doi.org/10.51891/rease.v9i10.12206

VIOLAÇÃO DE DADOS PESSOAIS EM INSTITUIÇÕES BANCÁRIAS: A IMPORTÂNCIA DO *COMPLIANCE* COMO MEIO DE CONTROLE INTERNO

Leticia Passinho Silva[1]
Thyara Novais[2]

RESUMO: O presente artigo aborda a crescente preocupação com a violação de dados pessoais em instituições bancárias, destacando a importância do *compliance* como meio de controle interno para mitigar tais ameaças. A pesquisa fundamenta-se em um extenso levantamento bibliográfico que inclui legislações pertinentes, doutrinas especializadas, artigos científicos e análises de plataformas digitais. O objetivo primordial é contribuir para o debate sobre a proteção de dados pessoais dos usuários, fornecendo insights valiosos sobre a necessidade de medidas efetivas para garantir a privacidade e a segurança dos dados coletados. O artigo enfatiza a urgência de uma fiscalização rigorosa para coibir possíveis abusos e violações da lei, considerando as implicações legais e éticas envolvidas. Ao explorar a interseção entre *compliance*, proteção de dados e fiscalização, a pesquisa busca não apenas identificar os desafios existentes, mas também propor soluções proativas para fortalecer a integridade dos sistemas de informação nas instituições bancárias, promovendo assim um ambiente mais seguro e confiável para os clientes e usuários em geral.

Palavras-chave: *Compliance*. Dados Bancários. Instituições Financeiras. Lei Geral de Proteção de Dados. Violação Dados Pessoais. Controle Interno.

1. INTRODUÇÃO

Num mundo onde a informação é o ativo mais valioso, a proteção dos dados pessoais emerge como uma necessidade premente para garantir a confiança e a segurança nas transações digitais. Instituições bancárias, detentoras de vastos volumes de dados sensíveis, enfrentam desafios significativos na salvaguarda dessas informações contra ameaças cada vez mais sofisticadas. O advento da era digital e a proliferação de plataformas online intensificaram a exposição dos dados pessoais a riscos, tornando imperativa a implementação de estratégias eficazes de proteção.

Ao considerarmos o cenário brasileiro, no qual a proteção de dados pessoais ganha destaque com a promulgação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), as palavras de Coelho (2018, s.p) ressoam: "A proteção de dados tornou-se um pilar fundamental para a preservação dos direitos individuais na era digital". A legislação brasileira, inspirada em princípios internacionais, reforça a necessidade de atenção

[1]Discente do curso de Direito da Faculdade de Ilhéus, Centro de Ensino Superior, Ilhéus, Bahia.
[2] Docente do curso de Direito da Faculdade de Ilhéus, Centro de Ensino Superior, Ilhéus, Bahia.

=

redobrada por parte das instituições bancárias para assegurar a conformidade e a integridade na gestão de dados pessoais.

Neste contexto, a presente pesquisa visa explorar a problemática da violação de dados pessoais em instituições bancárias, concentrando-se na necessidade premente de adotar medidas de *compliance* como meio de controle interno. Como destacado por Warren e Brandeis (1890,s.p), 'o direito à privacidade é o direito de ser deixado em paz'. Esta máxima ganha nova relevância no ambiente contemporâneo, onde violações de dados comprometem não apenas a privacidade, mas também a confiança essencial para o funcionamento saudável do sistema financeiro.

Esta pesquisa, fundamentada nas contribuições teóricas de autores brasileiros, busca não apenas examinar a vulnerabilidade dos dados pessoais nas instituições bancárias, mas também destacar a relevância do *compliance* como meio essencial de controle interno. Ao promover essa discussão, almejamos não apenas contribuir para o arcabouço acadêmico sobre o tema, mas também fornecer subsídios práticos para a efetiva implementação de medidas que assegurem a privacidade e a segurança dos dados coletados, em consonância com os preceitos legais e éticos que regem essa questão no contexto brasileiro.

O artigo apresentado busca também trazer novas perspectivas para o campo do Direito Digital, especificamente no que tange ao banco de dados de usuários e clientes de instituições bancárias. A dinâmica atual, impulsionada pela Revolução Digital, está no centro de um dos temas mais debatidos na sociedade contemporânea, que é a gestão e exploração de um recurso que tem se tornado cada vez mais valioso nas últimas décadas: as bases de dados que abrigam informações pessoais.

O artigo proposto será estruturado em seções que abordarão aspectos fundamentais relacionados à violação de dados pessoais em instituições bancárias, concentrando-se em diferentes perspectivas e contextos. A seção de Fundamentação Teórica explorará o surgimento do Direito Digital, analisando seu desenvolvimento ao longo do tempo e sua relevância no cenário atual. Além disso, examinará a história e a evolução legislativa bancária, delineando as mudanças normativas que moldaram o ambiente financeiro. A digitalização dos bancos e o surgimento de fintechs serão considerados como fatores preponderantes na transformação do setor, destacando as implicações dessa revolução tecnológica. O *compliance* e sua aplicação nas instituições bancárias serão discutidos como instrumento vital para assegurar a conformidade com as leis e normas pertinentes,

especialmente no que se refere à proteção de dados pessoais.

A seção também se aprofundará no tema do Controle Interno, delineando sua importância na gestão eficaz da segurança da informação. Por fim, o artigo explorará aspectos relevantes da Resolução CMN nº4.968/2021, analisando como essa normativa contribui para o fortalecimento das práticas de segurança e *compliance* no âmbito bancário, proporcionando uma visão abrangente e atualizada sobre a proteção de dados em instituições financeiras.

