CONTROLE E CONSENTIMENTO: OS DESAFIOS DA IMPLANTAÇÃO DA LGPD NAS INSTITUIÇÕES FINANCEIRAS NO BRASIL E SUA GESTÃO DE RISCOS

CONTROL AND CONSENT: THE CHALLENGES OF IMPLEMENTING THE LGPD IN FINANCIAL INSTITUTIONS IN BRAZIL AND THEIR RISK MANAGEMENT

RAQUEL CESÁRIO BELTRÃO

RESUMO: Este artigo examina os desafios enfrentados pelas instituições financeiras na implantação da Lei Geral de Proteção de Dados (LGPD) no Brasil, cujo processo é complexo e desafiador. É crucial que as instituições financeiras estejam atentas às exigências da LGPD e atuem proativamente para garantir a confiança dos clientes e o fortalecimento da segurança cibernética. De forma concisa, a implantação da LGPD exige um compromisso firme com a conformidade legal e quanto à sua responsabilização, embora sejam passíveis de sanções caso não cumpram as disposições da LGPD. Isso pode incluir advertências, multas e até mesmo a proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados. A gestão de riscos está diretamente relacionada à implantação da LGPD nas instituições financeiras no Brasil, pois envolve a identificação, avaliação e mitigação dos possíveis riscos associados ao tratamento de dados pessoais. Dessa forma, é essencial que as instituições financeiras adotem uma abordagem ágil para garantir a eficácia da governança de dados. A presente pesquisa busca não apenas identificar os desafios existentes, mas também propor soluções adequadas para fortalecer a integridade dos sistemas de informação nas instituições bancárias. À medida que os bancos fortalecem seus sistemas, os fraudadores desenvolvem novas técnicas para contorná-las, desse modo, é pertinente analisar esse tema.

Palavras-chave: LGPD; Desafios; Instituições financeiras; Gestão de riscos.

ABSTRACT: This article examines the challenges faced by financial institutions in implementing the General Data Protection Law (LGPD) in Brazil, the process of which is complex and challenging. It is crucial that financial institutions are aware of LGPD requirements and act proactively to ensure customer trust and strengthen cybersecurity. Concisely, the implementation of the LGPD requires a firm commitment to legal compliance and accountability, although they are subject to sanctions if they do not comply with the provisions of the LGPD. This may include warnings, fines and even a partial or total ban on carrying out activities related to data processing. Risk management is directly related to the implementation of LGPD in financial institutions in Brazil, as it involves the identification, assessment and mitigation of possible risks associated with the processing of personal data. Therefore, it is essential that financial institutions adopt an agile approach to ensure effective data governance. This research seeks not only to identify existing challenges, but also to propose appropriate solutions to strengthen the integrity of information systems in banking institutions. As banks strengthen their systems, fraudsters develop new techniques to circumvent them, so it is pertinent to analyze this topic.

Keywords: LGPD; Challenges; Financial Institution; Risk management.

1. INTRODUÇÃO

Como começar a adequação à LGPD? Conhecer o negócio, os acionistas, colaboradores, em síntese, todos os stakeholders1. Avaliar os dados nas instituições financeiras e verificar se estão adequadamente protegidos, constatar as responsabilidades de todos os envolvidos, enumerar todas as possíveis situações de riscos, bem como as respectivas ações preventivas e corretivas, envolvendo toda estrutura institucional, no entanto, focando nas áreas mais sensíveis e definir um monitoramento e um procedimento.

Antes da implementação da LGPD, a preocupação com a privacidade e proteção de dados pessoais por parte das instituições financeiras no Brasil era, de fato, uma questão que nem sempre recebia a devida atenção. As instituições financeiras lidam diariamente com uma quantidade expressiva de dados sensíveis de clientes, incluindo informações financeiras, pessoais e transacionais. No entanto, a proteção adequada desses dados nem sempre era priorizada da maneira que se esperaria.

Nesse contexto, a promulgação da Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, representa um marco regulatório significativo, estabelecendo diretrizes claras para o tratamento de informações pessoais e impondo obrigações específicas às organizações que lidam com tais dados. A implementação da lei é necessária devido à falta de precedentes e para avaliar as ações e os gastos exigidos para cumprir os requisitos da nova legislação.

Na visão de Bruno Bioni, especialista em LGPD e GDPR, que é um dos principais autores nesse tema, enfatiza que a relação entre essas duas legislações é fundamental para entender a implementação da LGPD no Brasil:

> "O GDPR da União Europeia serviu como modelo e referência para a LGPD brasileira, uma vez que ambos os regulamentos compartilham objetivos semelhantes em relação à proteção de dados pessoais."2

O GDPR foi promulgado em 2016 e entrou em vigor em 2018, estabelecendo uma legislação abrangente e rigorosa para proteger os dados pessoais dos cidadãos da União Europeia. Seu escopo extraterritorial impactou empresas em todo o mundo que processam dados de cidadãos da UE, levando muitas organizações brasileiras a se prepararem para conformidade com seus requisitos.

