuar que os programas de compliance são mais do que o cumprimento de normas, pois refletem mudanças nos processos internos da organização e impactam na eficiência organizacional. Portanto, ao serem implementados, os programas criam um ambiente seguro e previsível, alinhando-se às exigências necessárias para as organizações se adequarem as diretrizes definidas pela legislação (OLIVEIRA, 2024).

Por este motivo, o compliance é imprescindível para as organizações, e no âmbito da LGPD, possui como finalidade principal implementar procedimentos internos para que o tratamento dos dados dos titulares esteja em conformidade com a norma vigente, visando a segurança e proteção das informações tratadas pelas organizações.

1.2 Conceito de dados

De acordo com o conteúdo demonstrado anteriormente, a LGPD preza pela proteção dos dados pessoais dos usuários; e com isso, em seu Art. 5º ela conceitua o que são os dados, que são divididos em quatro tipos: dados pessoais, dados pessoais sensíveis, dados anonimizados e banco de dados (BRASIL, 2018).

Tal diferenciação é necessária, tendo em vista a necessidade de diferentes formas de tratamentos que cada um deles recebe, conforme será melhor aduzido posteriormente.

De início, no que tange os dados pessoais, o Art. 5º, inciso I da LGPD define que o dado pessoal é qualquer informação estritamente relacionada com uma pessoa natural identificada ou identificável (BRASIL, 2018). Ou seja, tratam de informações objetivas que identificam a pessoa civilmente perante a sociedade como sujeito de direitos e deveres, tais como nome, endereço, número de telefone, endereço de e-mail e outros documentos que não expõem sua intimidade.

Ao contrário dos dados pessoais, os dados pessoais sensíveis estão ligados à esfera subjetiva do sujeito, e, conforme o Art. 5º, inciso II da LGPD, consistem em:

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; (BRASIL, 2018).

Tendo isso em vista, existe a necessidade maior de proteção desses dados, pois permitem delinear o perfil da pessoa, posto que tais informações dizem respeito a suas preferências baseadas nos seus gostos, podendo ser utilizados para fins que podem acarretar em diversos prejuízos ao sujeito.

Além dos dados pessoais e dos dados pessoais sensíveis, os dados anonimizados, previstos no inciso III do Art. 5º da Lei, são os dados relativos aos titulares que não podem ser identifi-

cados, logo, a forma de tratamento desses dados se dá de forma diversa a dos anteriores (BRASIL, 2018).

E, por fim, no que tange o conceito de dados previsto no Art. 5, inciso IV da LGPD, estão os bancos de dados; estes que são o conjunto de dados pessoais estruturados em diversos locais, podendo ser suportados de forma física ou eletrônica, armazenados em servidores (BRASIL, 2018).

Diante disso, os dados são informações essenciais em todas as áreas da vida do indivíduo e da sociedade, abrangendo desde as atividades mais básicas do cotidiano, como saúde, educação, segurança e emprego; ou até mesmo o oferecimento de diversos serviços alinhados as necessidades e anseios do consumidor, realizando uma intersecção com os diversos ramos do direito.

Contudo, a LGPD regula o tratamento dos dados com a finalidade de que não sejam utilizados de forma indevida ou sem autorização dos titulares, podendo incidir em riscos à privacidade e à segurança dos indivíduos em diversos níveis, como a esfera criminal através de fraudes e discriminação, ou até mesmo na coleta dos dados para uso em eleições ou outros eventos relevantes no cenário geopolítico, conforme mencionado anteriormente no caso Cambridge Analytica.

Outrossim, no que tange os dados, tais informações sempre estão vinculadas a um titular que tem suas informações tratadas por alguma entidade pública ou privada, conforme prevê o Art. 5º, inciso V da LGPD, o qual dispõe o seguinte:

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; (BRASIL, 2018).

Entretanto, embora no caso dos dados anonimizados num primeiro momento o titular possa ser identificado, ainda sim, a sua não identificação não implica a inexistência de um titular, portanto, qualquer dado que seja objeto de tratamento pertence a um titular de direitos e obrigações quanto a essas informações.

Em razão disso, a LGPD regula como é realizado o tratamento desses dados em seu Art. 5º, inciso X:

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; (BRASIL, 2018).