A metodologia adotada nesta pesquisa baseia-se em um rigoroso levantamento bibliográfico, abrangendo legislações atuais, doutrinas jurídicas especializadas, artigos científicos relevantes e análises de plataformas digitais. Através dessa abordagem, busca-se oferecer uma análise aprofundada da importância do *compliance* como instrumento fundamental para a proteção dos dados pessoais em instituições bancárias, além de contribuir para o debate acadêmico sobre a urgência de medidas efetivas e fiscalização rigorosa para salvaguardar os direitos dos usuários e evitar abusos e violações da lei.

Este artigo tem por objetivo contribuir para o debate sobre a proteção de dados pessoais dos usuários, demonstrando a importância da adoção de medidas efetivas para garantir a privacidade e a segurança dos dados coletados, bem como a necessidade de uma fiscalização rigorosa para coibir possíveis abusos e violações da lei. Buscar-se-á uma compreensão clara e precisa dos principais aspectos envolvidos no tratamento de dados pessoais, saber se há pessoas capacitadas e especializadas envolvidas no processo.

2. FUNDAMENTAÇÃO TEÓRICA

2.1 Surgimento do Direito Digital

Ao iniciar o conceito de proteção de dados e, acima de tudo, a origem da lei que rege os dados dos usuários, é necessário antes fazer uma breve jornada no tempo, a fim de compreender e examinar o seu surgimento. Na Constituição Federal de 1988 já havia disposição em seu artigo 5ª, inciso X, o conceito da inviolabilidade da vida privada, mas não havia expressão direta da privacidade no aspecto digital.

Posteriormente, o artigo LXXIX foi adicionado por meio de uma Emenda constitucional (EC nº 115/2022), garantindo o direito à segurança das informações pessoais, incluindo no âmbito digital, consolidando assim a proteção de dados como um direito fundamental. Segundo Frazão (2014):

> O Direito Digital é uma vertente do Direito que abrange as relações jurídicas

> estabelecidas no ambiente virtual, tratando das questões legais relacionadas à sociedade da informação e às novas tecnologias".

Diante do conceito acima, faz-se necessário a imersão num breve contexto histórico do surgimento do direito digital. Destaca-se para três datas, que foram o ponto crucial de divisão para que hoje possamos falar sobre o assunto.

Antes do século XIX, a privacidade não tinha um espaço como direito autônomo, mas sim, subsidiário da honra e da propriedade. Ao final desse mesmo século, com o surgimento e o avanço das tecnologias, *Warren e Brandeis* publicaram na *Harvard Law Review,* o artigo *The Right to Privacy*, que trouxe uma visão avançada no que se refere a privacidade, pois ao defender a inviolabilidade pessoal da intimidade, trouxe autonomia ao direito *a quo*.

A internet surgiu em meados dos anos 60, criada por militares durante a guerra fria. Foi durante a Segunda Guerra Mundial que os EUA percebem mais do que nunca que precisariam de tecnologia para vencer a guerra, e desta maneira, reunindo pesquisadores, num projeto chamado *alendure,* tinha como objetivo quebrar o código alemão. Ao final da Segunda Guerra, ao assistir seus aliados vencedores, os EUA continuaram sua linha de pesquisa tecnológicas, que se chamou posteriormente de internet.

O surgimento da internet representou uma revolução na forma como as sociedades contemporâneas se relacionam, comunicam e compartilham informações. Nesse contexto, Luiz Edson Fachin, jurista e professor brasileiro, destaca que "a internet trouxe consigo uma transformação paradigmática nas relações sociais, comerciais e jurídicas, desencadeando uma nova era marcada pela instantaneidade da comunicação e pela globalização da informação" (Fachin, 2012, p. 45). A citação de Fachin enfatiza a magnitude das mudanças trazidas pela internet, indo além dos aspectos técnicos para ressaltar as implicações sociais e jurídicas desse fenômeno.

Dentro desse contexto, tem sido dito que “a informação é o (novo) elemento estruturante que (re) organiza a sociedade tal como o fizeram a terra, as máquinas e a eletricidade bem como os serviços, respectivamente, nas sociedades agrícolas, industrial e pós-industrial” (Bioni, 2019).

Após sofrer um ataque contra o Japão em 1941, os Estados Unidos intentam decentralizar o poder, com o uso da nova tecnologia chamada internet, para que assim possa governar de diversas partes do Estado, fazendo grandes investimentos nesta tecnologia, que

posteriormente seria comercializada. Com o passar do tempo e o governo em busca de se manter alerta para uma nova guerra, passou a utiliza-la para a *cyber* espionagem.

Deve-se considerar também o acontecimento que marcou o mundo no dia 11/09/2001, o qual os Estados Unidos sofreram o ataque às torres gêmeas, dessa vez contra um inimigo invisível. Este dia se tornou uma marco na vida dos americanos que renunciaram subjetivamente a privacidade em favor de sua segurança. Por haver então esse compartilhamento de informação entre governos, foi se criando um clima de desconfiança entre os países.

O fenômeno dos vazamentos de dados e o surgimento de novos profissionais no campo da cibersegurança, muitas vezes referidos como "crackers", destacam-se como características marcantes desta era digital. Conforme ressaltado por Solove (2007, p. 112), "o crescente número de incidentes de vazamento de dados ressalta a vulnerabilidade crescente das informações pessoais na era digital". Esses vazamentos, que afetam empresas e indivíduos, desencadeiam uma série de desafios para a segurança da informação e a proteção da privacidade. Ao mesmo tempo, o surgimento de profissionais especializados em segurança cibernética evidencia a necessidade premente de expertise para combater ameaças digitais. Esses especialistas, muitas vezes chamados erroneamente de crackers, desempenham um papel crucial na proteção de dados e na mitigação de riscos associados à *cibersegurança*[3].

Dessa forma, é possível compreender que a maneira como as empresas lidam com a privacidade dos dados dos consumidores que a fornecem, pode se tornar um ponto de vantagem competitiva e vantajosa para os negócios.

