



**CENTRO UNIVERSITÁRIO DE EXCELÊNCIA
COLEGIADO DO CURSO DE DIREITO**

**RESPONSABILIDADE CIVIL DAS INSTITUIÇÕES FINANCEIRAS NA
PREVENÇÃO E COMBATE A CRIMES CIBERNÉTICOS**

**Vitória da Conquista
2024**

**CENTRO UNIVERSITÁRIO DE EXCELÊNCIA
COLEGIADO DO CURSO DE DIREITO**

**Daniela da Costa Gomes Santos
Davi Novais Brezolin
Luiza de Almeida Chaves**

**RESPONSABILIDADE CIVIL DAS INSTITUIÇÕES FINANCEIRAS NA
PREVENÇÃO E COMBATE A CRIMES CIBERNÉTICOS**

Projeto entregue para acompanhamento
como parte integrante das atividades de
TCC II do Curso de Direito do Centro
Universitário UNEX.

**Vitória da Conquista
2024**

RESPONSABILIDADE CIVIL DAS INSTITUIÇÕES FINANCEIRAS NA PREVENÇÃO E COMBATE A CRIMES CIBERNÉTICOS

DANIELA DA COSTA GOMES SANTOS

DAVI NOVAIS BREZOLIN

LUIZA DE ALMEIDA CHAVES

RESUMO

O presente trabalho teve como objetivo analisar a responsabilidade civil das instituições financeiras, enfocando a Lei Geral de Proteção de Dados (LGPD) e seu papel no combate e na prevenção de vazamentos de dados dos clientes. A pesquisa investigou as principais falhas nos sistemas dessas instituições, com o intuito de propor soluções para aumentar a segurança dos usuários, através de métodos e análise e pesquisa em fontes acadêmicas, legislação, avaliação de normas e regras, decisões judiciais e casos práticos pertinentes acerca da responsabilidade civil das empresas financeiras e delitos cibernéticos. Estes métodos de pesquisa oferecem uma maneira ampla e detalhada de examinar a responsabilidade legal das instituições diante dos delitos cibernéticos, misturando análises baseadas em teoria, regulamentação e evidências concretas para alcançar resultados importantes e pertinentes. Além disso, foram avaliadas as medidas de segurança adotadas pelos bancos, considerando sua eficácia na proteção dos dados. A partir dessa análise, foram propostas recomendações específicas para fortalecer a segurança da informação dos consumidores, além de explorar maneiras de auxiliar as instituições financeiras no cumprimento das exigências da LGPD e na prevenção de novos incidentes de vazamento de dados.

Palavras-chave: Responsabilidade Civil; Instituições Financeiras; Vazamento de Dados; Falhas nos Sistemas.

CIVIL LIABILITY OF FINANCIAL INSTITUTIONS IN THE PREVENTION AND COMBATING OF CYBERCRIMES

ABSTRACT

The aim of this study was to analyze the civil liability of financial institutions, focusing on the General Data Protection Law (LGPD) and its role in combating and preventing customer data breaches. The research investigated the main vulnerabilities in the systems of these institutions, with the goal of proposing solutions to enhance user security. Additionally, the security measures adopted by banks were evaluated, considering their effectiveness in data protection. Based on this analysis, specific recommendations were made to strengthen consumer data security, as well as explore ways to assist financial institutions in complying with the requirements of the LGPD and preventing future data breach incidents.

Keywords: Civil Liability; Financial Institutions; Data Breach; System Failures.

1. INTRODUÇÃO:

Na atualidade, as organizações financeiras possuem uma importância fundamental na economia mundial, porém enfrentam desafios significativos devido ao avanço da tecnologia. Com o aumento dos crimes cibernéticos, torna-se essencial investigar a responsabilidade civil dessas instituições na prevenção e combate a tais ameaças. Neste estudo, busca-se realizar uma análise detalhada das responsabilidades legais e éticas das organizações financeiras, ressaltando suas medidas de segurança e ações diante de incidentes cibernéticos, com o objetivo de colaborar para a efetividade das políticas de segurança digital e redução de prejuízos.