Não obstante isso, Art. 6º da Lei prevê os princípios que norteiam as ações quanto ao tratamento dos dados, que são finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização (BRASIL, 2018).

Além disso, no que diz respeito ao tratamento de dados pessoais, o artigo 7º da Lei Geral de Proteção de Dados (LGPD) elenca as bases legais que autorizam esse processamento, tais como: autorização expressa do titular; cumprimento de deveres legais ou normativos pelo agente de tratamento; atuação de entidades da administração pública; condução de pesquisas por instituições científicas; execução de contratos; exercício legítimo de direitos em processos judiciais, administrativos ou arbitrais; preservação da vida ou integridade física do titular ou de terceiros; assistência à saúde; atendimento ao interesse legítimo do controlador ou de terceiros, bem como para fins de proteção ao crédito (BRASIL, 2018).

No mesmo sentido, no que diz respeito aos dados pessoais sensíveis, é necessário destacar que o Art. 11 prevê as hipóteses de tratamento, porém, observa-se que a única diferença no trato das informações é que o consentimento é realizado de forma específica e destacada, para finalidades específicas (Art. 11, inciso I), com o restante dos requisitos igual, com algumas hipóteses previstas para os dados pessoais não se estendendo aos dados sensíveis (BRASIL, 2018).

Em suma, ao observar os tipos de dados, se vê que a distinção entre eles reside no grau de proteção necessário para garantia da segurança das informações, os dados pessoais por caracterizarem informações de identificação do indivíduo e os dados sensíveis por abrangerem a intimidade, necessitam de maior proteção, tendo em vista que própria lei dá uma tutela reforçada as informações que, se utilizadas indevidamente, podem infringir os direitos da personalidade previstos na Constituição Federal.

Após apresentar o conceito de dados e como são tratados, também é imprescindível destacar as hipóteses sobre as quais o tratamento de dados termina.

Previstas no Art. 15 da LGPD, o controlador encerra a utilização dos dados do titular quando a finalidade é alcançada (inciso I); o período de tratamento se encerra (inciso II); revogação do consentimento (inciso III) ou mediante determinação da Autoridade Nacional de Proteção de Dados (ANPD), – que será explicitada mais adiante – em razão de irregularidade ou infração à lei (BRASIL, 2018).

Diante disso, conclui-se que o término do tratamento dos dados está intrinsecamente ligado ao princípio da finalidade, o qual define que os dados podem ser mantidos enquanto estiverem sendo utilizados de acordo com finalidade determinada ao momento do consentimento do tratamento (BRASIL, 2018), evitando qualquer desvio de finalidade decorrente do uso prolongado dos dados.

Por este motivo, após o fim do tratamento, o ciclo de tratamento dos dados finaliza com a eliminação dos dados. Tal procedimento é previsto pelo Art. 16 da Lei, e implica apagar completamente as informações tratadas de forma física, lógica ou ainda através da anonimização, um procedimento que dissocia os dados de seu titular, impedindo a sua identificação (BRASIL, 2018).

Logo, os dados devem ser eliminados de todas formas de armazenamento. Contudo, os dados ainda podem ser conservados se forem utilizados para as seguintes finalidades:

- I - cumprimento de obrigação legal ou regulatória pelo controlador;
- II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados. (BRASIL, 2018).

Essa possibilidade têm a pretensão de preservar a segurança jurídica e a finalidade legítima da manutenção dos dados, devendo ser excluídos após o término da finalidade, desde que o titular dos dados autorize expressamente.

1.3 Dos responsáveis pelos dados

A Lei Geral de Proteção de Dados (LGPD) elabora e organiza de forma clara e concisa os responsáveis pelo tratamento dos dados nas organizações, definindo para cada responsável o desenvolvimento de competências específicas no que tange o controle das informações, exercendo um papel preponderante, garantindo o cumprimento das disposições legais, proporcionando a segurança dos dados e direitos dos titulares.

No escopo da LGPD, os agentes principais definidos para o tratamento dos dados nas organizações são: o controlador, o operador e o encarregado (ou Data Protection Officer – DPO). A seguir, serão elencadas suas atribuições e onde cada um deles se encaixa dentro da organização.