[1] "Qualquer grupo ou indivíduo que pode afetar ou ser afetado pelos objetivos da organização" – R. Edward Freeman

[2] (Bioni, Proteção de Dados Pessoais: a função e os limites do consentimento, 2019)

No entanto, o contexto jurídico e cultural do Brasil exigiu adaptações significativas para que a LGPD fosse aprovada e implementada de forma eficaz. Diferentemente do GDPR, que é um regulamento diretamente aplicável em todos os Estados membros da UE, a LGPD precisou ser aprovada como uma lei ordinária devido à estrutura legal brasileira. Além disso, a LGPD incorporou certas peculiaridades do ordenamento jurídico brasileiro, como a criação da Autoridade Nacional de Proteção de Dados (ANPD) e a previsão de sanções administrativas específicas para infrações à legislação.

Apesar das diferenças formais entre o GDPR e a LGPD, seus objetivos essenciais são os mesmos: proteger os direitos fundamentais à privacidade e à proteção de dados pessoais. Ambas as legislações visam promover uma cultura de proteção de dados, responsabilizando as organizações pelo tratamento adequado das informações pessoais e garantindo o direito dos indivíduos sobre seus próprios dados.

Quando uma instituição financeira possui um alto nível de maturidade em relação à segurança de informação e gestão de riscos, o seu problema é menor do que o daquelas empresas em que tudo é feito “para auditoria”, sem nunca terem enfrentado um problema de vazamento de informações, ciberataque ou interrupção de negócios. Investir na construção de uma cultura de segurança sólida e na implementação de controles de segurança robustos é fundamental para mitigar riscos e proteger os interesses da instituição e de seus clientes.

Portanto, a abordagem deste artigo busca solucionar os desafios da LGPD e ter uma análise crítica das práticas atuais das instituições financeiras em relação ao tratamento de dados pessoais, identificando lacunas e propondo soluções inovadoras para a gestão do controle e consentimento exigidos pela legislação, explorando as complexidades da gestão de riscos em um ambiente regulatório em evolução e possíveis estratégias.

1 REVISÃO DE LITERATURA

1.1 Contexto histórico: Lei geral de proteção de dados

A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, foi promulgada em 14 de agosto de 2018 e passou a vigorar a partir de setembro de 2020. Inspirada nos princípios do Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, que entrou em vigor em maio de 2018, a LGPD representa um marco significativo no cenário brasileiro quanto à proteção e privacidade dos dados pessoais. A legislação visa estabelecer diretrizes claras e robustas para o tratamento de informações pessoais, alinhando o Brasil aos padrões internacionais de proteção de dados. (Roque, 2019).

Ao adotar conceitos e diretrizes semelhantes ao GDPR, a LGPD busca garantir que instituições financeiras, no qual é o foco desta pesquisa, adotem práticas transparentes, seguras e éticas no manuseio de dados dos indivíduos. Esse movimento reflete a crescente importância da privacidade digital e da segurança cibernética em um mundo cada vez mais conectado e dependente da tecnologia para as operações cotidianas.

Como destaca Ana Frazão, especialista em direito digital, “a LGPD é mais do que uma simples regulamentação; é um instrumento fundamental para garantir a privacidade e a segurança dos dados em um cenário cada vez mais digitalizado”. Ao revisar estudos anteriores sobre a implementação da LGPD em diferentes setores, torna-se evidente que as instituições financeiras enfrentam desafios específicos ao buscar conformidade com essa legislação, demandando estratégias e práticas adaptadas a sua complexa operação. (Frazão, 2019).

As instituições financeiras enfrentam desafios complexos relacionados à proteção dos dados sensíveis dos clientes, como informações financeiras e de identificação pessoal. Esse cenário demanda a implementação de medidas de segurança cibernética robustas para mitigar riscos de violações de dados e ciberataques. Além disso, garantir o consentimento claro e informado para o tratamento de dados pessoais torna-se imperativo, exigindo políticas e procedimentos claros que estejam em conformidade com a LGPD.

