

Desafios de *Compliance da LGPD*: Implantação na Indústria de Software Brasileira

Juliana Saraiva¹, Cleidson de Souza², Sérgio Soares³

¹Departamento de Ciências Exatas - Universidade Federal da Paraíba (UFPB)
Rio Tinto, PB – Brasil

²Instituto de Ciências Exatas e da Natureza - Universidade Federal do Pará (UFPA)
Belém, PA – Brasil

³Centro de Informática - Universidade Federal de Pernambuco (UFPE)
Recife, PE – Brasil

julianajags@dcx.ufpb.br, cleidson.desouza@acm.org, scbs@cin.ufpe.br

Abstract. *The challenging LGPD implementation for software companies is also due to the lack of clear guidelines from the ANPD, requiring practical solutions that guarantee legal compliance and protection of personal data. Non-compliance results in administrative and legal proceedings, or non-monetary sanctions such as suspension of data use. Thus, the need to comply with the LGPD, international privacy laws, and the challenges related to AI demand solutions that are still non-existent or insufficient for the implementation of the law in the software industry. This scenario requires compliance analyses, aligned policies, audits, tests, and maturity models that were defined and are already being evaluated to support the software industry.*

Resumo. *O desafio da implantação da LGPD para empresas de software se dá por várias razões, inclusive pela falta de orientações claras e a exigência de soluções práticas que garantam a conformidade legal e proteção dos dados pessoais. A não conformidade acarreta processos administrativos e judiciais, ou sanções não monetárias, como suspensão de uso dos dados. Assim, a necessidade de cumprir a LGPD, leis internacionais de privacidade e os desafios relacionados à IA demandam soluções ainda inexistentes ou insuficientes para a implantação da lei. Este cenário requer políticas alinhadas, auditorias, testes e modelos de maturidade, que já foram definidos e estão sendo avaliados para dar suporte à indústria de software.*

1. O desafio da implantação da LGPD e sua opacidade normativa

A Lei Geral de Proteção de Dados (LGPD) é uma norma brasileira sancionada em 2018, vigorando a partir de 2020, que tem como objetivo assegurar a privacidade e a proteção dos dados pessoais dos cidadãos [LGPD 2018]. Ela se aplica a todas as pessoas naturais (CPFs) e jurídicas (CNPJs) que lidam com informações pessoais no Brasil, através da prestação de bens ou serviços. Baseia-se em princípios gerais e abstratos, em vez de tratar diretamente de situações específicas e detalhadas, deixando em aberto a interpretação e aplicação prática de como esses princípios devem ser seguidos em contextos específicos. Algumas dessas diretrizes ainda necessitam de regulamentação, que deve ser realizada pela Autoridade Nacional de Proteção de Dados (ANPD)¹.

¹<https://www.gov.br/anpd/pt-br>

Neste contexto, é importante frisar que a LGPD se caracteriza como uma lei que abarca três dimensões a serem observadas numa empresa de software: **jurídico, segurança da informação e governança**. Adicionalmente, ela tem uma natureza transversal no Direito Brasileiro, uma vez que influencia, e é influenciada, por outras normas já em vigor no país, como o Marco Civil da Internet, Lei da Informática, Leis dos Crimes Cibernéticos, Código de Defesa do Consumidor, Código Civil e outras. Como consequência, as empresas de software *não* podem se limitar a compreenderem apenas a LGPD para estarem em conformidade legal.

Neste conjuntura de complexidade e opacidade normativa, uma vez que a ANPD ainda não publicou um guia, protocolo ou arcabouço para que as instituições possam facilmente compreender como a lei deve ser efetivada, a maioria das empresas brasileiras ainda não estão adequadas à LGPD, incluindo as de software [Daryus 2023]. Para minimizar os riscos, algumas delas adotaram algumas medidas de segurança da informação *ad hoc*, mas ainda estão aquém do que seria a implantação de um Programa de Adequação à LGPD satisfatório. Além disso, pesquisas apontam que a maior parte das empresas de software no Brasil são microempresas, empresas de pequeno porte ou startups [SEBRAE 2020]. Assim, elas possuem recursos limitados e muitas vezes, equipes enxutas, prejudicando a implementação de políticas de privacidade robustas, a garantia da segurança dos dados pessoais, a obtenção do consentimento dos titulares de dados de forma adequada e respostas a possíveis vazamentos de informações. Adicionalmente, a falta de conhecimento especializado sobre a legislação e seus requisitos técnicos pode tornar o processo de adequação à LGPD ainda mais complexo.

