ISSN 3085-5624

Eixo Temático 1 - Produção, Mediação e Gestão da Informação

GOVERNANÇA DE DADOS E PRIVACIDADE NO SETOR SECURITÁRIO

DATA GOVERNANCE AND PRIVACY IN THE INSURANCE SECTOR

Dario Albuquerque Lima - Universidade Federal de Alagoas (UFAL), *dario_albuquerque@hotmail.com,* https://orcid.org/0009-0004-7400-2639

Alessio Sandro de Oliveira Silva - Universidade Federal de Alagoas (UFAL), *alessiosandro@gmail.com*, https://orcid.org/0000-0003-4880-5855

Cláudia Ney Alves de Assis - Sindicato dos Corretores de Seguros e de Capitalização (Sincor-AL), *claudia-seguro@hotmail.com*, https://orcid.org/0009-0009-8770-3174

Francisca Rosaline Leite Mota - Universidade Federal de Alagoas (UFAL), *francisca.mota@ichca.ufal.br, https://orcid.org/0000-0002-7283-0770*

Modalidade: Trabalho Completo

Resumo: A crescente digitalização no setor securitário brasileiro impõe desafios regulatórios complexos, destacando a imperatividade da privacidade de dados sob a Lei Geral de Proteção de Dados. O presente estudo visa analisar as estratégias e os obstáculos enfrentados pelas seguradoras na implementação da governança de dados para assegurar a conformidade e a proteção das informações. Através da revisão bibliográfica, da análise normativa e das políticas setoriais, buscou-se identificar as melhores práticas e as lacunas existentes. Os resultados evidenciam que a efetiva adequação demanda um robusto arcabouço de governança, uma cultura organizacional permeada pela proteção de dados e investimentos estratégicos em tecnologia.

Palavras-chave: Governança de Dados; Privacidade; LGPD; Setor Securitário; Proteção de Dados.

***Abstract**: The increasing digitalization in the Brazilian insurance sector imposes complex regulatory challenges, highlighting the imperative of data privacy under the General Data Protection Law. This study aims to analyze the strategies and obstacles faced by insurance companies in implementing data governance to ensure compliance and information protection. Through a bibliographic review, normative analysis, and sectoral policy examination, the research sought to identify best practices and existing gaps. The results show that effective compliance demands a robust governance framework, an organizational culture permeated by data protection, and strategic investments in technology.*

***Keywords**: Data Governance; Privacy; LGPD; Insurance Sector; Data Protection.*

1 INTRODUÇÃO

Na contemporaneidade, a informação emerge como o principal ativo para as organizações, redefinindo modelos de negócio e impulsionando inovações em diversos setores. O volume exponencial de dados gerados, processados e armazenados diariamente

transforma-o não apenas em um recurso, mas em um imperativo estratégico para a competitividade e tomada de decisões qualificadas. Essa centralidade da informação, no entanto, é acompanhada por crescentes desafios relacionados à sua gestão e, sobretudo, à sua proteção. Isto fica patente na obra de Castells (2000) quando afirma que "a produtividade e a competitividade na produção informacional se baseiam na geração de conhecimentos e no processamento de dados. A geração de conhecimentos e a capacidade tecnológica são as ferramentas fundamentais para a concorrência entre empresas, organizações de todos os tipos e, por fim, países".

Particularmente no setor securitário, a gestão de dados atinge uma dimensão crítica. Seguradoras operam com vastos volumes de informações pessoais, frequentemente de natureza sensível, a exemplo de dados de saúde, financeiros e judiciais, essenciais para a precificação de riscos, regulação de sinistros e personalização de produtos. Essa dependência informacional, embora vital para o negócio, eleva exponencialmente os riscos associados a vazamentos, uso indevido e acessos não autorizados, impactando diretamente a confiança do segurado e a reputação das empresas.

Rony Vainzof (2019) aponta que "a LGPD busca a proteção de direitos e garantias fundamentais da pessoa natural [...] de modo a mitigar riscos e estabelecer regras bem definidas sobre o tratamento de dados pessoais". Mais ainda, no que se refere aos dados pessoais sensíveis, como é o caso da área de seguros, o referido autor alerta que os agentes de tratamento "deverão, durante todo o ciclo de vida de tratamento de dados sob sua responsabilidade, analisar a conformidade legal e implementar os procedimentos de proteção dos dados pessoais, de acordo com a sua própria ponderação de riscos".