A União Europeia, como uma das principais instituições da UE responsáveis por promover a cibersegurança, através da ENISA (Agência Europeia para a Segurança das Redes e da Informação), ao perceber a proliferação de violações e manobras realizada pelo Estados Unidos, adota medidas para controlar seus próprios dados e da sua população. Surge então o regulamento Europeu, chamado de Regulamento Geral sobre a Proteção de Dados (GDPR) 2018/1725, que visa proteger dados pessoais, estabelecendo regras relativas a

[3] A cibersegurança refere-se às práticas, técnicas e medidas adotadas para proteger sistemas, redes e dados contra ameaças digitais. Ela envolve a implementação de estratégias para prevenir, detectar, responder e recuperar-se de incidentes de segurança cibernética. O objetivo fundamental da cibersegurança é garantir a confidencialidade, integridade e disponibilidade das informações em ambientes digitais.

tratamento de dados, que posteriormente será inspiração para a Lei Geral de Proteção de Dados. Esse regulamento tem relevância pois transcende as fronteiras da UE, pois influenciou muitos países e organizações em todo o mundo a revisar e fortalecer suas próprias leis e práticas de proteção de dados. O Brasil, por exemplo, implementou sua própria Lei Geral de Proteção de Dados (LGPD), inspirada em grande parte no GDPR, para fornecer uma estrutura abrangente para o tratamento de dados pessoais.

2.2 A história e a evolução legislativa bancária

Seguindo no contexto histórico legislativo, é importante ressaltar que as Instituições Financeiras têm sido regidas por uma lei específica desde 2001, que aborda o tratamento de dados de seus clientes e estabelece a obrigação de preservar o sigilo das transações financeiras confiadas a cada instituição. Conhecida como Lei Complementar 105, datada de 10 de janeiro de 2001, a Lei do Sigilo Bancário é o principal marco normativo no que diz respeito à privacidade para bancos e outras empresas listadas em seu artigo 1º.

Durante os últimos dezoito anos, essa legislação tem impulsionado mudanças significativas em relação à segurança da informação e cibersegurança, termos amplamente mencionados na atualidade

A introdução de novas tecnologias modifica a forma como as instituições operam e como os consumidores acessam serviços e produtos. Conforme salienta Fonseca (2010, p.96):

> Os bancos passaram a utilizar a automação para melhorar a qualidade dos serviços, procurando reduzir o tempo de processamento das transações. E paralelamente passaram a ampliar a rede física de agências, aumentando os pontos de contato com os clientes, o que por sua vez acarretava um aumento do número de bancários.

O setor de serviços financeiros é o mais tecnológico e digitalizado do país. Os bancos investem, anualmente, cerca de 20 bilhões em tecnologia da informação. Segundo a FEBRABAN (2023), em 2022, o volume do orçamento em tecnologia representou um crescimento de 18% em relação a 2021, somando R$ 34,9 bilhões e sendo uma das maiores altas dos últimos anos, impulsionado por implementação de recursos que atendem às necessidades de escalabilidade e de flexibilidade para a organização, como cloud e inteligência artificial. Sendo assim, inovar é preciso, desde que haja cautela e sustentabilidade, atendendo princípios de segurança e privacidade de dados cada vez mais cobrados e exigidos pela sociedade.

A Resolução nº 4.658 de 26 de abril de 2018, emitida pelo Banco Central do Brasil (BCB), estabelece princípios, diretrizes e requisitos mínimos de governança, gestão de riscos e controles internos para as instituições financeiras, visa fortalecer a segurança e a estabilidade do sistema financeiro, além de promover a proteção dos interesses dos clientes e a integridade das informações, processamento de dados e computação em Nuvem.

Essa resolução é aplicável a todas as instituições financeiras autorizadas a funcionar pelo Banco Central do Brasil, incluindo bancos, cooperativas de crédito, financeiras e outras entidades do sistema financeiro. Ela tem como objetivo principal garantir a adoção de práticas adequadas de gestão de riscos e controles internos, visando prevenir fraudes, proteger os interesses dos clientes e assegurar a confiabilidade das operações financeiras.

A atividade bancária tem passado por uma significativa evolução, em consonância com os avanços tecnológicos ocorridos na última década. O conceito de "digital" tem substituído as tradicionais filas em agências bancárias, trazendo à tona uma nova era de serviços online que antes eram predominantemente conduzidos através de interações físicas com os profissionais bancários.

Assim, os bancos têm se adaptado e incorporado inovações em suas operações. A internet e os dispositivos móveis abriram novas possibilidades, permitindo que os clientes realizem transações financeiras, acessem suas contas, solicitem empréstimos e façam investimentos, tudo isso com apenas alguns cliques.

Os aplicativos bancários móveis tornaram-se uma ferramenta essencial para os clientes, proporcionando conveniência e acessibilidade. Através desses aplicativos, é possível verificar saldos, fazer transferências, pagar contas e até mesmo investir, tudo de forma rápida e segura. Além disso, serviços como pagamentos digitais e carteiras eletrônicas se tornaram cada vez mais populares, facilitando as transações do dia a dia.

Bioni (2019, p.39), destaca:

> Como já adiantado, essa base legal ganhou ainda mais relevância diante da emergência de tecnologias e no contexto de uma economia baseada no uso intensivo de dados (subcapítulo 5.4). Tal como o consentimento no início do progresso geracional das leis de proteção de dados pessoais (subcapítulo 2.5), o legítimo interesse ganhou o status de uma nova 'carta coringa regulatória' para abraçar uma miríade de possíveis usos dos dados.

Nesse sentido, a digitalização dos serviços bancários traz consigo a necessidade de implementar medidas de segurança robustas para garantir a privacidade e a integridade das informações pessoais e financeiras dos clientes. É disso que se trata a evolução tecnológica, e com essa evolução surge novos desafios relacionado a segurança e a ocorrência de fraudes.

Ela também abre portas para possíveis vulnerabilidades e ataques cibernéticos exigindo que as instituições financeiras sejam proativas na proteção dos dados.