Diante do aumento significativo de operações financeiras realizadas digitalmente e o consequente crescimento de crimes cibernéticos que visam usurpar dados pessoais e financeiros dos usuários e clientes, emerge a necessidade de

investigar a extensão da Responsabilidade Civil das Instituições Financeiras na proteção desses dados. Portanto, o nosso Projeto de Pesquisa adotará um estudo e análise da responsabilidade civil, investigando até que ponto a implementação da LGPD tem sido eficaz na prevenção de fraudes e ataques cibernéticos em instituições financeiras, identificando as principais lacunas, desafios e oportunidades para fortalecer a segurança de dados e a proteção ao consumidor. Qual a responsabilidade civil das instituições financeiras nos crimes cibernéticos?

Além disso, cabe destacar que, através da aplicação da Lei Geral de Proteção de Dados, bem como o uso de tecnologias de inteligência artificial, treinamento de funcionários e elaboração de campanhas de conscientização, pelas instituições financeiras, possibilitará uma redução significativa na incidência de crimes cibernéticos, pois auxiliará em seu combate e prevenção. Será analisado ainda como o tamanho e os orçamentos das instituições financeiras será capaz de afetar a sua capacidade de implementação de medidas eficazes de segurança.

DA RESPONSABILIDADE CIVIL

2.1. CONCEITO DE RESPONSABILIDADE CIVIL

O vocábulo “responsabilidade”, tem origem etimológica do verbo *respondere* em latim, que significa a obrigação, garantia ou contraprestação. Contém ainda, a raiz latina *spondeo*, uma fórmula pela qual o devedor se vinculava, no Direito Romano, nos contratos verbais. Conforme expõe Pablo Stolze (2024, p.1), a noção de **responsabilidade está associada ao surgimento** de uma obrigação derivada, ou seja, um dever jurídico que surge como consequência de um fato jurídico em sentido amplo. Esse dever é fundamentado no princípio jurídico da “proibição de ofender”, que se baseia na ideia de que ninguém deve causar prejuízo a outrem (STOLZE, 2024, p.1).

No mesmo sentido, Maria Helena Diniz estabelece que a responsabilidade civil “[...] é a aplicação de medidas que obriguem uma pessoa a reparar dano moral ou patrimonial causado a terceiros, em razão de ato por ela mesma praticado” (Diniz, 2024, p. 22).

A responsabilidade civil está amparada no Código Civil, mais precisamente nos artigos 927 a 954 do Código Civil. O primeiro artigo deste capítulo estabelece que:

Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. [...] Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem (Brasil, 2002).

Ante o exposto, é de suma importância o estudo sobre a responsabilidade civil, (Carlos Roberto Gonçalves 2024, p. 3) discorre:

Grande é a importância da responsabilidade civil, nos tempos atuais, por se dirigir à restauração de um equilíbrio moral e patrimonial desfeito e à redistribuição da riqueza de conformidade com os ditames da justiça, tutelando a pertinência de um bem, com todas as suas utilidades, presentes e futuras, a um sujeito determinado, pois, como pondera José Antônio Nogueira, o problema da responsabilidade é o próprio problema do direito, visto que “todo o direito assenta na ideia da ação, seguida da reação, de restabelecimento de uma harmonia quebrada”.