Em virtude de tal quadro, o Brasil promulgou a Lei Federal nº 13.709/2018, intitulada Lei Geral de Proteção de Dados Pessoais (LGPD), que estabelece paradigma para o tratamento de dados pessoais no país. A LGPD impõe rigorosas obrigações a todas as organizações que coletam, armazenam, processam ou compartilham dados de pessoas naturais, independentemente do meio ou da nacionalidade do dado. Para o setor securitário, a observância de seus princípios, bases legais e direitos dos titulares não é apenas uma exigência legal, mas uma condição para a legitimidade e a confiabilidade pública.

Diante do cenário de crescente regulamentação e sensibilidade informacional, a governança de dados é pilar estratégico e operacional indispensável, visto que representa o conjunto de processos, políticas, padrões e métricas que garantem a qualidade, integridade, segurança e usabilidade dos dados ao longo de todo o seu ciclo de vida. Para as seguradoras, a implementação de uma governança de dados eficaz não se limita ao cumprimento legal da LGPD, mas se configura como um diferencial competitivo que fomenta a confiança dos clientes, otimiza processos internos e reduz riscos jurídicos e reputacionais.

A despeito da regulamentação proposta pela Lei Geral de Proteção de Dados, as seguradoras enfrentam desafios na sua aplicação em virtude dos dados sensíveis, com a imperiosa necessidade de reestruturação de seus procedimentos internos. Deste modo, diante da necessidade de otimização da governança de dados no setor securitário, surge o seguinte problema de pesquisa: quais os principais desafios e quais estratégias devem ser adotadas pelas seguradoras que atuam no mercado brasileiro para implementação de governança de dados que garanta a privacidade, em consonância aos ditames legais?

O objetivo geral da pesquisa é investigar os principais desafios e quais estratégias devem ser adotadas pelas seguradoras que atuam no mercado brasileiro para implementação de governança de dados que garanta a privacidade.

Para alcançar o objetivo postulado, inicialmente, aborda-se os fundamentos teóricos da governança e privacidade de dados, bem como os preceitos da LGPD. Posteriormente, apresenta a análise dos resultados, discutindo os impactos da LGPD no setor securitário e as estratégias adotadas pelas seguradoras. Por fim, são apresentadas as conclusões do estudo, com considerações acerca das limitações e desafios do setor.

2 PRIVACIDADE E PROTEÇÃO DE DADOS: ARCABOUÇO TEÓRICO E LEGAL

A despeito de não raras vezes serem utilizados como sinônimos, os conceitos de privacidade e proteção de dados possuem nuances distintas, mas relacionadas. A privacidade se refere ao direito individual de controlar as informações sobre si, definindo quem, como e sob quais circunstâncias seus dados podem ser coletados, utilizados e compartilhados, ou seja, trata-se de um direito fundamental assegurado na Constituição Federal que busca assegurar a autodeterminação informativa. A proteção de dados, a seu

turno, constitui o arcabouço normativo, técnico e organizacional que instrumentaliza o direito à privacidade, estabelecendo as salvaguardas necessárias para que o tratamento de dados pessoais ocorra de forma segura, justa e transparente.

O direito à privacidade evoluiu de uma concepção mais restrita, focada meramente na inviolabilidade da vida privada, para uma abordagem mais abrangente, que contempla o controle sobre os próprios dados no ambiente digital. Essa transformação foi impulsionada pela explosão da coleta e processamento de dados pessoais por empresas e pelo Estado, demandando um arcabouço legal que transcendesse as proteções constitucionais genéricas. A ausência de regras claras e a assimetria de poder entre titulares e controladores de dados geraram um vácuo regulatório que tornou imperativa a criação de legislações específicas, capazes de equilibrar a inovação tecnológica com a salvaguarda dos direitos fundamentais da personalidade.

3 A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) NO CONTEXTO BRASILEIRO

A LGPD representa um marco regulatório fundamental para a proteção da privacidade e dos direitos de personalidade no ambiente digital e analógico. A LGPD visa a criar um ambiente de segurança jurídica para o tratamento de dados pessoais, ao mesmo tempo em que garante ao titular o controle sobre suas informações. Seu principal propósito é estabelecer regras claras e transparentes para a coleta, uso, armazenamento e descarte de dados pessoais, buscando equilibrar o desenvolvimento econômico e tecnológico com a proteção dos direitos fundamentais.

