UNIVERSIDADE CESUMAR - UNICESUMAR
CENTRO DE CIÊNCIAS HUMANAS E SOCIAIS APLICADAS
CURSO DE GRADUAÇÃO EM DIREITO

CASO BANCO NEON: ANÁLISE DA RESPONSABILIDADE PENAL DAS EMPRESAS EM CASO DE VAZAMENTO DE DADOS PESSOAIS

ISABELLA LAGO TAVEIRA

MARINGÁ – PR
2025

Isabella Lago Taveira

CASO BANCO NEON: ANÁLISE DA RESPONSABILIDADE PENAL DAS EMPRESAS EM CASO DE VAZAMENTO DE DADOS PESSOAIS

Artigo apresentado ao Curso de Graduação em Direito da Universidade Cesumar – UNICESUMAR como requisito parcial para a obtenção do título de Bacharel(a) em Direito, sob a orientação do Prof. Dr. Welington Junior Jorge Manzato.

MARINGÁ – PR

2025

FOLHA DE APROVAÇÃO

ISABELLA LAGO TAVEIRA

CASO BANCO NEON: ANÁLISE DA RESPONSABILIDADE PENAL DAS EMPRESAS EM CASO DE VAZAMENTO DE DADOS PESSOAIS

Artigo apresentado ao Curso de Graduação em Direito da Universidade Cesumar – UNICESUMAR como requisito parcial para a obtenção do título de Bacharel(a) em Direito, sob a orientação do Prof. Dr.Welington Junior Jorge Manzato.

Aprovado em: ____ de _____ de _____.

BANCA EXAMINADORA

_____

Nome do professor – (Titulação, nome e Instituição)

_____

Nome do professor - (Titulação, nome e Instituição)

_____

Nome do professor - (Titulação, nome e Instituição)

CASO BANCO NEON: ANÁLISE DA RESPONSABILIDADE PENAL DAS EMPRESAS EM CASO DE VAZAMENTO DE DADOS PESSOAIS

Isabella Lago Taveira.

Welington Junior Jorge Manzato.

RESUMO

O trabalho intitulado "Caso Banco Neon: Análise da Responsabilidade Penal das Empresas em Caso de Vazamento de Dados Pessoais" tem como objetivo analisar as implicações penais atribuídas a empresas diante do vazamento de dados pessoais de clientes, a partir do estudo do caso recente do Banco Neon. Para alcançar tal finalidade, a pesquisa adotou o método qualitativo, com abordagem indutiva, fundamentando-se na análise de relatórios, notícias, boletins, decisões judiciais e legislação vigente, e empregando a técnica do estudo de caso para examinar, em profundidade, os fatores e desdobramentos do incidente. Os principais resultados apontam que o arcabouço jurídico brasileiro, embora dotado de princípios robustos, revela-se insuficiente e predominantemente reativo frente à velocidade das inovações tecnológicas e à sofisticação dos crimes digitais, particularmente no que concerne à responsabilização objetiva das instituições financeiras, à eficácia das sanções e à dissuasão de condutas negligentes por parte dos gestores. Constatou-se, também, que a insuficiência das medidas preventivas e a baixa efetividade das punições tornam o sistema vulnerável a recorrentes violações de direitos dos titulares de dados, gerando impactos reputacionais, financeiros e sociais para as empresas envolvidas. Conclui-se que, para a consolidação da segurança jurídica e digital, mostra-se imprescindível o aperfeiçoamento da legislação e da aplicação das normas, bem como o investimento contínuo em mecanismos de prevenção, compliance e governança de dados sensíveis, assegurando maior proteção ao consumidor e à coletividade.

Palavras-chave: Compliance. Crimes Digitais. Negligência.