Destarte, resta evidenciado que a responsabilidade civil é fundamental nos tempos atuais, porquanto visa restaurar o equilíbrio moral e patrimonial, promovendo a justiça e a redistribuição da riqueza, protegendo o direito de um indivíduo sobre seus bens, presentes e futuros. É de grande importância as instituições financeiras se mostrarem responsáveis quando o assunto são crimes cibernéticos, principalmente por conta dos serviços sensíveis que fornecem e da natureza dos dados financeiros em jogo. Abaixo estão listados pontos relevantes sobre essa responsabilidade:

As entidades bancárias devem adotar medidas eficazes de segurança online para resguardar as informações sigilosas e financeiras de seus usuários. Isso engloba a instalação de firewalls, criptografia de dados, vigilância de atividades suspeitas, entre outras ações. Conforme demonstrado no estudo da Deloitte "Segurança Digital no Setor Financeiro", a proteção online é uma prioridade fundamental para resguardar tanto o patrimônio das instituições financeiras quanto as informações reservadas dos clientes (LOPES, Jurídico, 2021).

Mesmo com todas as medidas preventivas, é possível que ocorram contratempos de segurança digital. Nestas situações, as organizações financeiras têm a obrigação de identificar prontamente o ocorrido, agir de forma eficiente para

minimizar prejuízos e notificar os clientes impactados e as autoridades pertinentes conforme estipulado por leis e normas. De acordo com o documento da IBM "O Prejuízo de Vazamentos de Informações", a pronta e adequada resposta a eventos de segurança pode reduzir consideravelmente os gastos de uma violação de dados.

É essencial que as instituições financeiras adotem medidas proativas para proteger os dados de seus clientes e garantir a segurança cibernética de suas plataformas. A conformidade com regulamentações de segurança de dados, investimento em tecnologias de proteção cibernética e treinamento contínuo dos funcionários são estratégias importantes para mitigar o risco de responsabilidade legal e civil, (BARROS; GARBOSSA; CONTE, 2007).

É imperioso destacar que, as instituições bancárias, quando estabelecem com seus clientes relações de consumo, fornecendo-lhes produtos e/ ou serviços, submetem-se às regras do Código de Defesa do Consumidor (Lei 8.078/90), consoante entendimento pacificado pelo STJ.

De acordo com o art. 14 do CDC, o fornecedor responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos (responsabilidade objetiva), ressalvada culpa exclusiva do próprio consumidor ou de terceiros.

Verificamos a seguir, consoante entendimento pacífico pelo Superior Tribunal de Justiça, jurisprudências e legislações, abordando as hipóteses de Culpa Exclusiva do Consumidor e da Instituição, a respeito do tema abordado:

AGRAVO INTERNO NO AGRAVO EM RECURSO ESPECIAL. CIVIL. AÇÃO DE REPARAÇÃO POR DANOS MATERIAIS E MORAIS. FALHA NA PRESTAÇÃO DE SERVIÇO BANCÁRIO. RESPONSABILIDADE OBJETIVA AFASTADA, NA ESPÉCIE. NÃO CONFIGURAÇÃO. CULPA EXCLUSIVA DA VÍTIMA E DE TERCEIRO. REVISÃO. IMPOSSIBILIDADE. SÚMULA 7/STJ. AGRAVO INTERNO DESPROVIDO. 1. **"Tratando-se de consumidor direto ou por equiparação, a responsabilidade da instituição financeira por fraudes praticadas por terceiros, das quais resultam danos aos consumidores, é objetiva e somente pode ser afastada pelas excludentes previstas no CDC, como por exemplo, culpa exclusiva da vítima ou de terceiro"** (REsp 1.199.782/PR, Rel. Ministro LUIS FELIPE SALOMÃO, SEGUNDA SEÇÃO, DJe de 12/09/2011). 2. **Na hipótese, o Tribunal de origem concluiu que não houve falha na prestação do serviço bancário, ficando evidenciada a culpa exclusiva da vítima e de terceiro pelas transações bancárias, uma vez que houve a negligência quanto à guarda do cartão e senha pessoal.** 3. A modificação de tal

entendimento demandaria o revolvimento do conjunto fático-probatório dos autos. 4. Agravo interno desprovido.