A LGPD estrutura-se em dez princípios fundamentais que devem nortear todo o tratamento de dados pessoais, garantindo que as operações sejam realizadas de forma ética e transparente. São eles: a) finalidade, que exige propósito legítimo e específico para o tratamento; b) adequação, que vincula o tratamento à finalidade informada; c) necessidade, que limita a coleta ao mínimo indispensável; d) livre acesso, que assegura a consulta facilitada dos dados; e) qualidade dos dados, que prevê exatidão e atualização; f) transparência, que impõe clareza nas informações sobre o tratamento; g) segurança, que requer medidas técnicas e administrativas para proteger os dados; h) prevenção, que visa evitar danos; i) não discriminação, que proíbe usos ilícitos ou abusivos; e j) responsabilização e prestação de contas, que exige a demonstração de conformidade pelo agente de

tratamento. A compreensão e aplicação desses princípios são essenciais para as seguradoras.

Para que o tratamento de dados pessoais seja lícito e esteja em conformidade com a LGPD, é indispensável que se enquadre em uma das bases legais previstas na lei. As mais relevantes para o setor securitário incluem o consentimento explícito do titular, o cumprimento de obrigação legal ou regulatória, a execução de contrato ou procedimentos preliminares relacionados a contrato do qual o titular seja parte, o exercício regular de direitos em processo judicial, administrativo ou arbitral, a proteção da vida ou incolumidade física do titular ou terceiro, a tutela da saúde, e o legítimo interesse do controlador ou de terceiro, observados os direitos e liberdades fundamentais do titular. A escolha da base legal adequada é um desafio complexo, notadamente para dados sensíveis como os de saúde, tão comuns na indústria de seguros.

A LGPD reforça a centralidade do titular dos dados, conferindo-lhe uma série de direitos que podem ser exercidos a qualquer momento. Destacam-se o direito de acesso aos dados, de correção de informações incompletas ou desatualizadas, de anonimização, bloqueio ou eliminação de dados desnecessários ou excessivos, de portabilidade, de revogação do consentimento e de oposição ao tratamento, conforme o art. 18 da lei em comento. Para garantir a efetividade desses direitos e a conformidade com a lei, a LGPD estabelece papéis e responsabilidades claras: o Controlador, que toma as decisões sobre o tratamento dos dados; o Operador, que realiza o tratamento em nome do Controlador; e o Encarregado pelo tratamento de dados pessoais. A correta definição e observância desses papéis são fundamentais para a implementação da governança de dados em qualquer organização, incluindo as seguradoras.

Para assegurar a efetividade da LGPD, foi criada a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal responsável por fiscalizar o cumprimento da lei, aplicar sanções e orientar os agentes de tratamento. A ANPD detém poder regulamentar sobre a matéria de proteção de dados, além de aplicar sanções administrativas. A potencialidade dessas sanções, somada ao risco de danos reputacionais e perdas de confiança, reforça a urgência e a criticidade da conformidade para todas as organizações, especialmente aquelas que lidam com um volume e sensibilidade de dados como as do setor securitário.

4 GOVERNANÇA DE DADOS: CONCEITOS E PRINCÍPIOS ESSENCIAIS

A gestão informacional transcende os limites da empresa, haja vista que a governança de dados é deveras essencial para o setor securitário, por estabelecer regras e processos que visam assegurar a precisão das informações, garantindo-se confiabilidade para o uso. A própria origem etimológica do termo “seguro” – do latim *securus*, que transmite a ideia de “garantido”, “sem necessidade de cuidados adicionais em virtude do alto zelo já empregado” – impõe a necessidade de governança de dados compartilhada de forma segura e eficiente, com a alta otimização do fluxo de trabalho. Tanto assim o é que Silva (2013) apregoa que o vocábulo se refere à “ação e efeito de tornar seguro ou de assegurar e garantir alguma coisa”, onde “qualquer que seja a sua aplicação, insere o sentido de tornar a coisa livre de perigos, livre de incertezas, assegurada de danos ou prejuízos, afastada de todo mal”.