Em primeiro lugar, o Controlador de Dados é a pessoa natural ou jurídica, de direito público ou privado, a quem competem todas as decisões correspondentes ao tratamento de dados pessoais, conforme prevê o Art. 5º, inciso VI da LGPD (BRASIL, 2018).

Além disso, segundo a Resolução nº 9 de 02/09/2020, “o Controlador é a pessoa jurídica de direito público interno a quem compete definir as principais ações relativas ao tratamento dos dados pessoais” (TJDFT, 2025).

Diante disso, o controlador é o ente que define a finalidade e os meios de tratamento dos dados do titular, promovendo neste processo os dados que serão tratados, a forma mais segura de tratamento, devendo também elaborar relatórios de impacto, esclarecendo todos os processos da organização quanto a forma de tratamento dos dados, demonstrando a eficácia nos procedimentos utilizados pela organização à fim de promover a segurança das informações por ela manipuladas (MELLO, MIRAMONTES, 2021).

Em suma, a função do controlador é definir todas as diretrizes sobre o tratamento de dados pessoais, sendo uma peça crucial para que o tratamento dos dados siga os parâmetros estabelecidos pela LGPD, à fim de cumprir com os princípios da finalidade, necessidade e a transparência que regem tal legislação.

Após definir quem é o controlador dos dados, a LGPD prevê em seu Art. 5º, inciso VII a figura do Operador de Dados:

Art. 5º Para os fins desta Lei, considera-se:

[...]

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; (BRASIL, 2018).

Não apenas isto, mas segundo a Resolução nº 9 de 02/09/2020 também prevê que o operador completa os referidos incisos, afirmando que sua responsabilidade se estende a “todas as instâncias da instituição ou no âmbito de contratos ou instrumentos congêneres firmados com ele.” (TJDFT, 2025).

Diante disso, observa-se que o operador atua como agente executor das decisões do controlador, desempenhando suas funções sob sua orientação direta. Submisso às diretrizes previamente definidas, cabe ao operador implementar as instruções recebidas, de modo a garantir o cumprimento da finalidade e dos meios de tratamento determinados pelo controlador (MELLO, MIRAMONTES, 2021).

Em suma, o operador é àquele que coloca em prática todo planejamento estratégico traçado pelo controlador, agindo em sua pessoa, sendo um funcionário da organização ou uma empresa contratada para efetuar os préstimos de tal atividade, além de ser um requisito essencial que o operador possua conhecimentos na área de tecnologia da informação e correlatas (FILHO, JUNIOR, 2021).

Após discorrer sobre o controlador e o operador dos dados, é imprescindível mencionar a figura do Encarregado de Proteção de Dados (Data Protection Officer – DPO), que está prevista no Art. 5º, inciso VIII da LGPD.

O DPO (Data Protection Officer), exerce uma função estratégica nas organizações, atuando como elo de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Cabe a esse profissional assegurar o cumprimento das disposições da LGPD, viabilizando a fiscalização, orientando sobre boas práticas e adotando medidas corretivas sempre que forem identificadas não conformidades. Para desempenhar suas atribuições de forma eficaz, é recomendável que o DPO possua conhecimentos sólidos em legislação de proteção de dados, governança corporativa, estrutura organizacional da empresa e segurança da informação (FILHO, JUNIOR, 2021).

Para a garantia de idoneidade das atividades praticadas pelo DPO, recomenda-se que este cargo seja apartado de qualquer vínculo empregatício com a organização, devendo ser um profissional com conhecimentos nas áreas de tecnologia e direito, tendo em vista o caráter das atividades exercidas, que exigem pleno conhecimento legislativo e tecnológico (MELLO, MIRAMONTES, 2021) (FILHO, JUNIOR, 2021).

Além disso, suas informações devem ser públicas, tendo em vista que é o receptor de todas as demandas externas, de forma a garantir o cumprimento da LGPD, bem como orientar toda a organização quanto as diretrizes e promover ações de conscientização, além de ser o responsável imediato por dispensar internamente as informações advindas da Agência Nacional de Proteção de Dados e providenciar as devolutivas para os titulares de dados (MELLO, MIRAMONTES, 2021).