BANCO NEON CASE: ANALYSIS OF CORPORATE CRIMINAL LIABILITY IN CASES OF PERSONAL DATA BREACHES

ABSTRACT

The work entitled "Banco Neon Case: Analysis of Corporate Criminal Liability in Cases of Personal Data Breaches" aims to analyze the criminal implications attributed to companies in the event of customer personal data breaches, based on the study of the recent Banco Neon case. To achieve this objective, the research adopted a qualitative method with an inductive approach, drawing upon the analysis of reports, news articles, bulletins, judicial decisions, and current legislation, and employing the case study technique to examine, in depth, the factors and developments of the incident. The main findings indicate that the Brazilian legal framework, although equipped with robust principles, proves insufficient and predominantly reactive in the face of the speed of technological innovations and the sophistication of digital crimes, particularly regarding the strict liability of financial institutions, the effectiveness of sanctions, and the deterrence of negligent conduct by managers. It was also found that the insufficiency

of preventive measures and the low effectiveness of punishments make the system vulnerable to recurrent violations of data subjects' rights, generating reputational, financial, and social impacts for the companies involved. The study concludes that, for the consolidation of legal and digital security, it is essential to improve legislation and the application of norms, as well as continuous investment in prevention mechanisms, compliance, and governance of sensitive data, ensuring greater protection for consumers and society.

Keywords: Compliance. Digital Crimes. Negligence.

1 INTRODUÇÃO

O presente artigo tem como tema o estudo do caso de vazamento de dados pessoais de clientes do Banco Neon e a análise da responsabilidade penal das empresas e gestores em caso de vazamento de dados. Esse tema é de grande relevância para a área do Direito Digital e à proteção de dados pessoais trazidos pela Lei Geral de Proteção de Dados, uma vez que, apesar dos avanços no que tange a proteção de dados pessoais, muitas empresas ainda enfrentam dificuldades em garantir uma segurança digital rigorosa e eficiente de dados da empresa e de seus clientes. O estudo busca explorar as questões que envolvem os crimes que podem ser atribuídos às empresas e gestores em casos de vazamento de dados pessoais à luz do caso do Banco Neon, uma análise da legislação vigente que regulamenta dados e informações que circulam na rede de internet e seus impactos sobre os crimes cibernéticos e à proteção de dados pessoais, e por fim, analisar a atuação dos tribunais na interpretação das normas penais em casos semelhantes ao do Banco Neon.

Um dos dilemas centrais abordados neste artigo é que apesar de atualmente no Brasil vigorarem diversas leis que garantem a proteção de dados pessoais e regulamentam o uso de dados pessoais na internet, ainda existem diversos casos de vazamento de dados pessoais de empresas gigantes do mercado, devido a brechas na segurança digital, ainda pior devido a penalização mais branda das leis que regulamentam a proteção de dados comparada a outros crimes. Tais desafios têm gerado discussões sobre a eficácia das leis que regulamentam a proteção de dados pessoais, que geram uma insegurança digital constante devido à incerteza de como os dados pessoais têm sido tratados no ambiente da internet. A partir desse cenário, surge o seguinte problema de pesquisa: Em um cenário de acelerado crescimento da tecnologia e uso da internet, o Direito precisa acompanhar a evolução de como diversos crimes têm sido praticados, e em casos como o do Banco Neon, como as empresas têm sido responsabilizadas pelo vazamento de informações sensíveis? Essa responsabilização tem sido eficaz ou indiferente para gerar uma verdadeira mudança digital nas empresas?

Diante disso, este artigo propõe um estudo do caso do Banco Neon e a análise da responsabilidade penal das empresas em caso de vazamento de informações pessoais. O principal objetivo deste trabalho é analisar as implicações penais das empresas que têm dados pessoais de seus clientes vazados, à luz do caso do Banco Neon, buscando compreender a aplicação da legislação penal em casos semelhantes, em especial no que tange aos crimes cibernéticos. Além disso, busca-se também avaliar, conjuntamente a possibilidade de

responsabilidade dos gestores e representantes legais, considerando o grau de envolvimento, bem como analisar a legislação vigente que regulamenta a proteção de dados digitais.