Apesar das inúmeras medidas de proteção adotadas pelos bancos, os criminosos continuam buscando maneiras de explorar possíveis falhas no sistema. Um exemplo de fraude comum no contexto digital é o *phishing*[4], onde os fraudadores enviam mensagens falsas por *e-mail, SMS* ou até mesmo por telefone, tentando obter informações confidenciais dos clientes, como senhas, números de cartão de crédito ou dados de identificação.

Outras formas de fraude incluem *malware*[5], *ransomware*[6] e ataques de engenharia social, todos projetados para comprometer a segurança dos sistemas bancários e obter acesso não autorizado aos dados dos clientes. Os bancos estão cientes dessas ameaças e têm investido em tecnologias avançadas de segurança, como autenticação em duas etapas, criptografia e detecção de atividades suspeitas. Além disso, eles implementam programas de conscientização e educação para os clientes, orientando sobre os riscos e como se proteger contra fraudes.

No entanto, é importante reconhecer que, apesar dos esforços contínuos das instituições financeiras, a evolução digital também implica um jogo de gato e rato entre os bancos e os criminosos cibernéticos. À medida que os bancos fortalecem suas defesas, os fraudadores desenvolvem novas técnicas para contorná-las.

2.3 A digitalização dos bancos e surgimento de *fintechs*

A palavra *fintech* é um termo termo que surgiu do inglês *"financial"*(financeiro) e *"technology"* (tecnologia), seu conceito vem de empresas que oferecem produtos financeiros digitais, destacando-se pela inovação tecnológica em relação às instituições financeiras tradicionais com uma ampla gama de soluções financeiras, como cartões de créditos, contas

4 O phishing é uma forma de ataque cibernético projetada para enganar pessoas e obter informações confidenciais, como senhas, informações de cartões de crédito e outros dados pessoais. Geralmente, os ataques de phishing são realizados por meio de e-mails fraudulentos, mensagens de texto, ou sites falsos que se passam por legítimos.
Os criminosos por trás do phishing costumam se fazer passar por instituições confiáveis, como bancos, empresas de tecnologia ou órgãos governamentais, para induzir as vítimas a revelar informações sensíveis. Os e-mails ou mensagens fraudulentas muitas vezes contêm links para páginas da web que parecem autênticas, mas são, na verdade, projetadas para coletar dados pessoais quando as vítimas inserem essas informações em formulários falsos.

5 Malware é uma abreviação para "software malicioso", e refere-se a qualquer software desenvolvido com a intenção de causar danos a um computador, rede, ou obter acesso não autorizado a informações confidenciais.

6 Ransomware é uma categoria específica de malware que criptografa os arquivos em um sistema, tornando-os inacessíveis, e os criminosos exigem um resgate (ou "ransom") para fornecer a chave de descriptografia.

digitais, empréstimos e seguros, geralmente permitindo que os clientes acesse e controlem seus produtos por meio de *smartphones*, sem a necessidade de visitar agências físicas.

Sendo assim, como qualquer processo evolutivo, a revolução digital também alcançou as instituições bancárias, impulsionada pelo avanço tecnológico e pelo desejo de proporcionar serviços de melhor qualidade e maior comodidade aos clientes. É notório que essa transformação digital tem facilitado significativamente a vida das pessoas. Antes, tarefas como sacar dinheiro ou pagar contas costumavam ser um verdadeiro tormento, com filas intermináveis e a necessidade de dedicar um dia inteiro a essas atividades. Hoje em dia, essas tarefas se tornaram acessíveis com apenas um clique no celular, no conforto da própria casa.

Historicamente, a evolução das operações bancárias começou com a introdução de computadores nas décadas passadas. Logo em seguida, na década de 60/70, surgiram os caixas eletrônicos, que permitiu ao cliente realizar transações básicas fora do horário de atendimento. Com o advento da internet, o "*internet banking*"[7] emergiu e impulsionou a criação de novos sistemas. A partir desse momento, com a criação e popularização dos *smartphones*, a evolução do setor bancário continuou a se acelerar, com aplicativos móveis, pagamentos digitais, tecnologia *blockchain*[8], criptomoedas e as chamadas "inteligências artificiais".

Com toda essa evolução tecnológica, tornou-se possível a realização de pagamentos por aproximação e a implementação do sistema Pix[9], uma inovação que transformou integralmente o setor bancário, oferecendo uma modalidade de pagamento rápida e eficaz, isenta de quaisquer encargos por parte das instituições financeiras. Essa transição digital ganhou impulso com a crise da pandemia, que já estava em curso de forma tímida anteriormente.

Um exemplo ilustrativo desse avanço ocorreu em julho de 2018, quando já existiam 2,88 milhões de contas bancárias 100% digitais no Brasil, de acordo com dados fornecidos

7 Internet Banking, também conhecido como banking online, é um serviço oferecido por instituições financeiras que permite aos clientes realizar transações bancárias e acessar informações relacionadas às suas contas por meio da internet. Essa modalidade de serviço bancário oferece conveniência, flexibilidade e acesso rápido a uma variedade de operações financeiras sem a necessidade de ir fisicamente a uma agência bancária.

8 Blockchain é uma tecnologia de registro distribuído que possibilita a criação de um registro seguro e imutável de transações em uma rede descentralizada.

9 O PIX é um sistema de pagamento instantâneo brasileiro, lançado pelo Banco Central do Brasil em novembro de 2020. O termo "PIX" deriva da palavra "pixel", simbolizando a ideia de instantaneidade e rapidez nas transações. Esse sistema oferece uma alternativa eficiente e segura para realizar transferências de dinheiro, pagamentos e outras transações financeiras.

pelo FEBRABAN. Esse mesmo levantamento revelou que a maioria dessas contas foi aberta por meio de dispositivos móveis, representando um impressionante aumento de 171% em relação ao ano anterior.