Por fim, o DPO trata-se do responsável por trazer equilíbrio entre os interesses da organização e do titular dos dados, zelando pela estruturação de uma cultura organizacional orientada à proteção dos dados pessoais, também sendo um canal de comunicação eficaz entre a ANPD, os titulares e o controlador dos dados.

Partindo de uma análise de todo o exposto, é clara a diferença entre os responsáveis pelo tratamento de dados pessoais nas organizações, conforme estabelece a LGPD: o Controlador, o Operador e o Encarregado (DPO) possuem funções diversas e complementares, fundamentais à proteção dos dados pessoais dos titulares.

Dessa maneira, percebe-se que os agentes compõem uma estrutura de responsabilidades interdependentes, com o controlador planejando e decidindo, compondo a parte estratégica; o operador executa as ações direcionadas pelo controlador, ou seja, compõe a parte operacional; e o encarregado fiscaliza, orienta e comunica para que o controlador planeje de acordo com os parâmetros definidos na LGPD e o operador execute em conformidade com os preceitos determinados.

Assim sendo, cada membro que compõe a cadeia de tratamento dos dados, com suas especificidades, é deveras indispensável ao cumprimento das condutas previstas na LGPD, a proteção efetiva dos dados pessoais bem como a promoção e o fortalecimento da cultura de privacidade nas organizações.

2. A fiscalização da aplicação da LGPD

O escopo da LGPD prevê ações práticas das organizações quanto a prevenção e o tratamento de dados, porém, para garantir o cumprimento da legislação, o cenário infere a necessidade de uma fiscalização eficaz para prevenção de abusos, o uso indevido de dados, além de promover uma cultura de respeito à privacidade dos titulares.

Diante disso, para atuar no âmbito da fiscalização das atividades das organizações, a LGPD em seu Artigo 55-A dispôs sobre a criação da Autoridade Nacional de Proteção de Dados (ANPD), sendo esta a responsável por zelar pela proteção dos dados pessoais, fiscalizar e aplicar sanções em caso de descumprimento da legislação, possuindo o múnus de promover o conhecimento da legislação não só para as organizações como também para os titulares, criando uma espécie de “cultura de proteção de dados” (BRASIL, 2018).

Sua atuação é imprescindível para que a LGPD seja aplicada de forma eficaz, visto que possui a incumbência de fornecer as diretrizes para as organizações e atuar mediando as relações entre os titulares e os agentes de tratamento dos dados (BRASIL, 2022).

Sua natureza jurídica é de autarquia especial, e mesmo vinculada ao Presidente da República, possui autonomia administrativa, técnica e decisória para exercer suas atividades de maneira independente, aplicando multas e sanções para as instituições (BEZERRA e SALES, 2022).

De acordo com o Decreto nº 10.474/2020, a estrutura organizacional da ANPD é disposta da seguinte forma (BRASIL, 2020):

1. **Conselho Diretor:** Órgão máximo de direção da ANPD, composto por cinco diretores, incluindo o Diretor-Presidente. É responsável por deliberar sobre as matérias de competência da Autoridade e por estabelecer diretrizes para sua atuação.

2. **Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPd):** Órgão consultivo, composto por representantes de diversos setores da sociedade, incluindo governo, setor empresarial, academia e sociedade civil. Tem como função propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade.

3. **Órgãos de Assistência Direta e Imediata ao Conselho Diretor:**

- **Secretaria Geral:** Responsável por prestar apoio técnico e administrativo ao Conselho Diretor.
- **Coordenação-Geral de Relações Institucionais e Internacionais:** Atua na articulação com outras instituições e na representação da ANPD em fóruns internacionais.

4. **Órgãos Seccionais:**

- **Corregedoria:** Responsável por apurar irregularidades e infrações disciplinares no âmbito da ANPD.
- **Ouvidoria:** Canal de comunicação entre a ANPD e os cidadãos, recebendo sugestões, reclamações e denúncias.
- **Procuradoria Federal Especializada:** Presta assessoria jurídica à ANPD.
- **Coordenação-Geral de Administração:** Cuida das atividades administrativas e logísticas da Autoridade.
- **Coordenação-Geral de Tecnologia da Informação:** Responsável pela gestão dos recursos de tecnologia da informação e comunicação.