Neste cenário, o grande desafio posto é a falta de **soluções que deem suporte prático em como implantar a LGPD pelas empresas de software**, descrevendo como fazer, quais etapas, quais profissionais devem se envolver, quais custos, quais formas de mensurar o processo e garantir a conformidade legal. Ressalta-se que além do desconhecimento por parte das empresas de software sobre como deve ser feito, os ataques cibernéticos e vazamentos de dados estão cada vez mais corriqueiros, e os softwares dessas empresas usam massivamente dados pessoais. Portanto, o objetivo deste artigo é destacar a importância e os desafios da implementação da LGPD no contexto das empresas de software no Brasil, abordando a complexidade da legislação, a falta de orientação prática por parte da ANPD, os recursos limitados das empresas de software, e a necessidade de suporte e orientação para garantir a conformidade legal e a proteção dos dados pessoais dos clientes, parceiros e colaboradores dessas empresas.

2. O Contexto da LGPD e seus Aspectos Humanos, Econômicos e Sociais na Indústria de Software

Aliado ao fato de que a LGPD é uma lei federal que deve ser seguida por todas as empresas que atuam no Brasil, a proteção de dados pessoais é uma preocupação global. Assim, a importância das empresas de software se adequarem à LGPD vai muito além da mera conformidade legal. Um dos **aspectos humanos** cruciais a serem considerados é a efetiva segurança dos dados pessoais, preservando sua integridade e privacidade, pois o uso indevido pode afetar a vida real dos usuários. Por exemplo, há possibilidades de fraudes financeiras, danos à reputação e prejuízos emocionais, roubo de identidade que levam a transações fraudulentas e comprometem a integridade financeira da vítima. Ademais, o vazamento de informações sensíveis pode abalar a confiança nas instituições

que coletam e armazenam esses dados, gerando um sentimento de vulnerabilidade e desconfiança em relação à segurança digital.

Neste cenário, as empresas de software precisam ter profissionais habilitados para lidar com a proteção de dados pessoais, nas áreas de segurança da informação, jurídica e de governança de dados pessoais. Portanto, a formação adequada dos profissionais nessas áreas garante não só o cumprimento das diretrizes legais, mas também uma cultura organizacional sólida e consciente da importância de proteger os dados pessoais de forma responsável e ética [Mendes 2023].

No mesmo sentido, a adequação a esta lei pelas empresas de software transcende o âmbito jurídico e adentra **aspectos sociais** de grande relevância. Os dados pessoais são frequentemente comparados ao petróleo do século XXI, representando um recurso valioso que pode influenciar não apenas a economia global, mas também a segurança nacional [Bergamasco 2021]. Nesse contexto, a conscientização e o letramento digital tornam-se fundamentais, especialmente no uso de softwares. A capacidade de entender e gerenciar adequadamente as informações pessoais dos usuários não só fortalece a confiança no ambiente digital, mas também contribui para a proteção dos direitos individuais e coletivos, promovendo assim uma sociedade mais segura e ética no uso da tecnologia.

Nesta conjuntura, o custo de implantação de medidas de conformidade pode ser significativo, especialmente para pequenas e médias empresas do setor, impactando **economicamente a indústria de software**. Além disso, a não conformidade com a LGPD pode acarretar em consequências financeiras severas, como o ressarcimento de indivíduos afetados por incidentes de vazamento de dados. Bancos e outras instituições financeiras, por exemplo, podem enfrentar altos custos relacionados ao estorno de pagamentos, transferências e créditos a titulares por causa de fraudes bancárias com dados pessoais. Instituições já estão sofrendo com multas, processos judiciais e danos à reputação por não cumprimento adequado das exigências da LGPD². Portanto, a adequação à legislação não apenas protege a privacidade dos usuários, mas também resguarda as empresas de possíveis impactos econômicos adversos decorrentes de violações à proteção de dados.

É relevante esclarecer que a LGPD estabelece sanções severas para a área de tecnologia em caso de descumprimento das normas de proteção de dados pessoais, o que aumenta a pressão sobre as empresas para garantir a conformidade. E mais, há outros tipos de punição como a advertência, a publicização da infração, o bloqueio dos dados pessoais, a eliminação dos dados pessoais, a suspensão parcial do funcionamento do banco de dados e a suspensão do exercício da atividade de tratamento dos dados pessoais [ANPD 2021]. Essas sanções não financeiras têm o objetivo de garantir o cumprimento das normas de proteção de dados e incentivar as empresas a adotarem práticas adequadas de tratamento das informações pessoais dos usuários, podendo afetar significativamente a indústria de software.

Quando se observa o desenvolvimento, distribuição e uso de softwares através da internet, o desafio das empresas de software em se adequarem à LGPD estão intrinsecamente ligados à necessidade de também cumprir leis internacionais. A natureza globalizada do software, juntamente com a distribuição geográfica de *datacenters* e a existência de outras legislações, como a GDPR (*General Data Protection Regulation*),

² <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-lista-de-processos-sancionatorios>

torna essencial o cumprimento das normas de proteção de dados não apenas em nível nacional, mas também em âmbito internacional. Adicionalmente, parcerias comerciais e relações intercontinentais exigem o cumprimento de diferentes regulamentações, destacando a complexidade e a importância de uma abordagem integrada e compatível com os padrões internacionais de privacidade e segurança de dados. Essa conformidade não apenas fortalece a reputação das empresas no cenário global, mas também garante a proteção dos direitos dos usuários em diferentes jurisdições.