> O número de empresas criando soluções inovadoras para o setor financeiro vem crescendo. Trata-se de uma tendência mundial de inovação que veio para transformar a relação das pessoas com o dinheiro. Em junho de 2018, um estudo do Finnovation apontou que o número de fintechs no Brasil era de 377. Em todo o mundo, elas já somam mais de 5,5 mil." (Blog Nubank, 2023, s.p)

As *fintechs* desempenharam um papel significativo no impulsionamento dos bancos digitais, transformando a indústria financeira de inúmeras maneiras. A concorrência e a inovação trazidas, estimulou os bancos digitais a se adaptarem e buscarem aprimorar seus serviços, tornando o setor financeiro mais centrado no ciente, eficiente e tecnologicamente avançado.

Portanto, o barateamento da tecnologia da informação e o aumento do acesso à internet possibilitaram um boom das *fintechs*. No Brasil, todas as empresas que atuam no setor financeiro precisam seguir regras estabelecidas pelo Banco Central, bem como regramento de políticas de proteção de dados que apresenta as leis que regulam as instituições bancárias.

2.4 O *compliance* e as instituições bancárias

O sistema de *compliance* (ou conformidade) (Bedford, 2023, s.p.) em uma empresa funciona para assegurar que ela opere de acordo com as leis e regulamentos, evitando problemas legais, protegendo sua reputação e mantendo padrões éticos, desempenhando um papel crucial na garantia de que a organização esteja em conformidade com leis e regulamentos, prevenindo a falência ou o fim da pessoa jurídica, na busca de mitigar riscos, além de promover uma cultura corporativa responsável.

De acordo com Assi (2018, s.p), conceitua como "o dever das empresas de promover uma cultura que estimule, em todos os membros da organização, a ética, e o exercício do objeto social em conformidade com a lei. " O *compliance* abrange diversas áreas, como a ética corporativa, a governança, a segurança da informação, a prevenção à corrupção e ao suborno, entre outras. Dessa forma, a relação entre *compliance* e as instituições bancárias é essencial, pois os bancos estão sujeitos a regulamentações rigorosas e o *compliance* garante a conformidade com leis, previne lavagem de dinheiro, gerencia riscos, promove ética, protege

clientes e evita consequências adversas da não conformidade, como multas e perda de reputação.

Dentre elas, cabe citar a gestão de risco, já que é através do sistema de *compliance* dentro das organizações bancárias que é identificado e gerenciado uma variedade de riscos, como operacionais, de crédito e de mercado. Além de garantir a proteção do cliente, na coleta e uso de dados, garantindo a transparência e a devida regulação com as normas consumeristas e de LGPD.

A temática de *compliance*, embora velha conhecida dos profissionais que atuem com conformidade, controles internos e auditoria, ganhou destaque nos últimos anos, consequência dos grandes escândalos que, no Brasil e no mundo, envolvem a prática de corrupção e lavagem de dinheiro.

Segundo a Cartilha *Compliance* (2015), que é uma cartilha de uso interno para empregados da Caixa Econômica Federal, instituição bancária e empresa pública, alerta que o Comitê de Supervisão Bancária da Basileia[10], sendo uma organização composta por autoridades na supervisão bancária e visando fortalecer a solidez dos sistemas financeiras, vem demonstrando desde 1998 a preocupação com controle internos, o que levou as instituições financeiras a se focarem nos benefícios do *compliance*.

O Comité de Basileia, define "*risco de Compliance*", como o risco de sanções legais ou regulamentares, de perdas financeiras ou de reputação que um banco pode sofrer, como consequência do não cumprimento de leis, regulamentos, regras, disposições regulamentares do setor e códigos de conduta aplicáveis à atividade bancária.[11]. Diante das recomendações do Comitê, O CMN emitiu no mesmo ano, a Res nº 2.554, que dispõe sobre a implementação de sistemas de controle interno, substituída posteriormente pela resolução CMN nº 4.968/2021.

Passados alguns anos e diante da necessidade de restabelecer a ordem após a divulgação de exemplos de mais condutas de empregados e dirigentes, inclusive em grandes e renomadas empresas, o Estado promulgou em 2013 a Lei nº 12.846/2013, conhecida como Lei Anticorrupção, que dispõe sobre a responsabilização administrativa e civil de pessoas

[10] O Comitê de Supervisão Bancária da Basileia (em inglês, Bank for International Settlements - BIS - Basel Committee on Banking Supervision) é uma organização internacional que serve como fórum para a cooperação regulatória e supervisão bancária. Ele opera sob os auspícios do Banco de Compensações Internacionais (BIS), uma instituição financeira internacional sediada em Basileia, Suíça.

[11] BCBS & BIS (2005) - "Compliance and the Compliance function in banks", p. 7.

jurídicas pela prática e atos contra a administração pública, nacional ou estrangeiras, e dá outras providências.

Em 2015, de forma a complementar as providências da Lei nº 12.846/2013, foi publicado o Decreto nº 8.420 que trouxe, entre outras, a responsabilização administrativa de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira.

Para tratar especificamente o tema *compliance*, o Conselho Monetário Nacional (CMN) editou em 2017 a Res nº 4.595 que dispõe sobre a política de *compliance* das instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Esta norma estabeleceu a obrigatoriedade de as instituições implementarem políticas de *compliance*, com base em regras, diretrizes e critérios estabelecidos pelo ato normativo.

Segundo dados da pesquisa realizada pela Consultoria Protiviti (2018) sobre o nível de maturidade em *compliance*, nas mais diversas empresas brasileiras, somente 45% das empresas brasileiras possuem alto grau de exposição a risco de corrupção. E somente 34% das instituições analisadas já mapearam os riscos de exposição depois da regulamentação da Lei Anticorrupção no país (em agosto de 2013); apenas 36% adotaram processos de análise de terceiros para identificar eventuais riscos vindos de prestadores de serviços ou parceiros de negócios externos. Já 38% dos das empresas ouvidas para a pesquisa disseram que promoveram, no último ano, práticas de *compliance* somente por meio de treinamentos ou comunicados gerais.