Cumpre de pronto esclarecer que “dado é o conjunto de registros qualitativos ou quantitativos conhecido que organizado, agrupado, categorizado e padronizado adequadamente transforma-se em informação; informação são dados organizados de modo significativo, sendo subsídio útil à tomada de decisão” (Miranda, 1999) e governança, a seu turno, “tem origem etimológica no verbo latino *gubernare* e no termo grego *kubernaein* e que significa, literalmente, governar, e é adotado para transmitir a ideia de fornecer diretrizes e de auxiliar no cumprimento de objetivos” (Schwaitzer, 2023).

Khatri e Brown (2010, p. 149) definem **governança de dados** como o sistema que determina **quem tem a autoridade para tomar decisões** sobre os ativos de dados de uma organização e quem é **responsável por essas decisões**. Destaque-se que os autores não diferenciam explicitamente "dado" de "informação".

Deste modo, governança de dados é uma ação multifacetada cujo objetivo precípuo é o tratamento de dados na qualidade de insumos ativos e tangíveis nas organizações (Santos, 2010). Este conceito refere-se ao conjunto de diretrizes, processos, responsabilidades e tecnologias que garantem a qualidade, integridade, segurança, usabilidade e conformidade dos dados. Não se trata apenas de aspectos técnicos, mas de uma disciplina que envolve pessoas, políticas e a cultura organizacional para assegurar que os dados sejam ativos confiáveis e estratégicos para a tomada de decisões.

A eficácia da governança de dados repousa sobre princípios fundamentais que orientam sua implementação. Destacam-se a responsabilidade pela propriedade e uso dos dados, a transparência nos processos de tratamento, a integridade e qualidade da informação, a segurança contra acessos indevidos e, crucialmente, a conformidade com as regulamentações pertinentes. Para tanto, a disciplina de governança de dados abrange diversos componentes, a exemplo da definição de políticas e padrões, a gestão do ciclo de vida dos dados, o gerenciamento de metadados, a arquitetura de dados e a atribuição de papéis e responsabilidades, incluindo a figura de um Comitê de Governança de Dados.

5 A INFORMAÇÃO NA SOCIEDADE CONTEMPORÂNEA E O SETOR SECURITÁRIO

A sociedade hodierna caracteriza-se pela ubiquidade e pelo papel central da informação como recurso estratégico. Cumpre de pronto destacar que a ubiquidade é a "qualidade do que está ou existe em todos ou em praticamente todos os lugares" (Michaelis, 2015), de tal sorte que a "ubiquidade da informação - e também do usuário - se intensifica com a tríade móvel, que proporciona o acesso sem limitações de tempo-espaço aos documentos e representações da informação" (Foresti, Gregorio, Godoy Vieira, 2018).

Neste cenário, a informação transcende sua função de mero dado para se tornar um ativo intangível de valor inestimável, capaz de impulsionar a inovação, otimizar processos e subsidiar a tomada de decisões em todos os níveis organizacionais (Castells, 2000). Para o referido autor, a informação é sua matéria-prima, com predomínio da lógica de redes, flexibilidade, uma crescente convergência de tecnologias, bem como os efeitos das tecnologias têm alta penetrabilidade, haja vista que a informação é parte inerente de toda atividade humana. Deste modo, a capacidade de coletar, processar, armazenar e disseminar informações de maneira eficaz e segura tornou-se um diferencial competitivo, exigindo das organizações uma gestão informacional cada vez mais sofisticada e responsável.

Cumpre esclarecer que o Contrato de seguro consiste em instrumento econômico e jurídico de fundamental importância no que respeita tanto a compensação quanto a distribuição e a pulverização de riscos, estimulando, assim, a adoção de posturas preventivas racionalmente orientadas (Kölling; Araújo; Xavier, 2024).

No setor securitário, a informação assume um papel ainda mais estratégico, constituindo o cerne das operações e da tomada de decisões. A avaliação de riscos, a precificação de apólices, a análise e regulação de sinistros e a personalização de produtos e serviços são diretamente dependentes da coleta, processamento e análise de vastos volumes de dados pessoais. A capacidade de gerir e interpretar esses dados de forma eficiente não apenas otimiza as operações, mas também se traduz em vantagem competitiva e na construção de um relacionamento de confiança com os segurados, um pilar fundamental em um mercado baseado na mutualidade e na credibilidade.