A contribuição deste estudo reside no fato de que casos como o do Banco Neon evidenciam a fragilidade das empresas no que tange a segurança de informações pessoais e sensíveis e a necessidade de uma legislação mais eficaz em lidar com os crimes digitais. Ao abordar a responsabilidade penal de empresas que têm dados vazados semelhantemente ao Banco Neon, espera-se que este artigo ofereça novas perspectivas sobre a responsabilização penal das empresas e seus gestores, buscando uma maior proteção aos direitos fundamentais, bem como podendo contribuir cientificamente ao trazer à luz problemáticas acerca do assunto de proteção de dados pessoais. Isso será fundamental para uma melhor adequação das empresas às normas vigentes que regulamentam a proteção de dados pessoais e a consciência da necessidade de uma segurança digital mais reforçada, garantindo segurança jurídica não apenas aos seus clientes, mas à própria empresa para que atue com mais confiança.

O principal objetivo deste trabalho é analisar as responsabilidades penais que podem ser atribuídas a empresas em caso de vazamento de dados pessoais, à luz do caso do Banco Neon. Especificamente, busca-se entender os crimes que podem ser atribuídos às empresas em casos semelhantes, a legislação vigente e seu impacto e força, bem como a interpretação dos tribunais e as jurisprudências obtidas em casos iguais aos do Banco Neon.

Para alcançar os objetivos propostos, o estudo utilizará o método qualitativo, adotando a metodologia indutiva, que consiste em analisar o caso particular do Banco Neon, para, ao fim, chegar em uma conclusão geral. Os dados serão coletados através de relatórios, jornais, boletins, portais dos tribunais, e analisados com base na técnica de estudo de caso, visando nos aprofundar no caso de vazamento de dados do Banco Neon, permitindo a identificação de fatores que podem influenciar casos semelhantes.

Embora o estudo ainda esteja em andamento, espera-se que as conclusões forneçam embasamento científico e concreto às empresas brasileiras que lidam com dados pessoais e sensíveis, a entenderem a necessidade do investimento na segurança dos dados pessoais administrados pelas empresas, garantindo segurança digital. Acredita-se que, ao investigar o caso de vazamento de dados do Banco Neon e os crimes que podem ser atribuídos aos gestores e a própria empresa, será possível trazer à luz a fragilidade das empresas na proteção de dados pessoais, tendo em vista que ainda é corriqueiro o vazamento de dados sensíveis por empresas, onde muitas vezes, os proprietários dos dados sequer têm consciência do vazamento e uso indevido de seus dados. Isso poderá gerar uma conscientização pessoal de como nossos dados têm sido tratados, os direitos e garantias previstos na constituição pátria e legislação vigente

acerca de dados pessoais e como devemos ter cuidados ao compartilhar dados sensíveis. No âmbito empresarial, a presente pesquisa poderá ter um impacto significativo, tendo em vista que são poucas as empresas que investem com prioridade na proteção de dados pessoais de seus clientes e dados da própria empresa. Tal investimento, atualmente, se mostra não apenas como uma recomendação, mas como uma necessidade, diante dos crescentes avanços dos crimes praticados do âmbito digital envolvendo dados empresariais e pessoais.

É necessário que as empresas tenham consciência de como as leis penais e digitais têm sido aplicadas em casos concretos como o do Banco Neon, para que entendam o impacto social e financeiro em casos de vazamento de dados, podendo até mesmo afetar de forma irreversível o prestígio e confiança de uma empresa aos olhos de seus clientes. É necessário a adequação empresarial à luz da legislação vigente, e um maior investimento no ramo da segurança digital dos dados sensíveis circulados pela empresa, um diferencial no mercado atual.