Item da Lei	GDPR	LGPD
Registro de atividades de processamento	Não obrigatório para empresas com menos de 250 funcionários	Não obrigatório para empresas com menos de 250 funcionários
Multas	Até 4% do faturamento (€ 20M)	Até 2% do faturamento (R$ 50M)
Requisição de direitos	Em até 30 dias, gratuidade opcional	Em tempo razoável, gratuita
Notificação obrigatória de incidentes	72 horas	Tempo razoável (a ser definido)
Agência reguladora	Definida	ANPD[1] (MP PROCON, outros)
DPO/ED[2]	Pessoa natural ou jurídica	Pessoa natural ou jurídica
Legítimo interesse	Mais restrito	Mais flexível
Dados anonimizados	Não são considerados pessoais em perfis	Podem ser considerados pessoais em perfis
Perfis comportamentais	Necessário causar impacto no titular dos dados	Sempre se considera causar impacto no titular dos dados
Transferências internacionais	Possível, com base no legítimo interesse, caso não seja frequente	Com consentimento específico, mesmo sem legítimo interesse
Dados de saúde	Não podem ser tratados mediante contrato	Podem ser tratados mediante contrato de prestação de serviço

Quadro 1 - Comparativo entre o GDPR e a LGPD

1 *ANPD: Autoridade Nacional de Proteção*

2 *DPO/ED: data protection officer/encarregado de dados.*

É crucial que a alta administração compreenda tanto os benefícios quanto os desafios da conformidade com a LGPD e o GDPR. Isso implica apresentar os riscos e oportunidades dessas regulamentações, garantir o apoio da gestão para os projetos de conformidade, designar um membro da diretoria como responsável pela LGPD e pelo GDPR, e integrar o gerenciamento de riscos de proteção de dados à estrutura corporativa de controle interno.

1.2 Surgimento e evolução legislativa bancária

No Brasil, leis como a Lei Complementar nº 105/2001 e a Lei Complementar nº 9.613/1998 desempenharam papéis fundamentais na história do sigilo bancário, estabelecendo diretrizes cruciais para a proteção das informações financeiras dos clientes. A primeira, ao regulamentar o acesso às informações bancárias e fiscais pela administração tributária e pela Receita Federal, definiu as condições em que as

autoridades fiscais poderiam ter acesso a dados bancários dos contribuintes, resguardando simultaneamente o sigilo bancário.

Já a Lei Complementar nº 9.613/1998 tratou da prevenção e combate à lavagem de dinheiro, estabelecendo procedimentos específicos para o sigilo de informações bancárias em casos relacionados a atividades suspeitas. Além disso, o Código Civil brasileiro também contribuiu para a proteção dos dados financeiros dos clientes ao determinar, em seus artigos 1.233 a 1.235, que os bancos só poderiam divulgar informações sobre as contas de um cliente em situações específicas, como por ordem judicial ou com o consentimento do titular da conta.

Essas leis representaram marcos importantes na história do sigilo bancário no país, fortalecendo a segurança e confidencialidade das informações bancárias dos cidadãos e estabelecendo parâmetros claros para o acesso e compartilhamento desses dados. Nos últimos dezoito anos, tais legislações impulsionaram mudanças significativas em relação à cibersegurança, termo amplamente mencionado nesta pesquisa.

Vale destacar as principais normativas que regem o setor bancário no Brasil que trazem a memória de eventos marcantes que moldaram o sistema financeiro nacional. O Banco Central do Brasil (BCB), instituído em 31 de dezembro de 1964, desempenha um papel central na regulação e supervisão das atividades financeiras, estabelecendo diretrizes abrangentes que tratam de requisitos de capital, liquidez e governança corporativa para que as instituições financeiras possam operar no país.

Paralelamente, a Comissão de Valores Mobiliários (CVM), fundada em 7 de dezembro de 1976, exerce uma função crucial na regulamentação e fiscalização do mercado de valores mobiliários no Brasil, incluindo as operações das instituições financeiras envolvidas nesse mercado, como bancos de investimento e corretoras de valores. Esses órgãos reguladores desempenham papéis fundamentais na garantia da estabilidade e eficiência do setor bancário brasileiro.

Historicamente, a evolução das operações bancárias começou com a introdução de computadores nas últimas décadas. Logo depois, nas décadas de 60/70, surgiram os caixas eletrônicos, permitindo clientes realizarem transações básicas fora do horário de funcionamento. Com o advento da internet, surgiu o “internet banking” que impulsionou a criação de novos sistemas.

A partir desse momento, com a criação e popularização dos smartphones, a evolução do sector bancário continuou a acelerar, com aplicações móveis, plataformas digitais de pagamentos, tecnologia blockchain, criptomoedas e a estimada “inteligência

artificial".

Com toda esta evolução tecnológica, tornou-se possível fazer pagamentos por aproximação e implementar o sistema Pix, uma inovação que completamente transformou o setor bancário, oferecendo um meio de pagamento rápido e eficiente, livre de quaisquer encargos por parte das instituições financeiras. Esta transição digital ganhou impulso com a crise pandêmica, que já se desenrolava de forma gradual anteriormente.