6 O SETOR SECURITÁRIO: ESPECIFICIDADES E DESAFIOS NO TRATAMENTO DE DADOS PESSOAIS

O setor securitário é, por sua própria natureza, uma indústria intensiva em dados. A atividade-fim das seguradoras - leia-se, a gestão de riscos - baseia-se na coleta e análise de uma vasta gama de informações para calcular probabilidades, precificar produtos, gerenciar sinistros e desenvolver ofertas personalizadas. Essa dependência informacional é amplificada pelo avanço tecnológico, que permite a captação de dados de múltiplas fontes, desde históricos médicos e financeiros até dados de telemetria e comportamento do consumidor.

Neste sentido, Miragem e Petersen (2020) instruem que para a mensuração do risco a ser garantido, tem toda relevância a análise dos dados pessoais do segurado. Há íntima relação que se estabelece entre dados pessoais e risco coberto, na medida em que o conjunto de características subjetivas e comportamentais do segurado (e.g. sexo, idade, profissão, endereço, estado de saúde, consumo de cigarro) define fatores que influenciam na dimensão do risco, aumentando ou diminuindo a probabilidade de sinistro.

Para a mensuração do risco a ser garantido, tem toda relevância a análise dos dados pessoais do segurado. Há íntima relação que se estabelece entre dados pessoais e risco coberto, na medida em que o conjunto de características subjetivas e comportamentais do segurado (e.g. sexo, idade, profissão, endereço, estado de saúde, consumo de cigarro) define fatores que influenciam na dimensão do risco, aumentando ou diminuindo a probabilidade de sinistro.

Apesar do valor estratégico, o tratamento de tais dados no setor securitário apresenta desafios complexos, particularmente no que tange à privacidade e segurança da informação. A sensibilidade dos dados de saúde e financeiros, a necessidade de compartilhamento entre diferentes partes (corretores, resseguradores, prestadores de serviço) e a longevidade dos contratos de seguro exigem um controle rigoroso do ciclo de vida da informação. Além disso, a rápida evolução tecnológica para análises preditivas e personalização, embora traga benefícios, também intensifica os riscos de viés algorítmico, discriminação e uso indevido, tornando a conformidade com a LGPD um verdadeiro desafio

7 METODOLOGIA

A presente pesquisa adota uma abordagem de natureza qualitativa, uma vez que busca a compreensão aprofundada dos fenômenos relacionados à governança de dados e privacidade no setor securitário, em vez de quantificar dados. Quanto ao tipo, configura-se como exploratória e descritiva. É exploratória por investigar um tema relativamente recente e em constante evolução no contexto brasileiro, a saber, a implementação da LGPD em um setor complexo como o de seguros, objetivando identificar os principais desafios e estratégias. É descritiva na medida em que objetiva caracterizar as práticas e os impactos da legislação, detalhando o cenário atual da conformidade.

A coleta de dados para esta pesquisa fundamentou-se em duas abordagens principais: a pesquisa bibliográfica e a pesquisa documental. A pesquisa bibliográfica consistiu no levantamento e análise de literatura científica especializada, incluindo artigos, teses, dissertações e livros, focando em temas como governança de dados, privacidade, proteção de dados, LGPD e o setor securitário. Foram consultadas bases de dados acadêmicas como Scielo e Dimensions, a base de dados em Ciência da Informação e periódicos relevantes da área de Ciência da Informação e do Direito.

Ademais, a pesquisa documental envolveu a análise de documentos legais e regulatórios, como a própria Lei nº 13.709/2018 (LGPD), regulamentações da ANPD e, quando disponíveis publicamente, diretrizes setoriais e políticas de privacidade de grandes seguradoras que atuam no mercado brasileiro. Esse procedimento permitiu compreender o arcabouço normativo e as práticas de mercado em relação à conformidade com a LGPD e à gestão da privacidade no setor.

A coleta de dados foi realizada nos meses de junho e julho de 2025. Quanto à pesquisa bibliográfica, utilizou-se as bases de dados Scielo e Dimensions com os seguintes descritores: "governança de dados", "privacidade", "LGPD", "setor securitário" e "proteção de dados", com os seguintes resultados: 409 na Scielo e 4.956 na Dimensions. Após a verificação dos títulos e respectivos resumos, estabeleceu-se como critério de inclusão os artigos/trabalhos publicados nos últimos cinco anos que abordassem o setor securitário com pertinência temática à governança de dados, LGPD e privacidade. A seu turno, foram excluídos os resultados duplicados e os que não se relacionavam com o objeto do trabalho, especialmente o setor securitário.