Por fim, destaca-se que a falta de conformidade com a LGPD coloca as empresas em um cenário de alto risco ao utilizarem IA de forma ampla e intensiva. Isso ocorre devido à natureza sensível dos dados pessoais envolvidos no treinamento e na operação de sistemas de IA. A LGPD estabelece diretrizes e normas específicas para o tratamento desses dados, garantindo a privacidade e a segurança dos indivíduos. Portanto, o cumprimento da LGPD é um pré-requisito fundamental para que as empresas possam adotar a IA de forma eficiente e responsável, minimizando riscos legais, éticos e de reputação, conforme prevê o art. 20 da lei.

3. Soluções preliminares de adequação à LGPD em empresas de software

A adequação das empresas de software à LGPD exige iniciativas reais e efetivas voltadas a garantir a conformidade com os requisitos da legislação. Isso inclui a implementação de políticas de privacidade e segurança de dados robustas, a realização de auditorias internas para identificar e corrigir possíveis vulnerabilidades, o treinamento adequado dos colaboradores sobre as boas práticas de tratamento de dados pessoais, dentre outras medidas [LGPD 2018]. A nomeação de um Encarregado de Dados, responsável por supervisionar e garantir o cumprimento das normas da LGPD, também é crucial em vários contextos de empresas de software [LGPD 2018].

A adequação das empresas de software à LGPD está sendo impulsionada por diversos fatores, incluindo a atuação educativa, regulamentadora e punitiva da ANPD que buscou sancionar de forma pedagógica para incentivar as empresas a se adaptarem às normas da legislação. Além disso, parceiros comerciais, tanto nacionais quanto internacionais, estão exigindo cada vez mais a conformidade com a LGPD como requisito para estabelecer relações comerciais, impulsionando as empresas a realizarem as adaptações necessárias, como editais públicos de licitação [Souza 2022] [Carniato 2022].

Estudos acadêmicos também desempenham um papel importante ao oferecerem suporte teórico e prático para as empresas compreenderem e implementarem as melhores práticas em relação à proteção de dados pessoais [da Silveira 2022] [Cardoso 2023] [Ruhmann 2024]. Estes estudos muitas vezes trazem normas de segurança da informação, não restritas à proteção de dados pessoais, que estão cobrindo os aspectos técnicos de TI, como por exemplo padrões ISO (ex.: Família ISO 27000). Além disso, as empresas vêm adotando medidas técnicas e organizacionais para proteger os dados dos usuários, como a criptografia, o uso de Sistemas de Gestão de Segurança da Informação (SGSI) e a realização de avaliações de impacto à proteção de dados em projetos que envolvam o tratamento de informações pessoais.

A ANPD vem publicando guias e instruções normativas³ nos âmbitos jurídicos e tecnológicos que visam facilitar o processo de adequação das empresas à LGPD. No

³ <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes>

entanto, tais recursos ainda são considerados insuficientes e, muitas vezes, utilizam uma linguagem técnica jurídica que dificulta a compreensão das empresas de software sobre o que e como devem fazer para estar em conformidade legal. Essa falta de clareza e detalhamento nas orientações da ANPD pode representar um desafio adicional para as empresas, que precisam investir esforços extras para interpretar e implementar corretamente as diretrizes estabelecidas pela legislação de proteção de dados.

4. Análise de *compliance* LGPD na indústria de software

A avaliação da adequação das empresas de software à LGPD é um processo complexo que envolve múltiplas dimensões. Inicialmente, é essencial analisar se a empresa possui políticas e procedimentos internos que estejam alinhados com as diretrizes estabelecidas pela legislação de proteção de dados. Isso inclui a existência de uma política de privacidade clara e transparente, mecanismos para obtenção de consentimento dos titulares dos dados, medidas de segurança adequadas e a designação de um Encarregado de Dados, responsável por supervisionar e garantir o cumprimento das normas da LGPD. Além disso, é importante verificar se a empresa realiza auditorias internas periódicas para identificar e corrigir eventuais falhas ou vulnerabilidades. Por fim, a avaliação da adequação também deve considerar a capacidade da empresa de responder a solicitações dos titulares dos dados, como acesso, correção e exclusão de informações pessoais, bem como sua prontidão para lidar com incidentes de segurança e notificar a ANPD e os titulares em caso de violações à proteção de dados.