A legislação bancária também trouxe à tona a necessidade de uma cultura organizacional voltada para a proteção de dados, promovendo a conscientização e responsabilidade de todos os colaboradores em relação à segurança das informações pessoais. A interação entre a evolução da legislação bancária e o direito digital no contexto da LGPD reflete não apenas a necessidade de adaptação das instituições financeiras às novas demandas regulatórias, mas também a importância de se garantir a proteção dos direitos individuais dos clientes em um ambiente cada vez mais digitalizado e interconectado.

Assim, o cumprimento dos requisitos da LGPD não apenas fortalece a confiança dos consumidores, mas também contribui para a construção de um ecossistema bancário mais transparente, ético e seguro. A lacuna na legislação em relação à proteção de dados representa uma ameaça substancial tanto para os consumidores quanto para as instituições financeiras.

1.3 Gestão de Riscos

A fim de reduzir os riscos, surge a gestão de riscos, que de acordo com Vitoriano (2012)3, é conceituada como um conjunto de procedimentos que visam o equilíbrio entre os riscos e custos, compreendendo o planejamento, organização e controle para que possa ser de fato consolidado dentro das instituições, tanto financeiras, quanto as demais.

Quanto à gestão de riscos das instituições financeiras, Gil, Arima e Nakamura (2013)4 destacam que é fundamental nas atividades bancárias, pois os bancos trabalham diretamente com o risco: nas operações de crédito, gestão de recursos e atividades de tesouraria. Esta visão vai de encontro com o pensamento de Coimbra (2017)5, que destaca a importância do gerenciamento dos riscos operacionais nas instituições financeiras,

[3] VITORIANO, Bárbara Cristina. Gestão de risco – você sabe o que é? [S.l.]
[4] GIL, Antonio de Loureiro; ARIMA, Carlos Hideo; NAKAMURA, Wilson Toshiro. Gestão: controle interno, risco e auditoria. [livro eletrônico] São Paulo: 2013. 126 p.
[5] COIMBRA, Fábio. Riscos operacionais: estrutura para gestão em bancos.

tendo em vista seu potencial de perdas com este tipo de risco.

O risco, apesar de estar presente em todas as empresas, tem uma relevância maior quando se trata de instituições financeiras, já que estas atuam diretamente com o crédito, muitas vezes por meio de operações de alto risco de inadimplência. Para reduzir os prejuízos decorrentes dos riscos da atividade, o controle interno e a gestão de riscos se tornam ferramentas essenciais.

2. METODOLOGIA

Para a elaboração deste artigo, adotou-se uma abordagem exploratória com viés qualitativo, empregando pesquisa bibliográfica e documental. O principal objetivo consistiu em investigar a proteção de dados pessoais e a aplicação da Lei Geral de Proteção de Dados (LGPD) no contexto atual das instituições financeiras no Brasil. Além disso, buscou-se desenvolver diagramações para modelos de dados, utilizando aplicações conceituais metodológicas.

Neste contexto, também foram consideradas as práticas de gestão de riscos relacionadas à implementação da LGPD, visando compreender os desafios enfrentados pelas instituições financeiras. As observações quanto à proposta e aplicação dos estereótipos nos modelos utilizados foram embasadas no estudo dos conceitos apresentados, incorporando cenários hipotéticos considerados mais alinhados ao contexto do estudo.

Essa abordagem permitiu não apenas explorar a conformidade com a LGPD, mas também analisar de forma mais ampla os potenciais riscos envolvidos na gestão de dados pessoais pelas instituições financeiras, contribuindo para uma compreensão abrangente dos desafios enfrentados por essas organizações.

Para a condução deste estudo, optou-se também por uma abordagem metodológica que visa contrastar as perspectivas apresentadas por determinadas obras do tema, dentre elas dois livros dos principais autores renomados no campo da Lei Geral de Proteção de Dados (LGPD). Os livros selecionados para esta análise são "Os 10 Mandamentos da LGPD - Como Implementar a Lei Geral de Proteção de Dados em 14 Passos", escrito por Fernando Marinho, um profissional especializado em tecnologia, e "Empresas e Implementação da LGPD – Lei Geral de Proteção de Dados Pessoais", coordenado por Tarcísio Teixeira, Advogado especializado em Proteção de Dados e Direito Digital, Doutor e Mestre em Direito Empresarial pela USP.

A escolha dessas fontes se baseia na necessidade de compreender e contrastar diferentes abordagens e insights sobre a implementação e os desafios práticos relacionados à LGPD. Fernando Marinho traz uma perspectiva centrada na aplicação prática da LGPD, oferecendo orientações detalhadas e passos concretos para a conformidade com a lei, enquanto Tarcísio Teixeira aborda a LGPD sob uma ótica mais jurídica, explorando as implicações legais e normativas da legislação.