5. **Órgãos Específicos Singulares:**

- **Coordenação-Geral de Normatização:** Elabora e propõe normas relacionadas à proteção de dados pessoais.
- **Coordenação-Geral de Fiscalização:** Executa atividades de fiscalização e aplicação de sanções previstas na LGPD.
- **Coordenação-Geral de Tecnologia e Pesquisa:** Desenvolve estudos e pesquisas para subsidiar a atuação da ANPD.

A referida estrutura tem como objetivo garantir a efetividade do cumprimento das atividades da ANPD, promovendo o cumprimento da LGPD pelas organizações, à fim de evitar sanções de qualquer tipo e a aplicação de multas, visando a proteção dos dados pessoais e a privacidade de seus titulares (GOVERNO DO BRASIL, 2020).

3.

3. A aplicação da LGPD de acordo com os programas de compliance, sua implementação e as medidas tomadas em casos de vazamentos de dados

Diante da latente necessidade de adequação das empresas quanto a implantação da LGPD, o *compliance* possui um papel essencial para que as organizações alinharem suas práticas ao novo cenário regulatório brasileiro, sendo uma medida estratégica que visa mitigar riscos e garantir que as atividades sigam as diretrizes estabelecidas pela LGPD.

Nesse sentido, ela estabelece suas diretrizes através dos princípios norteadores das ações de tratamento de dados pessoais, sendo estes: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização, além de possibilitar a criação de políticas e práticas para proteger a privacidade dos dados, impactando a gestão estratégica e operacional das organizações (BRASIL, 2018).

Disto surge o processo de implementação de adequação do *compliance*, o qual envolve diversas etapas, e à fim de demonstrar as fases da implementação, utilizando um dos exemplos do *compliance* aplicado à implementação da LGPD, segundo o Manual de Implementação da LGPD da Controladoria Geral do Estado do Paraná, as fases incluem (PARANÁ, 2021):

1. **Mapeamento de Dados:** Identificação dos fluxos de dados pessoais dentro da organização, incluindo a coleta, armazenamento, uso e compartilhamento das informações.
2. **Análise de Riscos:** Avaliação dos riscos associados ao tratamento de dados pessoais e identificação de medidas para mitigá-los.
3. **Elaboração de Políticas e Procedimentos:** Desenvolvimento de políticas de privacidade, termos de uso e procedimentos internos que estabeleçam as diretrizes para o tratamento de dados.
4. **Designação do Encarregado de Dados (DPO):** Nomeação de um profissional responsável por atuar como canal de comunicação entre a organização, os titulares dos dados e a ANPD.
5. **Treinamento e Conscientização:** Capacitação dos colaboradores sobre as práticas de proteção de dados e a importância da conformidade com a LGPD.
6. **Monitoramento e Auditoria:** Implementação de mecanismos de monitoramento contínuo e auditorias periódicas para assegurar a efetividade das medidas adotadas (ANPD, 2022).

Tais práticas contribuem significativamente para que as organizações atendam a norma vigente, fortalecendo sua reputação, promovendo a confiança dos clientes e parceiros, além de contribuir para a consolidação de uma cultura organizacional baseada nos princípios basilares da LGPD, que preza pela ética, transparência e responsabilidade com o tratamento dos dados pessoais.

3.1 As penalidades e sanções pelo descumprimento

Conforme já mencionado, a implementação da LGPD nas organizações possui como objetivo a adequação à legislação vigente, com a ANPD sendo o órgão responsável pela fiscalização

quanto a aplicação da lei, aplicando sanções nos casos de descumprimento por parte das organizações.

Em razão disso, os Artigos 52 e 53 preveem as sanções administrativas, que incluem:

- Advertência com indicação de prazo para adoção de medidas corretivas;
- Multa diária com limite total de R\$ 50.000.000,00;
- Publicização da infração após devidamente apurada e confirmada sua ocorrência;
- Bloqueio dos dados pessoais relacionados à infração até sua regularização;
- Eliminação dos dados pessoais relacionados à infração;
- Suspensão parcial do funcionamento do banco de dados por até seis meses, prorrogável por igual período, até a regularização da atividade de tratamento;
- Suspensão do exercício da atividade de tratamento dos dados pessoais por até seis meses, prorrogável por igual período;
- Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (BRASIL, 2018).