(STJ - AgInt no AREsp: 2335920 MA 2023/0102795-3, Relator: Ministro RAUL ARAÚJO, Data de Julgamento: 18/09/2023, T4 - QUARTA TURMA, Data de Publicação: DJe 22/09/2023) (grifo nosso)

CONSUMIDOR. PROCESSUAL CIVIL. RECURSO ESPECIAL. AÇÃO DECLARATÓRIA DE INEXISTÊNCIA DE DÉBITOS. DEVER DE SEGURANÇA. FRAUDE PERPETRADA POR TERCEIRO. CONTRATAÇÃO DE MÚTUO. MOVIMENTAÇÕES ATÍPICAS E ALHEIAS AO PADRÃO DE CONSUMO. RESPONSABILIDADE OBJETIVA DA INSTITUIÇÃO FINANCEIRA. RECURSO CONHECIDO E PROVIDO. 1. Ação declaratória de inexistência de débitos, ajuizada em 14/8/2020, da qual foi extraído o presente recurso especial, interposto em 21/6/2022 e concluso ao gabinete em 17/2/2023. 2. O propósito recursal consiste em decidir (I) se a instituição financeira responde objetivamente por falha na prestação de serviços bancários, consistente na contratação de empréstimo realizada por estelionatário; e (II) se possui o dever de identificar e impedir movimentações financeiras que destoam do perfil do consumidor. 3. O dever de segurança é noção que abrange tanto a integridade psicofísica do consumidor, quanto sua integridade patrimonial, sendo dever da instituição financeira verificar a regularidade e a idoneidade das transações realizadas pelos consumidores, desenvolvendo mecanismos capazes de dificultar fraudes perpetradas por terceiros, independentemente de qualquer ato dos consumidores. 4. **A instituição financeira, ao possibilitar a contratação de serviços de maneira facilitada, por intermédio de redes sociais e aplicativos, tem o dever de desenvolver mecanismos de segurança que identifiquem e obstem movimentações que destoam do perfil do consumidor, notadamente em relação a valores, frequência e objeto.** 5. **Como consequência, a ausência de procedimentos de verificação e aprovação para transações atípicas e que aparentam ilegalidade corresponde a defeito na prestação de serviço, capaz de gerar a responsabilidade objetiva por parte da instituição financeira.** 6. Entendimento em conformidade com Tema Repetitivo 466/STJ e Súmula 479/STJ: "As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias". 7. Idêntica lógica se aplica à hipótese em que o falsário, passando-se por funcionário da instituição financeira e após ter instruído o consumidor a aumentar o limite de suas transações, contrata mútuo com o banco e, na mesma data, vale-se do alto montante contratado e dos demais valores em conta corrente para quitar obrigações relacionadas, majoritariamente, a débitos fiscais de ente federativo diverso daquele em que domiciliado o consumidor. 8. Na hipótese, inclusive, verifica-se que o consumidor é pessoa idosa (75 anos - imigrante digital), razão pela qual a imputação de responsabilidade há de ser feita sob as luzes do Estatuto do Idoso e da Convenção Interamericana sobre a Proteção dos Direitos Humanos dos Idosos, considerando a sua peculiar situação de consumidor hipervulnerável. 9. Recurso especial conhecido e provido para declarar a inexigibilidade das transações bancárias não reconhecidas pelos consumidores e condenar o recorrido a restituir o montante previamente existente em conta bancária, devidamente atualizado.