A análise comparativa entre os dois autores será realizada por meio de uma abordagem sistemática, que envolverá a identificação e a comparação de conceitos-chave, recomendações e evidências apresentadas em ambos os livros. Essa análise permitirá uma compreensão mais abrangente das diferentes perspectivas sobre a LGPD, destacando áreas de convergência, divergência e possíveis complementaridades entre as visões de Marinho e Teixeira.

Por meio dessa metodologia de contraposição de autores, almeja-se contribuir para uma visão mais holística e informada sobre os desafios e oportunidades associados à implementação da LGPD, fornecendo insights valiosos tanto para profissionais da área de tecnologia quanto para especialistas jurídicos e demais interessados na temática.

3. APRESENTAÇÃO DOS RESULTADOS

4.1 Delegação de um DPO nas Instituições Financeiras

No início deste capítulo, será abordado de forma clara e objetiva os principais resultados obtidos na implantação da LGPD, e inicia-se com a descoberta e designação do responsável pelo assunto no contexto da implantação da LGPD. Este ponto é essencial não apenas para cumprir as exigências legais, mas também para estabelecer uma base sólida para o controle e gestão eficazes dos dados pessoais nas instituições financeiras. A designação do encarregado de dados, ou DPO (Data Protection Officer), é um marco significativo no processo de conformidade com a LGPD e do GDPR, que exige uma abordagem estratégica e integrada para lidar com os desafios decorrentes da proteção de dados.

Quando questionado sobre o perfil desse profissional, é comum destacar que sua principal habilidade deve ser a capacidade de interagir entre as áreas de negócios, jurídica e de tecnologia da informação/sistemas de informação (TI/SI), com o objetivo de atender aos requisitos da LGPD. Nesse sentido, sua competência primordial deve transcender o conhecimento tradicional, assumindo o papel de integrador de diferentes áreas de

conhecimento para alcançar os resultados desejados.

É imprescindível destacar que a necessidade de habilidades integrativas para o DPO, independentemente de sua formação como advogado ou técnico de tecnologia, pode gerar discussões e conflitos nas instituições financeiras. Essas questões surgem devido às distintas perspectivas e competências requeridas para o cargo, bem como às discordâncias sobre qual formação é mais adequada para desempenhar efetivamente as responsabilidades relacionadas à conformidade com a legislação de proteção de dados.

Conforme análise importante do escritor Fernando Marinho6, destaca-se:

> Sempre cito o comentário de um especialista português em um seminário de que participei quando lhe perguntaram sobre o "perfil de um DPO". Ele sorriu e disse: "Não existe um perfil único para DPO, porque cada empresa possui uma realidade e características próprias. Os profissionais que assumiram essa função na Europa estão aprendendo seu ofício na rotina do dia a dia". Enquanto isso, no Brasil, fantasiamos a respeito de um papel que atesta que passamos em uma prova ou concluímos um curso, como se isso comprovasse competência. Nenhum diploma universitário comprova competência. Mal comprova que o aluno cumpriu o programa de ensino e que demonstrou pelo menos x% de rendimento. Fato facilmente evidenciado por alguns profissionais diplomados que mal redigem um relatório ou aqueles que penalizam seus pacientes por erros médicos."

4.2 Designação de Comitê e suas exigências

A criação de um comitê para atuar em assunto que envolve a privacidade também é uma recomendação da LGPD, porém, deve-se levar em conta o seguinte contexto: um grupo de trabalho para atuar no projeto de implementação deve ter um perfil específico para atender ao objetivo do projeto, ou seja, a implementação da conformidade à LGPD. Já um comitê definido para tratar do assunto privacidade pode ter outro perfil, com objetivo mais estratégico.

Desde a promulgação da LGPD em agosto de 2018, as organizações têm enfrentado pressões crescentes para garantir a conformidade com as disposições da lei, que entrou em vigor em setembro de 2020. Essa legislação representa um marco importante na proteção da privacidade dos dados no Brasil e impõe novos desafios às instituições financeiras, que lidam diariamente com grandes volumes de informações sensíveis de clientes.

Para estabelecer um comitê eficaz de conformidade com a LGPD, as instituições financeiras precisam recrutar profissionais com expertise multidisciplinar, capazes de interpretar e aplicar os requisitos da lei de forma eficiente. Conhecimentos em direito, tecnologia da informação e gestão de negócios são essenciais para garantir uma

[6] (Fernando, pág. 104, 2020)

abordagem abrangente e integrada à proteção de dados. Como apontado por Fernando Marinho em seu livro "Os 10 Mandamentos da LGPD"7:

> "A criação de um comitê de conformidade exige uma visão estratégica e investimento em recursos humanos e financeiros para garantir o sucesso das atividades relacionadas à privacidade e proteção de dados. Essa abordagem não se limita apenas à implementação de medidas técnicas, mas também à promoção de uma cultura organizacional voltada para a segurança e privacidade dos dados, fomentando a conscientização e a responsabilidade em todos os níveis da instituição."