Além das sanções, por meio da Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023 (BRASIL, 2023), que parametrizou os critérios para aplicação das sanções administrativas através da dosimetria da pena, visando adequar a gravidade da infração e a sanção a ser aplicada, observando o devido processo legal e o contraditório (PEIXOTO, 2024).

Ainda no que tange as penas aplicadas, a mesma resolução inclui critérios na dosimetria da pena, observando a gravidade e natureza das infrações e dos direitos pessoais afetados; boa-fé do infrator; vantagem auferida ou pretendida pelo infrator; condição econômica do infrator; reincidência; grau do dano; cooperação do infrator; adoção de mecanismos e procedimentos internos capazes de minimizar o dano; adoção de política de boas práticas e governança; pronta adoção de medidas corretivas e proporcionalidade entre a gravidade da falta e a intensidade da sanção (BRASIL, 2023).

Em suma, com a aplicação das penalidades e a dosimetria da pena, se verifica o compromisso da ANPD para a promoção da proteção dos dados pessoais no Brasil, garantindo maior segurança jurídica e incentivando maior responsabilidade por parte das organizações quanto a segurança das informações fornecidas pelos titulares dos dados.

3.2 Os mecanismos de reparação e responsabilização para os titulares de dados vazados

As diretrizes para implementação da LGPD através do *compliance* pavimentam o caminho para maior conscientização e as práticas das organizações sigam a legislação brasileira, corroborando para maior segurança jurídica e mais do que isso, dos dados dos titulares tratados pelos entes jurídicos.

Todavia, mesmo com a adoção da LGPD, ainda podem ocorrer vazamentos de dados oriundos do descumprimento da legislação, prejudicando o titular e colocando em risco a segurança das informações em posse das organizações.

Por este motivo, para garantir a reparação e responsabilização dos agentes quanto a qualquer conduta que prejudique a segurança dos seus dados, a LGPD assegura ao titular medidas para que possa buscar seus direitos e ter ciência de como suas informações estão sendo tratadas.

Conforme já mencionado anteriormente, as informações de contato do Encarregado de Proteção de Dados (DPO) devem ser públicas e de fácil acesso aos titulares, tendo em vista sua função essencial no ecossistema de proteção dos dados, propiciando ao titular que entre em contato com ele, – tendo em vista que é a fonte oficial de comunicação com o Controlador dos Dados – à fim de solicitar as informações sobre como se deu o incidente, os dados afetados e as medidas adotadas para mitigar os danos (DUQUE, 2025).

Tal medida está prevista no Art. 18 da LGPD, garantindo ao titular o direito de obter do controlador, a qualquer momento, informações claras e acessíveis sobre o tratamento de seus dados pessoais (BRAISL, 2018).

Na hipótese dessa medida não ser efetiva, o titular pode entrar em contato com a ANPD, apresentando uma reclamação, com o órgão efetuando a abertura de um processo de fiscalização e posteriormente aplicando um processo administrativo sancionador, conforme prevê a Resolução CD/ANPD nº 1, de 28 de outubro de 2021 (ANPD, 2021).

Além disso, o titular também pode se valer da tutela jurisdicional por meio de ação judicial, pleiteando a reparação por danos morais e materiais, pois de acordo com o STJ, há uma evidente evolução quanto ao reconhecimento do direito à indenização em casos de falhas na proteção dos dados pessoais (STJ, 2023).

Nesse sentido, o julgamento do REsp 2.121.904/SP julgou procedente o pedido de reconhecimento da responsabilidade objetiva de uma seguradora em razão do vazamento de dados sensíveis, expondo o entendimento no sentido de que o simples vazamento já seria suficiente para ensejar o dano moral presumido, considerando como critério o risco à violação da dignidade e privacidade do consumidor (LEMOS e ROCHA, 2025).