(STJ - REsp: 2052228 DF 2022/0366485-2, Relator: Ministra NANCY ANDRIGHI, Data de Julgamento: 12/09/2023, T3 - TERCEIRA TURMA, Data de Publicação: DJe 15/09/2023) (grifo nosso)

EMENTA: AÇÃO DE INDENIZAÇÃO POR DANOS MATERIAIS E MORAIS. PAGAMENTO DE BOLETO FALSO. AUSÊNCIA DE PARTICIPAÇÃO DA INSTITUIÇÃO FINANCEIRA REQUERIDA. CULPA EXCLUSIVA DO CONSUMIDOR E DE TERCEIRO. AUSÊNCIA DE RESPONSABILIDADE DA REQUERIDA. MANUTENÇÃO DA INSCRIÇÃO NO CADASTRO DE

INADIMPLENTES. EXERCÍCIO REGULAR DE DIREITO. IMPROCEDÊNCIA MANTIDA. - **Tratando-se de relação de consumo, a responsabilidade do banco requerido é objetiva, dispensando a comprovação de culpa, nos termos do art. 14 do Código de Defesa do Consumidor** - De acordo com o art. 14, § 3º do Código de Defesa do Consumidor, **a responsabilidade é excluída em caso de culpa exclusiva do consumidor ou de terceiro** - São públicos e notórios os cuidados exigidos na realização de transações financeiras pela internet, cabendo ao consumidor agir de forma diligente para resguardar-se da atuação de fraudadores - **Se o requerente realiza pagamento induzido a erro por terceiros falsários e sem qualquer participação da instituição financeira requerida, restando comprovada sua culpa exclusiva no evento danoso, não é cabível a responsabilização da parte requerida** - Demonstrada a ausência de quitação da dívida, a manutenção do devedor nos registros dos órgãos de proteção ao crédito é lícita, decorrendo do exercício regular de direito do credor.

(TJ-MG - AC: 50189976120208130145, Relator: Des.(a) Luiz Carlos Gomes da Mata, Data de Julgamento: 14/04/2023, Câmaras Cíveis / 13ª CÂMARA CÍVEL, Data de Publicação: 17/04/2023) (grifo nosso)

Sendo assim, em busca de evitar eventuais problemas e uma possível ação judicial em desfavor da instituição financeira, alguns *métodos devem ser adotados*, que serão explicados logo abaixo.

3. APLICATIVOS, MÉTODO E INTELIGÊNCIA ARTIFICIAL

Os resultados apresentados acima podem servir como base para a criação de um programa de formação e treinamento e melhorias para os funcionários e sistemas das instituições financeiras, focando na identificação e mitigação de ameaças cibernéticas. Esse modelo de treinamento visa um aperfeiçoamento dos funcionários e sistemas referente a efetivação de redução nos riscos de golpes, vazamentos de dados e de uma possível ação judicial.

Estudos mostram que a conscientização dos funcionários reduz significativamente a ocorrência de incidentes (Costa, 2019). Empresas de tecnologia que fornecem serviços para o setor financeiro podem utilizar as descobertas para desenvolver ou melhorar soluções de segurança cibernética, como sistemas de autenticação avançada e ferramentas de monitoramento de atividades suspeitas (FERNANDES, 2021).

A educação e conscientização do cliente também pode contribuir para a proteção de dados e prevenção dos incidentes de crime cibernético. As instituições

financeiras podem desenvolver campanhas educativas voltadas aos seus clientes, aumentando a conscientização sobre práticas seguras no uso de serviços financeiros digitais (Martins, 2019).

3.1 APLICATIVOS E FERRAMENTAS

Norton, McAfee, Bitdefender e Kaspersky ajudam a detectar e eliminar malware. O Malware é qualquer tipo de software malicioso, ou seja, projetado para prejudicar computadores ou seus usuários, com a função de roubar informações confidenciais, enviar e-mails falsos, sequestrar dados, interromper sistemas críticos etc. Sendo assim, é de extrema importância que as empresas e instituições financeiras adotem o uso permanente dessas ferramentas.

ZoneAlarm e Comodo protegem redes contra acessos não autorizados. São Firewalls que protegem computadores contra acessos não autorizados e diversas ameaças cibernéticas. É conhecido por sua interface amigável e facilidade de uso

Firewall Bidirecional: Monitora tanto as entradas quanto as saídas de dados, bloqueando tráfego suspeito.

Proteção contra Malware: Inclui funcionalidades de detecção de malware, complementando a proteção do firewall.