4.3 As multas e penalidades elencadas pela LGPD

A LGPD representa importante progresso no tratamento de dados, uma vez que dispõe sobre a responsabilização solidária, no âmbito civil e administrativo, dos agentes de tratamento de dados que não cumprem com os preceitos descritos na referida legislação, por meio de programa de governança em privacidade e boas práticas (que também se pode convencionar como um Programa de Compliance).8

Aplicação de pesadas multas além na aplicação de outras sanções administrativas como publicização da infração, bloqueio ou eliminação de dados e suspensão ou proibição do exercício de atividades, podendo, assim, gerar impacto à reputação da empresa, assim como perda de vantagem competitiva. Ainda, em seu artigo 529, § 1o, prevê critérios de razoabilidade e proporcionalidade para eventuais punições. Denota-se a importância de boas práticas e governança bem estruturada, efetiva e documentada, sob a perspectiva da LGPD.

Poderá ser considerada como um dos critérios para fins da aplicação das cominações administrativas previstas nesta lei, caso algum ato lesivo venha a ser efetuado, ou seja, não afasta completamente a aplicação da penalidade, mas se a instituição financeira conseguir demonstrar que possui um efetivo Programa de Compliance, isto pode implicar atenuante da penalidade.

Em entendimentos jurisprudenciais, os dirigentes somente serão punidos quando tiverem ciência inequívoca das práticas delituosas, bem como tenham tido condições de evitá-las. Conforme dispõe o artigo 1310, parágrafo 2º do Código Penal que descreve a

[7] (Fernando, pág. 104, 2020)
[8] VIGLIAR, José Marcelo M. LGPD e a Proteção de Dados Pessoais na Sociedade em Rede. Grupo Almedina, pág. 221.
[9] § 1º "As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto..."
[10] Art. 13 - O resultado, de que depende a existência do crime, somente é imputável a quem lhe deu causa. Considera-se causa a ação ou omissão sem a qual o resultado não teria ocorrido. (Redação dada pela Lei nº 7.209, de 11.7.1984)

conduta por omissão, onde aquele que tem o dever de agir tem a obrigação de cuidado, proteção ou vigilância. Esta obrigação também á observada nos incisos I e II, do artigo 42 do Decreto 8.420/2015 que regulamenta e Lei Anticorrupção. (Nohara e Pereira, 2018, p. 215).

Além disso, essa condição é uma forma educativa e de incentivo às organizações de adotarem um programa de governança. Assim, pode-se dizer que estes foram importantes avanços na legislação brasileira para estimular Programas de Compliance nas empresas. A LGPD, reforçando o informado anteriormente, dispõe sobre a responsabilização dos agentes de tratamento de dados. Por isso, é imprescindível que a alta gestão da empresa apoie o Programa de Compliance, além de considerar os parâmetros de comprometimento de todos e de existência de padrões de conduta, políticas e código de ética.

Por exemplo, as multas podem chegar a até 2% do faturamento da empresa, com um limite máximo de 50 milhões de reais por infração. Portanto, as organizações precisam estar cientes do potencial impacto financeiro e de reputação que as multas podem acarretar, o que as torna uma preocupação central na implementação eficaz da LGPD.

Em face dessas penalidades, as empresas são incentivadas a investir em políticas e práticas de proteção de dados robustas, bem como em programas de treinamento para funcionários, a fim de evitar violações e proteger os dados pessoais de maneira adequada. As multas impostas pela LGPD são aplicáveis em casos excepcionais de falha grave, portanto, o adiamento da conformidade com a lei não representa um benefício para as empresas.

A postura reativa diante de um vazamento de dados pode resultar em sérios danos à imagem e reputação da organização, afetando seu valor de mercado e levando à perda de clientes para a concorrência, o que consequentemente reduziria sua lucratividade.

4. DISCUSSÃO

Ao confundir o conceito de privacidade com confidencialidade, as instituições financeiras têm delegado a missão de conduzir esse assunto às áreas de tecnologia e jurídico, com algumas exceções para compliance. Além desse ponto de debate, existem questões controvérsas e fundamentais, levantadas no livro “Os 10 Mandamentos da LGPD**”,** por Fernando Marinho11 e que ajudam as instituições financeiras a melhorar a

§ 2º - A omissão é penalmente relevante quando o omitente devia e podia agir para evitar o resultado.
[11] MARINHO, Fernando. Os 10 Mandamentos da LGPD. Pág. 97, Ed. Atlas, 2020.

conformidade com a legislação e a proteção dos dados pessoas dos clientes, são elas:

1) “Não estar disposto a investir no assunto”: Tentar resolver um problema começando pela economia é um dos fatores de risco mais comuns em qualquer tipo de empreendimento. Já vi empresas desejarem economizar, tentando dar utilidade a um conjunto de ativos de TI para atendimento a um determinado objetivo ou projeto. O trabalho que dá adaptar o que se tem para o que se deseja geralmente acaba saindo mais caro do que adquirir algo criado especificamente para o que se quer.