2 A EVOLUÇÃO DOS CRIMES DIGITAIS: UMA ANÁLISE HISTÓRICA E LEGISLATIVA

No presente artigo, o tema abordado acerca da análise da responsabilidade penal das empresas em caso de vazamento de dados pessoais, à luz do caso do Banco Neon, que tem sido amplamente discutido na literatura jurídica devido à sua relevância para o Direito Digital e o avanço deste campo do direito. O referencial teórico, fundamentado em autores como Pedro Augusto Zaniolo, Patrícia Peck Pinheiro, Joaquim Leitão Júnior, é essencial para embasar as ideias apresentadas e garantir a consistência argumentativa do trabalho. Através da análise de diferentes perspectivas teóricas, busca-se construir uma base sólida para a compreensão do tema, explorando as contribuições mais relevantes na área. A literatura existente sobre o vazamento de dados pessoais e suas implicações será utilizada para contextualizar e aprofundar a discussão proposta, demonstrando a importância deste estudo para o campo jurídico.

A princípio, antes de destrincharmos o caso objeto desta pesquisa, e consequentemente iniciarmos uma discussão acerca dos crimes digitais que abarcam o referido caso, é necessário entender inicialmente o surgimento e avanço da internet, concomitantemente ao surgimento dos crimes digitais, para, assim, traçarmos uma linha evolutiva para compreendermos claramente como chegamos até este estudo acerca dos crimes digitais. Além disto, é imperioso compreender a definição dos crimes digitais, para então, podermos nos aprofundar no caso do Banco Neon, objeto desta pesquisa, e entender o arcabouço legislativo regulamentadores dos crimes abarcados pelo caso.

O primeiro registro de interações online se deu na década de 1960, mais especificamente em 1962, por uma série de mensagens escritas por J. C. R. Licklider. Mais tarde, em 1965, após Licklider convencer o pesquisador Lawrence G. Roberts acerca da importância destas interações online, Roberts, junto a outro pesquisador, realizaram a primeira conexão entre dois computadores em localidades diferentes. Após a descoberta, Roberts foi para DARPA (*Defense Advanced Research Projects Agency*), uma agência governamental de pesquisa para o uso militar dos Estados Unidos, no qual trabalhou para o desenvolvimento da primeira rede de internet que estava para nascer, chamada "ARPANET", publicada em 1967, usada para o envio de informações entre o centro de pesquisa e o Pentágono.

Com o desenvolvimento da estrutura da "ARPANET", a agência DARPA criou então o programa *Interface Message Processors* (IMP's), uma tecnologia de redes que transmite dados dividindo-os em pequenos "pacotes". O primeiro IMP instalado se deu na Universidade da Califórnia, em Los Angeles (UCLA), e o segundo no Centro de Pesquisa de Stanford (SRI), onde foram enviadas as primeiras mensagens online. Ao longo dos anos, diversos computadores foram adicionados a rede "ARPANET", continuando a usarem o sistema "*Host-to-host*", uma ligação direta entre servidores de diferentes lugares. Em 1972 se deu início ao eletronic mail, popularmente conhecido como e-mail, uma das maiores aplicações online durante mais de uma década, o que levou ao nascimento em 1991, por Tim Berners-Lee, do *World Wide Web* (WWW), o meio de comunicação global através de computadores conectados à internet.

Os crimes, no geral, são comportamentos que fazem parte da sociedade, tipificados em diversos dispositivos legislativos. Com o nascimento da internet, houve também o nascimento de um espaço diverso para que os crimes aconteçam: "[...] os crimes cibernéticos são os delitos cometidos por pessoas por intermédio do uso de computadores e/ou dispositivos conectados a uma rede de conexão." (PECK, 2021, p.3).

Ao contrário do que se imagina, os crimes digitais não tiveram início apenas com a criação do *World Wide Web*, mas sim, paralelamente ao desenvolvimento da rede de internet. Peck (2021) traz que os primeiros registros de crimes realizados no âmbito da internet surgiram na década de 1970, no qual computadores começaram a ser usados em tentativas de invasão de sistemas, sem necessariamente ter uma intenção maliciosa ou lucrativa, visto que não era ainda uma realidade globalizada.