Controle de Aplicativos: Permite que os usuários decidam quais aplicativos podem acessar a internet.

Gerenciadores de Senhas, LastPass e 1Password são ferramentas essenciais para manter a segurança das informações pessoais e profissionais, permitindo que os usuários armazenem, gerenciem e gerem senhas de forma segura.

3.1.2. INTELIGÊNCIA ARTIFICIAL (IA)

ANÁLISE DE COMPORTAMENTO:

Sistemas que usam IA para analisar padrões de comportamento e identificar atividades anômalas que podem indicar uma violação de segurança. Ferramentas como **Darktrace** utilizam aprendizado de máquina para identificar e responder a ameaças em tempo real.

Darktrace é uma plataforma de segurança cibernética que utiliza inteligência artificial para detectar, responder e prevenir ameaças em tempo real. A tecnologia foi desenvolvida para ajudar as organizações a identificarem comportamentos anômalos e responder a incidentes de segurança antes que eles causem danos. Algoritmos de IA que analisam grandes volumes de dados para identificar tendências e padrões que podem indicar fraudes ou vazamentos.

TREINAMENTO E ABORDAGEM EM CONFORMIDADE COM A LGPD

O treinamento de conscientização é uma abordagem fundamental para proteger organizações contra ameaças como *phishing* e outras práticas maliciosas. É importante que o colaborador se identifique claramente como representante/colaborador da instituição, incluindo seu nome, cargo e a razão do contato, a fim de passar maior credibilidade e confiança ao cliente.

Utilize canais oficiais e verificados (e-mail institucional, telefone da empresa etc.) para garantir a legitimidade da comunicação. É de extrema importância, quando for tratar com o cliente, a explicação clara e o motivo do contato e como os dados do cliente foram obtidos, enfatizando que essa coleta está em conformidade com a LGPD, além de informar sobre os direitos do cliente em relação aos seus dados, como acesso, correção e exclusão.

Utilizar sempre uma linguagem simples e respeitosa, evitando jargões técnicos que possam confundir o cliente. Quando apropriado, busque obter o consentimento explícito do cliente para continuar o processo e o envio das demais informações. Isso reforça a transparência e a conformidade. Reforce sempre que, as informações do

cliente são tratadas com segurança e apenas utilizadas para fins específicos relacionados ao que se pretende.

4. METODOLOGIA

Para obtermos os resultados esperados, será realizada análise e pesquisa em fontes acadêmicas, legislação, avaliação de normas e regras, decisões judiciais e casos práticos pertinentes acerca da responsabilidade civil das empresas financeiras e delitos cibernéticos.

Estes métodos de pesquisa oferecem uma maneira ampla e detalhada de examinar a responsabilidade legal das instituições diante dos delitos cibernéticos, misturando análises baseadas em teoria, regulamentação e evidências concretas para alcançar resultados importantes e pertinentes.

5. RESULTADOS E DISCUSSÃO

O principal resultado esperado no presente trabalho é a consolidação de um fluxo sólido de ações para prevenção dos crimes cibernéticos por parte das instituições financeiras que incluem identificação de vulnerabilidades, avaliação das medidas atuais adotadas, eficácia da aplicação da LGPD, adoção de tecnologias, conscientização e treinamento.

A identificação detalhada das principais vulnerabilidades nos sistemas de segurança das instituições financeiras, que podem levar ao vazamento de dados dos clientes é um começo interessante para a prevenção contra o crime cibernético. Estudos mostram que a maioria dos incidentes de segurança cibernética em bancos resulta de falhas na segurança interna e de ataques externos sofisticados (Santos, 2021).

Propostas de melhorias específicas e práticas para as instituições financeiras fortalecerem suas defesas contra crimes cibernéticos é essencial. De acordo com Moura e Almeida (2022), a adoção de tecnologias avançadas, como inteligência

artificial e blockchain, podem melhorar significativamente a segurança dos dados financeiros (Moura e Almeida 2022).