2) “Querer o mais barato”: Eu sempre comento nas minhas turmas que ninguém escolhe uma babá (ou um dentista) pelo preço. Quando buscamos a solução para algo a que damos valor, tentamos adquirir a melhor solução possível de acordo com nosso orçamento. O que, obviamente, não significa o mesmo que o menor preço. Existe uma teoria estudada pelo Massachusetts Institute of Technology (MIT), chamada “arbitrariedade coerente”, cuja definição na Wikipedia é a seguinte: “consumidores são sensíveis a diferenças relativas, mas não aos preços absolutos, o que implica a impossibilidade de determinar corretamente o preço daquilo que avaliam.

   As pessoas julgam preços com base em pistas, algumas úteis (como o preço por quilograma e a inflação), mas a maioria não (como o tamanho da embalagem e o preço relativo)”. Em outras palavras: se você decidiu que está na hora de comprar uma nova calça jeans, o referencial de “caro” ou “barato” será definido pelo seu saldo no banco, ou limite do cartão de crédito, não pelo verdadeiro valor da calça. Logo, tentar avaliar o preço de um serviço de consultoria especializada pode acabar se tornando um grande problema, se o seu objetivo é resolver o problema apenas pelo menor valor.

3) “Deixa que eu faço”: Seja porque temos colaboradores de alto padrão intelectual ou consideramos que não haja assunto que nosso pessoal não consiga dominar, simplesmente entregamos nas mãos dos nossos funcionários a responsabilidade por resolver os problemas da empresa. Eu até concordo com essa teoria, se o assunto em pauta tiver estreita relação com o negócio da empresa ou com a formação profissional do funcionário. O grande problema da LGPD é que se trata

de um assunto novo, sem referência passada, orientada por uma Lei que não detalha muita coisa.

4) "Comprar uma solução completa": Essa é a famosa "bala de prata", que mata desde formigas até baleias-azuis (apesar desta ser uma espécie protegida). Essa solução que "assovia, chupa cana e escova os dentes ao mesmo tempo" provavelmente foi criada para um objetivo e seu desenvolvedor ou proprietário descobriu que, após um anjo abrir sua mente, ela também resolve o problema de conformidade à LGPD. Só é preciso fazer uma bela apresentação e criar um discurso de vendas campeão.

   Tal como a "panaceia universal" (remédio criado pelos alquimistas capaz de curar todos os males), ou, como já citei, o snake oil (medicamento oferecido no Velho Oeste norte-americano que curava de tudo), algumas empresas pensam que como é inevitável gastar para resolver esse assunto, que esse gasto seja com algo que resolva definitivamente todos os problemas. Infelizmente só descobrem que se trata de algo que não resolve o problema quando é tarde demais (depois de ter pago e quando o prazo para conformidade estiver perigosamente próximo).

5) "Copiar e colar": Não existe coisa pior do que a falta de profissionalismo de alguém que espera um trabalho ficar pronto para poder copiar, ajustar e dizer que está adequado. É o famoso "para inglês ver" e acontece muito com o Plano de Continuidade de Negócios (PCN) e Planos de Crise. Entretanto, cabe a ressalva de citar que, no contexto da Lei, existem mecanismos de controle que devem ser implementados e que não são simples papéis escritos.

É possível copiar e colar documentos como políticas de segurança, de privacidade ou de conduta, ajustando-se os atores para pertencerem ao ambiente da empresa que copiou. Porém, muito mais difícil será criar e manter as evidências de cada um dos itens que são abordados nesses documentos e que, a princípio, foram criados para outra estrutura. Muitas vezes, o texto pode não se adequar ao segmento ou mercado do novo proprietário. Neste caso, se houver um incidente de vazamento e for necessário apresentar as evidências de conformidade, o problema será muito maior que a falta de ética.

Consequentemente, assegurar a conformidade das instituições financeiras com as disposições da LGPD é de extrema importância, e o livro "Os 10 Mandamentos da LGPD"

oferece diretrizes valiosas nesse sentido. É crucial reconhecer que tentar economizar inicialmente pode acarretar custos significativos no longo prazo.