A análise dos dados coletados, tanto da revisão bibliográfica quanto da pesquisa documental, foi realizada por meio de uma abordagem de análise de conteúdo temática. Foram explorados os seguintes eixos temáticos: a) a interpretação e os desafios da aplicação dos princípios e bases legais da LGPD no contexto securitário; b) as estratégias organizacionais (processos, tecnologias, cultura) adotadas pelas seguradoras para a conformidade com a proteção de dados; e c) as oportunidades e riscos associados à gestão da informação e privacidade no setor. A análise permite observar convergências, divergências e lacunas entre a teoria, a legislação e as práticas de mercado, gerando reflexões e inferências sobre a efetiva adequação do setor às exigências da LGPD.

8 RESULTADOS E DISCUSSÃO

A implementação da LGPD representou uma mudança paradigmática na gestão de dados pessoais por parte das seguradoras que atuam no Brasil. Antes da vigência da lei, o tratamento de informações, embora regulado por normativos setoriais, carecia de uma abordagem unificada e de uma cultura corporativa focada na proteção da privacidade do titular. Com o advento da lei, as empresas do setor reavaliaram seus processos de coleta, armazenamento, processamento e compartilhamento de dados, passando de uma lógica reativa para uma postura proativa em relação à privacidade como design e privacidade por padrão. Este novo cenário exigiu não apenas adaptações jurídicas e de *compliance*, mas uma profunda revisão de arquiteturas de sistemas e da própria cultura organizacional.

Um dos impactos mais significativos da LGPD foi a exigência de uma revisão exaustiva dos processos internos de tratamento de dados pessoais. As seguradoras precisaram mapear integralmente o ciclo de vida da informação, desde a captação na prospecção do cliente até o descarte final, para identificar riscos e garantir a adequação às novas diretrizes. Essa reavaliação incluiu a análise minuciosa das bases legais que justificam cada operação de tratamento. Para dados sensíveis, como os de saúde necessários para seguros de vida ou planos de saúde, a obtenção do consentimento específico e destacado do titular tornou-se, em muitos casos, a via preferencial, embora outras bases como o cumprimento de obrigação legal ou a execução de contrato também sejam amplamente utilizadas. A complexidade dessa escolha e a necessidade de comprovar a licitude do tratamento impuseram um desafio ao setor. Como bem aponta Bergstein e Trautwein (2022), a LGPD veda o uso de dados pessoais em desacordo com as legítimas expectativas do seu titular e os direitos e liberdades fundamentais, posto que esse novo microssistema de proteção de dados pessoais no Brasil traz novas luzes sobre o uso de informações pessoais pelo mercado de consumo, atribuindo responsabilidade e graves sanções nas hipóteses de uso indevido ou ilegítimo de dados pessoais.

Cumpre lugar de destaque o relatório intitulado “Regulação e Governança Regulatória do Setor de Seguros” elaborado pelo Instituto de Inovação em Seguros e Resseguros da Fundação Getúlio Vargas (FGV IISR, 2024). O relatório destaca que se implementou nacionalmente, através da Resolução nº 415/2021 do Conselho Nacional de Seguros Privados (CNSP), o *Open Insurance*, cujo objetivo é interligar ao *Open Finance* de modo a viabilizar dados e serviços financeiros e securitários no ecossistema. A despeito da facilidade de propostas adequadas aos perfis dos clientes com potencial redução de custos, podem surgir problemas em decorrência da segurança, da privacidade de dados, da fragmentação do mercado e fraudes.

Outro impacto direto e transformador da LGPD reside na exigência de garantir os direitos dos titulares de dados. Seguradoras foram impelidas a desenvolver canais e procedimentos eficientes para que os segurados pudessem exercer seus direitos de acesso, retificação, exclusão e portabilidade de dados. Isso demandou não só adequação tecnológica, mas também a designação de profissionais para a interlocução entre a empresa, os titulares e a ANPD. A criação e o fortalecimento de estruturas de governança, como

comitês de privacidade e unidades de *compliance* dedicadas, tornaram-se imperativos para gerenciar esses novos fluxos de informação e assegurar que as respostas aos titulares fossem dadas dentro dos prazos e padrões exigidos pela legislação.