De acordo com Assi (2018, s.p), o *compliance* então é sobre pessoas, sejam elas decisores, gestores ou colaboradores, que devem pautar suas ações na responsabilidade corporativa, escolhendo sempre, fazer o que é certo ate que este comportamento se naturalize, como as que impactam diretamente a operação, como por exemplo, na implementação de tecnologias, planejamento de prevenção de riscos de desvio de conduta, incorporação de métodos para detectá-los e controla-los, mobilizando os gestores a uma postura mais proativa no gerenciamento dos riscos que permeiam a atividade da instituição e comprometem sua sustentabilidade, tais como, falhas em ferramentas de TI, sistemas e na segurança da informação armazenada e compartilhada; fraudes e desvios financeiros por parte dos que ocupam cargos de confiança e gestão; corrupção de agentes público, dentre outros.

2.3.1 Controle Interno

Controle é um importante elemento das funções administrativas de uma organização, pois permite a constante avaliação do alcance dos objetivos estratégicos e operacionais. Quando implantados, são capazes de amenizar ou eliminar gargalos que impeçam o alcance desses objetivos.

O controle interno fornece um conjunto de políticas, procedimentos e praticas implementadas por uma organização para proteger seus ativos, abrangendo diversas áreas, incluindo contabilidade, segurança da informação, gestão de riscos e conformidade regulatória, tendo como objetivo assegurar a eficiência operacional, a prevenção de fraudes e proteção de dados sensíveis, e por isto, o controle interno desempenha um papel primordial na governança corporativa.

Apesar de existirem vários os conceitos dados por diversos autores, percebe-se que existe uma unidade de pensamento sobre o que se compreende por controle interno: são mecanismos adotados pelas empresas no sentido de minimizar o impacto de riscos de processo e de negócio.

Langlet diz, os controlos internos são ferramentas internas da empresa que têm como principal função fornecer uma razoável segurança à realização das operações da organização, assim como, atribuir confiabilidade aos relatórios financeiros, conformando-se com a lei e os regulamentos aplicáveis. [12]

De acordo com Almeida (1996), o Instituto dos Auditores Internos do Brasil (AUDIBRA), através da Instrução SEST nº 02, de 5 de outubro de 1986, estabelece como orientação específica as normas para o exercício profissional da auditoria interna e enfatiza que controle interno corresponde a qualquer ação tomada pela administração (assim compreendida tanto a alta administração como os níveis gerenciais apropriados) para aumentar a probabilidade de que os objetivos e metas estabelecidos sejam atingidos.

O Departamento do Tesouro Nacional (1991), por sua vez, através da Instrução Normativa nº 16, de 20 de dezembro de 1991, traz o conceito de controle interno como sendo: o conjunto de atividades, planos, métodos e procedimentos interligados utilizado com vistas a assegurar que os objetivos dos órgãos e entidades da administração pública sejam

[12] Langlet, Marc (2014) - "The Compliance function in banks", Horizons Bancaires, n.º 321.

alcançados, de forma confiável e concreta, evidenciando eventuais desvios ao longo da gestão, até a consecução dos objetivos fixados pelo Poder Público.

Portanto, pode-se dizer que um meio de efetivo de prevenção de violação de dados pessoais nas organizações bancárias é através do controle interno. A implementação de um sistema de gestão de riscos tem relação direta com os mecanismos de governança e de controle interno. O processo de controle interno é parte integrante da gestão de riscos, que por sua vez, integra a governança da organização.

Para entender sobre controles internos, Bandarovsky (s.p)no E-book "*Compliance Risk Assessment* em 8 passos", demosntra que é necessário conhecer o COSO – *Comitee of Sponsoring Organizations of the Treadway Commission*, entidade privada que tem como objetivo o desenvolvimento de estruturas abrangentes e diretrizes sobre controles internos, gerenciamento de riscos corporativos e fraude, para aprimorar a performance e supervisão organizacional e reduzir a extensão das fraudes nas organizações.

Esse comitê elaborou o *Internal Control – integrated framework* ou Controle Interno – Estrutura Integrada, que é um modelo de referência de gestão corporativa de riscos, baseado nas melhores práticas internacionais sobre o tema. A primeira versão da proposta do COSO para Controle Interno foi publicada em 1992, e desde então vem obtendo espaço cada vez maior no meio corporativo.

Em 2013, o COSO realizou uma ampla revisão da estrutura, constituindo um modelo conceitual para o Sistema de Controle Interno, útil para as organizações em desenvolvimento e na manutenção de sistemas alinhados aos objetivos do negócio e adaptados às constantes mudanças no ambiente empresarial, oferecendo uma orientação para todos os níveis da administração em relação ao desenvolvimento, à implementação e à condução do controle interno e à avaliação de sua eficácia.

De acordo com o COSO 2013, o controle interno é um processo dinâmico e integrado, conduzido pela estrutura de governança e, administração e outros profissionais da entidade, e desenvolvido para proporcionar segurança razoável com respeito à realização dos objetivos relacionados a operações, divulgação e conformidade.

2.3.2 Aspectos relevantes da resolução CMN nº4.968/2021

A Resolução CMN nº 4968/2021, foi publicada em 25/11/2021, revogando a Resolução CMN nº 2.554/1998 e dispõe sobre a implementação, manutenção e responsabilidades dos

Sistemas de Controles Internos nas Instituições Financeiras.

Dentre as principais alterações trazidas pela nova norma, destacam-se a atualização e aprimoramento de conceitos, diretrizes e regras, com foco no monitoramento contínuo das atividades de controles internos.