No entanto, nas décadas seguintes os crimes foram se diversificando, iniciando-se a pirataria de programas, invasões em sistemas, golpes e manipuladores de rede bancária, *phishing*, *malwares*, vírus de computadores, entre outros.

Diante dos avanços do crime cibernético em todo o mundo com o avanço da globalização digital, se tornou necessário regulamentar e tipificar condutas realizadas no âmbito da internet, antes não previstas no Código Penal (1940). Com isto, surgiu a Lei 12.737 de 2012, apelidada de “Lei Carolina Dieckmann”, que surgiu após a invasão do computador da atriz Carolina Dieckmann, na qual um hacker roubou fotos íntimas, usando-as como chantagem financeira para a não divulgação das fotos. No referido caso, a atriz se recusou a fornecer o pagamento ao hacker e teve suas fotos espalhadas por toda a internet, o que gerou grande comoção nacional e levou a criação da referida lei, um grande avanço legislativo no âmbito de crimes cibernéticos. A Lei 12.737/2012 foi a primeira lei que tipifica exclusivamente crimes cometidos no ambiente digital.

Já em 2014, nasceu a “Constituição” dos crimes digitais, a Lei nº 12.965 de 2014, o “Marco Civil da Internet”, na qual abarca princípios, garantias, direitos e deveres para o uso e regulamentação da internet no Brasil. Apesar de um grande marco na regulamentação do uso da internet, a lei não trouxe menção à crimes digitais, mas trouxe a positivação de um importante princípio: a proteção de dados pessoais.

Em 2018 então, surge, inspirada na *General Personal Data Protection*, uma lei europeia, a Lei Geral de Proteção de Dados Pessoais (LGPD). A Lei 13.709/2018 abarcou acerca da proteção e tratamento de dados pessoais nos meios digitais, trazendo alguns fundamentos positivados também na Lei 12.965/2014.

Nesta toante acerca da proteção de dados pessoais, chegamos ao caso objeto desta pesquisa. No início de 2025, o Banco Neon teve os dados pessoais de mais de 30 milhões de clientes vazados em uma postagem cibercriminosa, o que levou a preocupações sobre a conformidade com a Lei Geral de Proteção de Dados.

Diante do cenário atual de crescimento de ataques e golpes ligados a instituições financeiras, a presente pesquisa se faz necessária para analisarmos a legislação atual à luz de um caso tão recente, e que pode levar a consequências bilionárias. O caso do Banco Neon não é um caso isolado, o que tem gerado insegurança por parte dos usuários de bancos digitais. Analisar o caso do Banco Neon nos auxilia em entender que apesar dos grandes avanços legislativos, diversas empresas ainda carecem de medidas rigorosas de proteção de dados de clientes, o que gera consequências para a própria empresa, diante do alto gasto despendido em caso de vazamento de dados, bem como aos usuários, diante da existência de algumas lacunas legislativas e a branda penalização tipificada nas leis.

A presente pesquisa traz à existência o debate acerca de como o Banco Neon e outras empresas serão e podem ser responsabilizadas em caso de vazamento de dados pessoais, trazer

à luz problemáticas na proteção de dados pelas empresas, bem como a aplicação das normas que regulamentam crimes digitais e outras normas análogas pelo judiciário. Por fim, a presente pesquisa se mostra relevante para auxiliar usuários do meio digital a conhecerem o que a legislação atual protege e como ela tem sido aplicada, além de guiar diversas empresas ao estudo e ao entendimento da importância do investimento em proteção de dados pessoais, os gastos despendidos na responsabilização em caso de vazamento e a devida adequação à legislação atual, garantindo, portanto, a segurança jurídica e digital.

Portanto, passaremos a analisar, à luz do caso do Banco Neon, os crimes que podem ser atribuídos às empresas em caso de vazamento de dados pessoais de seus clientes, bem como a possível responsabilização dos gestores e programadores do banco de dados das empresas. Iremos analisar também, a legislação vigente e seu impacto e proteção no que tange aos crimes digitais e à proteção de dados pessoais, e por fim, analisar na prática, a interpretação dos Tribunais e aplicação das normas em casos semelhantes, fundamentais para entender possíveis lacunas normativas, trazendo uma maior concretização da proteção de dados pessoais no Brasil.