8.1 Estratégias de governança de dados e privacidade adotadas pelas seguradoras

Para atender às exigências da LGPD, as seguradoras atuantes no mercado nacional têm adotado uma série de estratégias que abrangem desde a reestruturação de processos até a implementação de tecnologias avançadas e o desenvolvimento de uma cultura organizacional focada na proteção de dados. A conformidade não é vista apenas como uma obrigação legal, mas como uma oportunidade para fortalecer a confiança dos clientes e otimizar a gestão interna da informação. O primeiro passo para muitas dessas instituições foi a realização de um diagnóstico aprofundado do fluxo de dados, identificando quais informações são coletadas, onde são armazenadas, como são utilizadas e quem tem acesso a elas.

A partir do mapeamento de dados, as seguradoras concentraram esforços na elaboração e implementação de políticas e procedimentos internos robustos. Isso incluiu a criação de políticas de privacidade claras e acessíveis, termos de consentimento transparentes, regras para retenção e descarte de dados, e diretrizes para resposta a incidentes de segurança. A estruturação de um Comitê de Privacidade ou Governança de Dados também se tornou prática comum, garantindo a supervisão contínua e a tomada de decisões estratégicas sobre o tema, com profissionais da área jurídica e da tecnologia, os quais atuam como uma espécie de catalisador para a cultura de proteção de dados dentro da seguradora.

Ademais, as seguradoras têm investido em soluções tecnológicas para automatizar e otimizar a gestão da proteção de dados. Isso inclui a implementação de sistemas de gestão de consentimento, ferramentas para anonimização e pseudonimização de dados - técnica de proteção de dados que substitui identificadores diretos por identificadores indiretos -, plataformas de segurança da informação mais robustas, e sistemas de monitoramento de acessos. Todavia, a tecnologia por si só não garante a conformidade, e é fundamental que seja acompanhada por uma cultura organizacional que valorize a privacidade e a segurança.

Para tanto, programas contínuos de treinamento e conscientização de todos os colaboradores, desde a alta direção até as equipes operacionais, têm sido cruciais para disseminar as boas práticas e assegurar que a proteção de dados seja responsabilidade de todos na empresa.

8.2 Desafios e oportunidades na adequação à LGPD no setor securitário

Apesar dos significativos avanços na implementação da governança de dados e das estratégias de privacidade pelas seguradoras, o processo de adequação à LGPD ainda enfrenta desafios persistentes e complexos. Um dos principais obstáculos é a complexidade inerente aos dados do setor, que envolvem vastas redes de informações interconectadas, legados tecnológicos e a necessidade de interoperabilidade com múltiplos *stakeholders* (corretores, prestadores de serviço, resseguradores). Destaque-se que a migração de dados antigos e a garantia da conformidade em sistemas legados representam ônus deveras considerável para as empresas.

Além das barreiras técnicas, as seguradoras também enfrentam desafios de ordem cultural e de recursos humanos, uma vez que algumas corretoras que atuam no mercado brasileiro são oriundas de outros países, não raras vezes com cultura organizacional que tradicionalmente via o dado como um ativo a ser maximizado e que precisa se adaptar para a realidade nacional que exige zelo no tratamento dos dados. Diante disto, bem como das eventuais alterações normativas, há uma necessidade premente de capacitação contínua de profissionais em todos os níveis, desde a alta gerência, que precisa entender os riscos e as oportunidades estratégicas da conformidade, até as equipes operacionais, que lidam diretamente com os dados no dia a dia. Outrossim, a escassez de especialistas no mercado com o conhecimento multidisciplinar - jurídico, de segurança da informação e de governança - exigido pela LGPD agrava esse cenário, tornando a formação interna de equipes um investimento estratégico.

Por fim, destaque-se que a adequação à LGPD por parte das seguradoras implica na melhoria da governança e, por conseguinte, aumenta a credibilidade no mercado perante os concorrentes.

9 CONCLUSÃO

A presente pesquisa analisou a adequação aos requisitos da LGPD por parte das seguradoras atuantes no mercado nacional, e constatou-se que houve a necessidade de reestruturação dos procedimentos internos e atualização tecnológica. Tal adequação não é mero *compliance*, mas sim um verdadeiro mapeamento do fluxo dos dados.