A resolução estabelece que o Sistema de Controle Interno deve prever aspectos relacionados à cultura de controle, à identificação e à avaliação de riscos, às atividades de controle e segregação de funções, à informação, à comunicação e ao monitoramento.

Além disso, prevê a obrigatoriedade de comunicação tempestiva pelos empregados de problemas nas operações de situações de não conformidade com os padrões de conduta definidos e violações das políticas da instituição ou de disposições legais e regulamentares e determina a proibição do estabelecimento de metas que incentive a tomada de decisão em desacordo com o apetite a risco da organização, visando o cumprimento de seus objetivos estratégicos.

A referida norma discorre, ainda, acerca da necessidade de revisão e acompanhamento de atividades relevantes pela gestão corporativa, com controles de atividades apropriados e adequados à estrutura da organização, que visem a evitar o envolvimento da instituição em atividades indevidas ou ilícitas, em especial as relacionadas aos riscos sociais, ambientais e climáticos, bem como à prevenção da prática dos crimes de " lavagem" ou ocultação de bens, direitos e valores , de financiamento do terrorismo e prevenção, detecção, investigação e correção de fraudes.

Outro ponto relevante trata sobre a segregação apropriada das funções, com o intuito de evitar situações de potencial conflito de interesses. A segregação de funções consiste na separação das funções de autorização, aprovação, execução, controle e contabilização, de modo que, para mitigar potencial conflito deve-se repartir atividades incompatíveis, como executar e fiscalizar uma mesma atividade, evitando que apenas um empregado ou equipe controle todas etapas-chave de determinado processo.

Além desse ponto, também destaca a relevância do papel da alta administração no fornecimento do Sistema de Controle Interno, uma vez que os dirigentes e conselheiros da Instituição Financeira que dão o tom que os empregados devem seguir para assegurar um ambiente de controle robusto e sustentável.

CONSIDERAÇÕES FINAIS

O estudo sobre a violação de dados pessoais em instituições bancárias revela a urgência de abordar as complexidades crescentes da segurança cibernética no setor financeiro. Ao longo deste artigo, exploramos a importância crucial do *compliance* como meio de controle interno para mitigar os riscos associados à violação de dados pessoais. Através da pesquisa do cenário atual, destacamos a necessidade de instituições bancárias adotarem medidas efetivas para garantir a privacidade e segurança dos dados coletados de seus clientes.

A implementação de políticas robustas de *compliance* não apenas se torna uma necessidade estratégica, mas também uma resposta ética à crescente digitalização do setor financeiro. Os resultados deste estudo apontam para a importância da conscientização e educação contínuas sobre questões de segurança cibernética entre os profissionais do setor. Além disso, ressaltamos a relevância de uma fiscalização rigorosa para coibir possíveis abusos e violações da lei, promovendo a responsabilidade e transparência por parte das instituições financeiras.

A pesquisa abrangeu aspectos relacionados a violação de dados dos clientes de instituições bancárias, e trouxe como efetiva resolução o *compliance* e o controle interno, onde fora demonstrado e comprovado ao longo do presente artigo, que a proteção de dados no ambiente digital se tornou prioridade à medida que vazamentos de dados foram demonstrando a vulnerabilidade das informações pessoais, e como empresas que detinham o poder desses dados, passou a obter vantagens nos negócios.

Foi abordado assuntos relacionados com a revolução digital, análise histórica do surgimento das normas bancárias, as novas tecnologias digitais e profundas transformações quanto as instituições bancárias, apresentou conceitos e definições de *fintechs* e banco digitais, a importancia dos mecanismos de *compliance* e controle interno, e demonstrou os aspectos relevantes da Resolução CMN nº 4.968;2021.

Logo, a aplicação de princípios de *compliance* é essencial para a manutenção e prevenção de riscos de natureza fraudulenta, pois envolve a criação de uma cultura organizacional, que promove a ética e o cumprimento de leis e regulamentos, evitando o surgimento de problemas de ordem legal.

O controle interno é uma parte vital do *compliance* e envolve a implementação de políticas, procedimentos e práticas para proteger os ativos da organização e garantir a eficiência operacional. Isso inclui a identificação e mitigação de vulnerabilidades, a restrição

de acesso a dados sensíveis, o monitoramento contínuo de atividades treinamento e conscientização dos funcionários, conformidade com regulamentações e a preparação para responder a incidentes de segurança.

O COSO (*Comitee of Sponsoring Organizations of the Treadway Commission)* fornece um modelo de referência de gestão corporativa de riscos, controle interno e governança que ajuda as organizações a desenvolver sistema de controle eficazes e alinhados com seus objetivos.

Embora se mencione o uso de máquinas e inteligência artificial para detectar e erradicar violações de dados pessoais, assim como elaborar planos e metódos visando evitar danos institucionais, por fim, é crucial ressaltar que o investimento na capacitação pessoal dos colaboradores representa a solução mais eficaz. A presença da mão de obra humana é indispensável para esse processo.

Em síntese, este artigo não apenas contribui para o entendimento da vulnerabilidade dos dados pessoais em instituições bancárias, mas também destaca a necessidade premente de ações proativas. A adoção de medidas efetivas de compliance emerge como uma estratégia essencial para enfrentar os desafios contemporâneos de segurança cibernética, garantindo não apenas a conformidade legal, mas também a confiança contínua dos clientes em um ambiente bancário cada vez mais digitalizado.

REFERÊNCIAS

A IMPORTANCIA DO COMPLIANCE: PROMOVENDO A ÉTICA E A SUSTENTABILIDADE NAS EMPRESAS. **Russel Bedford.** Disponível em: <https://russellbedford.com.br/a-importancia-do-compliance/>. Acesso em: 26 out 2023

ALMEIDA, M.C. **Auditoria: um curso moderno e completo**. São Paulo, Atlas, 1996.

ASSI, Marcos. **Compliance como implementar.** – São Paulo: Editora Trevisan, 2018.