O mapeamento do panorama das medidas de segurança atualmente adotadas pelas instituições financeiras, incluindo políticas, protocolos e tecnologias de proteção de dados pode contribuir para motivar a melhoria contínua do sistema de proteção de dados. Segundo Silva e Castro (2020), muitas instituições financeiras ainda não implementaram completamente os requisitos de segurança da LGPD, o que aumenta o risco de incidentes cibernéticos (Silva e Castro 2020).

É de total interesse da instituição financeiro a investigação sobre a eficácia das medidas implementadas em conformidade com a LGPD na redução da incidência de crimes cibernéticos. Estudos de caso e jurisprudências indicam que a conformidade com a LGPD tem um impacto significativo na redução de incidentes de segurança cibernética (Santos, 2021).

Por fim, a capacitação, aplicabilidade e treinamento dos colaboradores, o aumento da conscientização entre as instituições financeiras sobre a importância da conformidade com a LGPD e a adoção de medidas proativas de segurança cibernética é que pode manter a coesão das medidas de proteção. A pesquisa de Lima (2020) destaca que a educação e a reciclagem contínua do treinamento dos funcionários são cruciais para a eficácia das políticas de segurança (Lima 2020).

6. CONSIDERAÇÕES FINAIS

Por fim, é essencial destacar a relevância da responsabilidade civil das organizações financeiras na prevenção e combate aos delitos virtuais. Estratégias como a adoção de medidas de segurança sólidas, investimento em tecnologias de identificação e resposta, juntamente com a instrução e conscientização dos usuários, são essenciais. Êxitos significativos podem ser obtidos na diminuição de ocorrências e prejuízos monetários, assegurando a confiança dos consumidores e a estabilidade do sistema financeiro como um todo. Entretanto, trata-se de um esforço incessante que requer adaptação às novas ameaças virtuais em constante evolução.

REFERÊNCIAS

BRASIL. Lei n. 10.406, de 10 de janeiro de 2002. **Institui o Código Civil**. Diário Oficial da União: seção 1, Brasília, DF, 11 jan. 2002.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro**: Responsabilidade Civil. 38. ed. São Paulo: Saraiva Jur, 2024.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo Mário Veiga. **Novo curso de direito civil**: v. 3. Responsabilidade civil. 22. ed. São Paulo: SaraivaJur, 2024.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro**: Responsabilidade Civil. 19. ed. São Paulo: Saraiva Jur, 2024.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena. **Lei Geral de Proteção de Dados Pessoais e Suas Repercussões no Direito Brasileiro**. São Paulo: Editora Revista dos Tribunais, 2023.

TARTUCE, Flávio. **Responsabilidade Civil**. 5. ed. Rio de Janeiro: Forense, 2023.

SANTOS, Raabe. **A Conformidade com a LGPD e a Redução de Incidentes Cibernéticos**. 2021.

FERNANDES, Antonio. **Tecnologias de Segurança Cibernética para o Setor Financeiro**. 2021.

COSTA, João. **Conscientização e Treinamento de Funcionários para a Prevenção de Crimes Cibernéticos**. 2019.

MOURA, Alfredo; ALMEIDA, Carlos. **Adoção de Inteligência Artificial e Blockchain em Instituições Financeiras**. 2022.

SILVA, Mariana; CASTRO, Roberto. **A Implementação da LGPD em Instituições Financeiras**. on-line: JusBrasil, 2020. Disponível em: <https://www.jusbrasil.com.br>. Acesso em: 10 out. 2024.

LOPES, A. M. **Direito Digital e LGPD na Prática**. São Paulo: Editora Rumo Jurídico, 2021.

TEFFÉ, C. S. de. **A importância da LGPD no contexto da inteligência de dados**. ITS, Rio de Janeiro/RJ, 2022.