Para a Ciência da Informação, o presente estudo contribuiu ao analisar a aplicação prática da governança e gestão de dados no complexo setor do mercado securitário. Restou demonstrado que há a imperiosa necessidade de contínua capacitação em prol da privacidade dos dados dos clientes.

Destaque-se que o presente estudo foi tão somente bibliográfico, documental e normativo, e sugere-se que haja posteriormente o desenvolvimento de estudos aprofundados com dados empíricos e pesquisas práticas de campo com as seguradoras visando analisar o modo como se dá a implantação de governança de dados e a preservação da privacidade dos segurados, o que promoverá maior compreensão do mercado securitário pátrio.

REFERÊNCIAS

BERGSTEIN, L.; TRAUTWEIN, J. R. A proibição de discriminação e os critérios do cálculo atuarial nos contratos de seguro. **Revista Científica da Academia Brasileira de Direito Civil**, Rio de Janeiro, v. 4, p. 53–67, 2022. DOI: 10.56119/rcabdc.v4.51. Disponível em: https://abdc.emnuvens.com.br/abdc/article/view/51. Acesso em: 8 ago. 2025.

CASTELLS, M. A era da informação: economia, sociedade e cultura. *In:* CASTELLS, M. **A Sociedade em rede**. São Paulo: Paz e Terra, 2000. v. 1.

FORESTI, F.; GREGORIO, V.; VIEIRA, A. F. G. Ubiquidade e ciência da informação. **Revista Ibero-Americana De Ciência Da Informação**, v. 12, n. 1, p. 191–216, 2018. Disponível em: https://doi.org/10.26512/rici.v12.n1.2019.19106. Acesso em: 8 ago. 2025.

FUNDAÇÃO GETULIO VARGAS – FGV. **Governança Regulatória**: regulação e governança regulatória do setor de seguros. Rio de Janeiro: FGV, 2024. Disponível em: https://fgviisr.fgv.br/sites/default/files/2024-05/Relatorio%20FGV%20-%20Regulacao%20e%20Governanca.pdf. Acesso em: 8 ago. 2025.

KHATRI, V.; BROWN, C. V. Designing data governance. **Communications of the ACM** v. 53, n. 1, p. 148-152, 2010.

KÖLLING, G. J.; ARAÚJO, C. V. P.; XAVIER, L. C. Gestão dos riscos climáticos, papel do setor securitário brasileiro. **Revista de Direito Econômico e Socioambiental**, Curitiba, v. 15, n. 2, e260, maio/ago., 2024.

MICHAELIS: Dicionário Brasileiro da língua portuguesa. São Paulo: Melhoramentos, 2015. Disponível em: https://michaelis.uol.com.br/busca?r=0&f=0&t=0&palavra=ubiquidade. Acesso em: 24 jul. 2025.

MIRAGEM, B.; PETERSEN, L. O contrato de seguro e a lei geral de proteção de dados. **Revista dos Tribunais**, v. 1018, n. 2020, ago. 2020.

MIRANDA, R. C. da R. O uso da informação na formulação de ações estratégicas pelas empresas. **Ciência da Informação**. v. 28, n. 3, 1999. Disponível em: https://doi.org/10.1590/S0100-19651999000300006. Acesso em: 8 ago. 2025.

SANTOS, I. M. F. dos. **Uma proposta de governança de dados baseada em um método de desenvolvimento de arquitetura empresarial**. 2010. 140 p. Dissertação (Mestrado em Informática) – Centro de Ciências Exatas e Tecnologia, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2010. Disponível em: http://www.repositorio-bc.unirio.br:8080/xmlui/bitstream/handle/unirio/12868/MI%2013%20-%202010.pdf?sequence=1&isAllowed=y. Acesso em: 24 jul. 2025.

SCHWAITZER, L. B. S. Governança de dados e o arquivista diplomatista. **Archeion Online**, v. 11, n. edi, 2023.

SILVA, De Plácido e. **Vocabulário jurídico**. 30. ed. Rio de Janeiro: Forense, 2013.

VAINZOF, R. Disposições preliminares. *In*: MALDONADO, V. N.; BLUM, R. O. (coord.). **LGPD**: lei geral de proteção de dados comentada. São Paulo: Thomson Reuters Brasil, 2019.