BRASIL. Constituição Federal (1988). **Constituição da República Federativa do Brasil de 1988.** Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm . Acesso em: 01 jun 2023.

BRASIL. **Lei Complementar nº 105, de 10 de janeiro de 2001**. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Disponível em: http://www.planato.gov.br/ccivil_03/leis/lcp/lcp105.htm . Acesso em: 01 jun 2023.

BRASIL. Banco Central do Brasil. **Resolução nº 4.658, de 26 de abril de 2018.** Dispõe sobre a política de segurança cibernética, sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e sobre a política de segurança cibernética para as instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Diário Oficial da União, Brasília, DF, Edição: 82 Seção: 1 Página: 26, 2018.

___. **Lei nº 12.965,** de 23 de abril de 2014. Lei do Marco Civil na Internet. Disponível em: http://www.planato.gov.br/ccivil_03/ato2011-2014/2014/lei/L12965.htm . Acesso em: 01 jun 202.
___. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Disponível em: <http://www.planato.gov.br/ccivil_03/ato2015-2018/2018/lei/L13709.htm>. Acesso em: 01 jun 2023.
____. **Proteção de Dados Pessoais – UFS**. Disponível em: <lgpd.ufsc.br/duvidas-frequentes/>. Acesso em: 01 jun 2023.

BANCO CENTRAL DO BRASIL. **Resolução CMN nº 4.968**, de 25 nov 2021. Disponível em: http://www.bcb.gov.br/estbilidadefinanceira/exibenormativo?tipo=Resolução%20CMN&numero=4893 . Acesso em: 31 out 2023.

BANCO CENTRAL DO BRASIL. **Resolução nº 4.893**, de 26 fev 2021. Disponível em: http://www.bcb.gov.br/estbilidadefinanceira/exibenormativo?tipo=Resolução%20CMN&numero=4893 . Acesso em: 01 jun 2023.

BANDAROVSKY, B. P. **Compliance Risk Assessment em 8 passos.** Documento Interno.
BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.** 2 ed. FORENSE: Rio de Janeiro, 2019.
BONFIM, T. **Segurança e Transparência no uso de dados de clientes de bancos digitais no Brasil.** Dissertaçao (mestrado) – Universidade do Vale dos Sinos. Porto Alegre, 2020
CAIXA ECONÔMICA FEDERAL. **Curso Compliance Interno e Externo.** Documento interno, 2015.

CAIXA ECONÔMICA FEDERAL. **Cartilha Normas Externas e Internas.** Documento interno, 2015.

CANCELIER, Mikhail Vieira de Lorenzi. **O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro.** Florianópolis: Scielo, 2017. Disponivel em: https://www.scielo.br/j/seq/a/ZNmgSYVR8kfvZGYWW7g6nJD/# . Acesso em: 30 set 2023.
COELHO, S. **Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018): Comentários Artigo por Artigo**. Ed. Forense, 2018.

COSO – Committee of Sporing Organizations. Disponivel em: < https://www.coso.org/about-us>. Acesso em: 30 out 2023.
FACHIN, L. E. Internet: o direito na era virtual. Saraiva, 2012.

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

FONSECA, Carlos Eduardo Correa da. CORREA, Carlos Eduardo . MEIRELLES Fernando. DINIZ, Eduardo. **Tecnologia bancária no Brasil : uma história de conquistas, uma visão de futuro**. Coordenação editorial Sonia Penteado. – São Paulo : FGVRAE, 2010.

FRAZÃO, A. **Direito Digital.** Saraiva, 2014.

FEBRABAN. **Pesquisa Febraban de Tecnologia Bancária 2023**. Disponível em: https://febrabantech.febraban.org.br/temas/inovacao/investimento-dos-bancos-em-tecnologia-deve-chegar-a-r-45-1-bilhoes-em-2023-com-alta-de-29. Acesso em 15 nov 2023.

GONSALES, A. et al. **Diretrizes do Compliance Financeiro.** 2ª ed. São Paulo: LEC, 2023. Disponível em: https://universidade.caixa/plugnfile.php/1783735/mod_resource/cotent/2/E_book_LEC_Diretrizes_do_compliance_Financeiro.pdf . Acesso em: 04 de set de 2023.

LEITE, B. **Proteçao de dados e os impactos da LGPD nas instituições financeiras**. Monografia(graduação) – Universidade de Tatuapé. Tatuapé, SP. 2022

ONOME IMONIANA, Joshua; JORDAN NOHARA, Jouliana. **COGNIÇÃO DA ESTRUTURA DE CONTROLE INTERNO: UMA PESQUISA EXPLORATÓRIA**. Revista Base (Administração e Contabilidade) da UNISINOS, vol. 2, núm. 1, enero-abril, 2005, pp. 37- 46 Universidade do Vale do Rio dos Sinos São Leopoldo, Brasil. Disponivel em: https://www.redalyc.org/pdf/3372/337228628004.pdf . Acesso em: 28 de out de 2023.

O QUE É FINTECCH E POR QUE ESSE TERMO FICOU TÃO POPULAR? **Blog Nubank.** Disponível em: https://blog.nubank.com.br/fintech-o-que-e/ . Acesso em: 22 de set 2023.

RODRIGUES, J. **Compliance nas relações bancárias: Relação com o Sistema de Controlo Interno e Auditoria Interna.** Tese (Mestrado em Direito) – Faculdade de Direito, Escola do Porto, 2019.

VILELA, T. **Lei Geral de Proteção de Dados e a Atividade Bancária: Base Legal do Interesse Legítimo e sua Aplicação.** Trabalho de conclusao de curso – Insper 2019. Sao Paulo/ SP, 2019.

WARREN, S. D.e BRANDEIS, L. D. (1890). **The right to Privacy.** Harvard Law Review. Disponível em: http://doi.org/10.2307/1321160 Acesso em: 04 abr 2023.