Além disso, é fundamental compreender que optar pela solução mais barata nem sempre é a abordagem mais vantajosa, pois a qualidade muitas vezes supera o preço. A delegação exclusiva da responsabilidade pela conformidade da LGPD aos funcionários é arriscada, dada a complexidade do assunto. A cautela também é recomendada ao evitar soluções "mágicas" que prometem uma conformidade fácil e completa, pois tais abordagens podem resultar em desperdício de recursos e falta de eficácia.

5. CONSIDERAÇÕES FINAIS

À luz de tudo que foi discutido, fica claro que a Lei Geral de Proteção de Dados (LGPD) abriu portas para uma nova era no setor bancário, permitindo que o processamento de dados aconteça de maneira mais segura, justa e ordenada. A LGPD não deve ser vista como um instrumento de punição rígida, mas sim como um marco de transformação no Direito Brasileiro, capaz de fortalecer e modernizar um universo já amplamente influenciado pelas relações digitais entre indivíduos e empresas.

Em conclusão, a implantação o da LGPD nas instituições financeiras no Brasil é um processo desafiador, mas essencial para garantir a segurança e a confiança dos clientes. A abordagem estruturada da LGPD, juntamente com a nomeação de um DPO e a formação de comitês dedicados, reforça a importância de uma gestão de riscos eficaz. Embora as multas e penalidades elencadas pela LGPD representem um mecanismo de controle, elas também incentivam as instituições a adotar práticas mais robustas de proteção de dados.

Ao investir em segurança, promover transparência e cultivar uma cultura organizacional orientada para a proteção de dados, as instituições financeiras podem não apenas cumprir a LGPD, mas também diferenciar-se no mercado por sua abordagem ética e responsável. Isso não apenas reduz o risco de penalidades, mas também fortalece a reputação da instituição e cria uma vantagem competitiva no setor financeiro cada vez mais digital e centrado no cliente.

O futuro do setor bancário dependerá da capacidade de adaptação e inovação no âmbito da proteção de dados. As instituições financeiras devem continuar a aprimorar suas práticas para atender aos requisitos da LGPD, fortalecendo assim sua relação com os clientes e garantindo a conformidade legal. Este estudo mostrou que, ao adotar uma

abordagem proativa e comprometida, o setor bancário pode transformar os desafios impostos pela LGPD em oportunidades para um futuro mais seguro e transparente.

REFERÊNCIAS:

BIONI, Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. 2ª ed. São Paulo: Editora Revista dos Tribunais, 2019.

COIMBRA, Fábio. Riscos operacionais: estrutura para gestão em bancos. São Paulo: Saint Paul, 2017. 146 p.

DWORKIN, Ronald. Levando os Direitos a Sério. São Paulo: Martins Fontes, 2010.

FILHO, V. M., CERQUEIRA, A. R. Compliance: Como Implementar na Prática. Editora Atlas, 2020.

FONSECA, Edson Pires da. LGPD em CASOS. Hotmart, 2021. FRAZÃO, A. Direito Digital. Saraiva, 2014.

GIL, Antonio de Loureiro; ARIMA, Carlos Hideo; NAKAMURA, Wilson Toshiro. Gestão: controle interno, risco e auditoria. [livro eletrônico] São Paulo: Abril de 2024. 126 p.

MARINHO, Fernando. Os 10 Mandamentos da LGPD. Ed. Atlas, 2020. MALDONADO, Viviane Nóbrega (Coord.). Lei Geral de Proteção de Dados Pessoais – Manual de Implementação. São Paulo: Editora Revista dos Tribunais, 2019.

NOHARA, Irene Patrícia; Pereira, Flávio de Leão Bastos (coord.) et al. Governança, compliance e cidadania. São Paulo: Thomson Reuters Revista dos Tribunais, 2018.

SENADO FEDERAL. Lei Geral de Proteção de Dados Pessoais entra em vigor; Brasilia. Disponível em: https://www12.senado.leg.br/noticias/materias/2020/09/18/lei-geral-deprotecao-de-dados-entra-em-vigor. Acesso em: 10 de abril de 2024.

TEIXEIRA, Tarcisio. (coord.). Empresas e implementação da LGPD – Lei Geral de Proteção de Dados Pessoais. Salvador: Juspodivm, 2021.

TEIXEIRA, Tarcisio. Os benefícios da adequação à LGPD para o seu comércio eletrônico. Disponível em: https://www.ecommerce-brasil.com.br/artigos/os-beneficios-da-adequacao-a-lgpd-para-o-seu-comercio-eletronico. Acesso em: 10 de abril de 2024.

VIGLIAR, José Marcelo M. LGPD e a Proteção de Dados Pessoais na Sociedade em Rede. Grupo Almedina, 2022. E-book. ISBN 9786556276373.

VITORIANO, Bárbara Cristina. Gestão de risco – você sabe o que é? [S.l.], 2012. Acesso em: 29 de abril de 2024.