Esse diagnóstico de *compliance* da LGPD nas empresas de software pode ser aprimorado por meio de pesquisas que quantifiquem o número de empresas que estão em conformidade com a legislação, a realização de auditorias padronizadas e a verificação do nível de conformidade. Isto pode proporcionar *insights* valiosos sobre o status de adequação das organizações. É igualmente importante realizar uma contabilidade rigorosa dos incidentes de segurança enfrentados pelas empresas de software, a fim de compreender os desafios enfrentados e identificar áreas que precisam de maior atenção. Paralelamente, a análise jurídica das decisões administrativas e judiciais relacionadas à LGPD para empresas de software pode fornecer orientações jurídicas valiosas para o aprimoramento da conformidade.

Nesse sentido, existe uma proposta em construção de um **Modelo de Maturidade de Adequação Institucional à LGPD (MMAI-LGPD)**⁴, que tem o objetivo principal estabelecer uma estrutura e um conjunto de diretrizes para avaliar e aprimorar a conformidade das instituições com a LGPD. Este modelo está organizado em 5 níveis de maturidade, contendo 57 itens de inspeção, contemplando os âmbitos jurídicos, de segurança da informação e de governança. Ele foi estruturado tendo como base a LGPD, resoluções da ANPD, recomendações da ISO e de boas práticas internacionais no que tange à privacidade e proteção de dados pessoais.

Ele será auxiliado por um sistema computacional de suporte à implantação e auditoria. Sendo extensível e escalável para diferentes contextos, espera-se que a proposta sirva também como um arcabouço para (1) Governança de dados, (2) Atendimento ao titular do dados, (3) Gestão de incidente de segurança, (4) Implantação de controles de segurança da informação e (5) Elaboração de termos e políticas. Atualmente ele está em

⁴ <https://mmai-lgpd.dcx.ufpb.br/>

processo de avaliação e espera-se que seja uma ferramenta útil para as empresas identificarem seu progresso em relação aos requisitos da legislação.

AGRADECIMENTOS

Este trabalho é parcialmente financiado pelo INES 2.0 (www.ines.org.br), bolsa CNPq 465614/2014-0, bolsa FACEPE APQ-0399-1.03/17 e APQ/0388-1.03/14, bolsa CAPES 88887.136410/2017- 00. Sérgio Soares é parcialmente apoiado pela bolsa CNPq 306000/2022-9.

Referências

Autoridade Nacional de Proteção de Dados (ANPD). (2021). Resolução ANPD nº 1/2021, Aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados (alterado pela RESOLUÇÃO CD/ANPD Nº 4, DE 24 DE FEVEREIRO DE 2023), 28 de outubro de 2021, <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/regulamentacoes-da-anpd/resolucao-cd-anpd-no1-2021>.

Cardoso, D., & Cardoso, T. (2023). Adequação da LGPD via “Projetos Ágeis Scrum”. Boletim Do Gerenciamento, 35(35), 28-41. Recuperado de <https://nppg.org.br/revistas/boletimdoGerenciamento/article/view/731>.

Carniato, S. H. (2022). Revisão e atualização de contrato sob o prisma da privacidade e proteção de dados. Cadernos Jurídicos Da Faculdade De Direito De Sorocaba, 3(1), 95–106. Recuperado de <https://fadi.emnuvens.com.br/cadernosjuridicos/article/view/90>.

da Silveira, K. (2022). Segurança em Banco de Dados para Adequação a LGPD. In Anais do XXII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais, (pp. 278-287). Porto Alegre: SBC. doi:10.5753/sbseg.2022.223953.

Daryus (2023, 04 de janeiro). LGPD está fora da realidade de 80% das empresas no Brasil, diz estudo. FEBRABRAN TECH. <https://febrabrantech.febraban.org.br/blog/lgpd-esta-fora-da-realidade-de-80-das-empresas-no-brasil-diz-estudo>.

Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709, de 14 de agosto de 2018. 04/01/2023.

Mendes, Laura Schertel et al. Anuário do Observatório da LGPD da Universidade de Brasília: análise comparada entre elementos da LGPD e do GDPR. Brasília: Universidade de Brasília, Faculdade de Direito, 2023. v. 1. DOI: <https://doi.org/10.26512/9786500923988>.

Ruhmann Chou, E. N., Albano, C. J., & Almeida, P. H. (2024). Lei Geral de Proteção de Dados: uma análise da ISO 27701 como ferramenta de controle para LGPD. Revista Ifes Ciência , 10(1), 01-15. <https://doi.org/10.36524/ric.v10i1.2445>.

SEBRAE (2020, 11 de maio). Painel de Empresas Dashboard. SEBRAE. <https://datasebrae.com.br/totaldeempresas-11-05-2020/> .

Souza, Camila Aparecida Alves de. Os reflexos das leis protetivas de dados nos contratos. 2022. Monografia de Especialização (Especialização em Direito Contratual) - da Pontifícia Universidade Católica de São Paulo, São Paulo, 2022.