Diante disso, é necessário destacar, que o artigo 48 da LGPD prevê que em casos de incidentes de segurança que possam gerar qualquer dano ao titular dos dados, o controlador é obrigado a informar a ANPD e o titular sobre o ocorrido, devendo ser realizada em prazo razoável, e contendo as informações descritivas sobre o tipo de dados, a quais titulares pertencem, bem como todas as medidas de segurança que serão ou que foram efetivadas para anular ou mitigar eventuais prejuízos causados (BRASIL, 2018).

Por fim, a LGPD fornece ao titular diversas vias para que seus dados sejam protegidos, de forma a ver seus direitos garantidos caso ocorra o vazamento de informações, promovendo a comunicação com o controlador, a ANPD ou através da tutela jurisdicional, caso a situação não seja resolvida através da via administrativa.

Considerações finais

O principal propósito deste estudo foi examinar a aplicação dos programas de *compliance* como um instrumento crucial para a adaptação das empresas à Lei Geral de Proteção de Dados Pessoais (LGPD), Lei no 13.709/2018.

Através do método qualitativo, baseado na pesquisa bibliográfica e documental, foi possível compreender a estrutura normativa da LGPD, os princípios basilares que a norteiam no que tange o tratamento dos dados pessoais e sensíveis, além do papel dos principais agentes encarregados do tratamento de dados nas instituições: o controlador, o operador e o encarregado (DPO).

Não obstante, chegou-se à compreensão sobre a importância dos programas de *compliance* como ferramentas organizacionais essenciais para assegurar a legalidade, permitindo que as organizações não só evitem penalidades administrativas e legais, garantido segurança jurídica, mas também a promoção de uma cultura que promove a importância da proteção dos dados, além de fortalecer sua imagem institucional perante a sociedade.

Em seguida, o presente artigo também possibilitou uma análise da função e das atividades desempenhadas pela da Autoridade Nacional de Proteção de Dados (ANPD), demonstrando o processo de aplicação das penalidades e os instrumentos legais disponíveis ao titular em caso de vazamento ou mau uso de seus dados.

Assim sendo, observa-se que os objetivos gerais e específicos delineados no início desta pesquisa foram atingidos de forma satisfatória, respondendo os questionamentos, permitindo maior conhecimento sobre a implementação da LGPD através do *compliance*, demonstrando sua essencialidade para as organizações no que tange a proteção dos dados pessoais e destacando sua crescente relevância no cenário jurídico brasileiro.

Referências

- ALMEIDA, A. A proteção de dados e a posição de hipervulnerabilidade do titular. Revista Brasileira de Proteção de Dados, 2020.
- BIONI, B. Tratamento de dados pessoais: a função e os limites do consentimento do titular. Revista de Direito Civil Contemporâneo, n. 21, 2020.
- BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado, 1988.
- BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais – LGPD. Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.
- BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Diário Oficial da União: seção 1, Brasília, DF, 24 abr. 2014.
- BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos – Lei Carolina Dieckmann. Diário Oficial da União, Brasília, DF, 3 dez. 2012.
- BRASIL. Lei nº 12.414, de 9 de junho de 2011. Dispõe sobre a formação e consulta a bancos de da-

dos com informações de adimplemento de pessoas naturais ou de pessoas jurídicas para formação de histórico de crédito – Lei do Cadastro Positivo. Diário Oficial da União, Brasília, DF, 10 jun. 2011.

BRASIL. Decreto nº 10.474, de 26 de agosto de 2020. Regulamenta a estrutura da Autoridade Nacional de Proteção de Dados – ANPD. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10474.htm. Acesso em: 2 jun. 2025, às 17h20.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 4 jun. 2025, às 20h40.

G1. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. G1, 2018. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml>. Acesso em: 21 abr. 2025, às 21h40.

CAETANO, C.; BIFF, C. LGPD: Lei Geral de Proteção de Dados Pessoais comentada: guia prático para adequação de empresas e profissionais. São Paulo: Revista dos Tribunais, 2024.

FILHO, J. C. A.; JUNIOR, M. A. D. Compliance e a LGPD: fundamentos e práticas para empresas. São Paulo: Juspodivm, 2021.

LEMO, R. apud PINHEIRO, M. F. Regulação e privacidade de dados: um olhar comparado entre LGPD e GDPR. Revista de Direito Digital e Novas Tecnologias, São Paulo, v. 6, n. 2, p. 15-30, 2020.

MELLO, J. P.; MIRAMONTES, R. F. Manual prático de adequação à LGPD: obrigações, agentes de tratamento e boas práticas. Rio de Janeiro: Forense, 2021.

INSTITUTO RUI BARBOSA – IRB. Lei Geral de Proteção de Dados Pessoais (LGPD): desafios da adequação à lei para as instituições públicas e privadas. Disponível em: <https://irbcontas.org.br/artigos/lei-geral-de-protecao-de-dados-pessoais-lgpd-desafios-da-adequacao-a-lei-para-as-instituicoes-publicas-e-privadas/>. Acesso em: 1 jun. 2025, às 08h40.

MENDES, L.; CARVALHO, J. O compliance e sua relevância para o setor público e privado. Revista Cosmos Acadêmico, v. 5, n. 1, 2018. Disponível em: <https://multivix.edu.br/wp-content/uploads/2021/06/revista-cosmos-academico-v05-n01-artigo05.pdf>. Acesso em: 4 jun. 2025, às 21h45.

SALES SARLET, G. B.; PIÑEIRO RODRIGUEZ, D. A Autoridade Nacional de Proteção de Dados (ANPD): elementos para uma estruturação independente e democrática na era da governança digital. Revista Direitos Fundamentais & Democracia, v. 27, n. 3, p. 217–253, 2022. DOI: 10.25192/issn.1982-0496.rdfd.v27i32285. Disponível em: <https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2285>. Acesso em: 1 jun. 2025, às 13h22.

SCIMAGO. Panorama jurídico sobre a proteção de dados no Brasil após a LGPD. Revista Scimago Jurídica, São Paulo, 2023. Disponível em: <https://www.scielo.br/j/emquestao/a/w3xQNY4bnytwK6MxzgyKgsy>. Acesso em: 13 mai. 2025, às 14:23.

TJDFT – Tribunal de Justiça do Distrito Federal e Territórios. Resolução nº 9, de 02 de setembro de 2020. Dispõe sobre medidas para implementação da LGPD no âmbito do TJDF. Disponível em: <https://www.tjdft.jus.br/transparencia/protecao-de-dados-pessoais/agentes-de-tratamento-e>

[encarregado](#). Acesso em: 14 de maio de 2025, às 15:50.

ALMEIDA, V. S. LGPD: fundamentos, impacto e desafios na sua aplicação. Revista Brasileira de Direito da Tecnologia da Informação, São Paulo, v. 4, n. 1, p. 45-59, 2020.

VERÍSSIMO, L. A importância do compliance nas instituições públicas. Tribunal de Contas dos Municípios de Goiás, 2021. Disponível em: <https://www.tcm.go.gov.br/escolatcm/wp-content/uploads/2021/10/Artigo-A-importancia-do-compliance-nas-instituicoes-publicas.pdf>. Acesso em: 4 jun. 2025, às 16h13.

Controladoria-Geral do Estado do Paraná. Manual de Implementação da LGPD. Curitiba: CGE-PR, 2021. Disponível em: https://www.cge.pr.gov.br/sites/default/arquivos_restritos/files/documento/2021-06/manual_implementacao_lgpd.pdf. Acesso em: 2 jun. 2025, às 20h07.

Autoridade Nacional de Proteção de Dados – ANPD. Guia orientativo para definição dos agentes de tratamento e do encarregado. 2. ed. Brasília: ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf. Acesso em: 28 mai. 2025, às 09h45.

PAMPLONA FILHO, João; SOUZA, Maria Clara; LIMA, Pedro Henrique. A Lei Geral de Proteção de Dados Pessoais e seus impactos no Direito do Trabalho. Revista Direito UNIFACS – Debate Virtual, Salvador, v. 5, n. 1, p. 15–30, 2021. Disponível em: <https://revistas.unifacs.br/index.php/redu/article/view/7108/4278>. Acesso em: 04 jun. 2025.