2.1 O Caso do Banco Neon e uma Análise da Responsabilidade das Instituições Financeiras

Na data de 15 de fevereiro de 2025, milhões de clientes do banco digital Neon receberam um e-mail informando que o banco havia tomado conhecimento de uma possível cópia indevida de dados pessoais de seus clientes. Eis que então, surge a notícia: no dia 09 de fevereiro de 2025 o banco Neon sofreu um ataque cibernético por um hacker, que resultou no vazamento de dados pessoais de milhões de clientes do banco. O próprio banco informou os clientes que os seguintes dados foram copiados: Nome, CPF, e-mail, telefone, nome do pai e nome da mãe, mas assegurava serem dados “simples”.

Na mesma semana, o jornalista Felipe Payão, especialista em cibersegurança, publicou uma matéria surpreendente sobre o caso. O jornalista afirma ter recebido um link de um colega, que direcionava a um fórum hacker bem reconhecido na comunidade do cibercrime. No link, era possível constatar uma publicação com dados de 30 milhões de clientes do banco. Verificou-se que os dados que o Banco Neon afirmou terem sido copiados, era apenas uma parte deles. Na postagem no fórum hacker é possível verificar os seguintes dados: sexo, CEP, profissão, renda, saldo, número da conta, fotos (*selfies*), imagens de documentos, e até mesmo o modelo do aparelho celular usado pelo cliente.

O jornalista também teve uma conversa com o suposto hacker que vazou os dados dos clientes do banco, que se identifica como Pegasus. O hacker afirma que o vazamento ocorreu após sua insatisfação com o Banco Neon, após o mesmo ter identificado uma falha de domínio no sistema da instituição bancária, e, após entrar em contato com o banco buscando uma recompensa - ou *bug bounty* - o banco se recusou a fornecer o pagamento. Desta forma, o hacker fez a publicação no fórum hacker, e surpreendentemente, enviou diversos SMS's para os clientes titulares dos dados, informando que os dados haviam sido expostos.

É necessário entender também, o que significa *bug bounty*: são programas na qual pesquisadores de segurança fazem testes de invasão e extração de informações de forma controlada, com o fim de corrigir vulnerabilidades e erros dos sistemas de empresas que aderem ao programa. A prática é comum nos Estados Unidos, onde empresas como *Google*, *Microsoft*, *Facebook*, e até mesmo órgãos públicos do país possuem o programa *bug bounty*. Uma das vantagens da prática do *bug bounty* é que a empresa que adota o programa está constantemente aprimorando a segurança das suas redes e dados, antes que criminosos possam detectá-las, podendo ser até mesmo uma alternativa mais acessível, tendo em vista que a multa por vazamento de dados pode ser assustadora.

No site *Google Bug Hunters*, é possível analisar as regras do programa junto a empresa Google. O site traz as regras para pesquisar falhas nos produtos da Google, ajudando-os a manter a segurança e proteção, traz vídeos explicativos de como o programa de prêmios funciona, um formulário para reportar as falhas de maneira formal, e até mesmo dicas do próprio time da Google do que procurar nos aplicativos e sites.

No Brasil, atualmente, não existem normas ou programas que regulamentam o bug bounty. A Lei Geral de Proteção de Dados, em seu artigo 6º traz a positivação de dois princípios importantes - o da segurança e da prevenção - que assegura a adoção de medidas preventivas para ocorrência de vazamento de dados e a utilização de medidas de proteção aos dados pessoais de acessos não autorizados. O artigo 46 do mesmo diploma legal determina que os agentes de tratamento de dados pessoais devem adotar medidas de segurança aptas a proteger os dados pessoais. No entanto, em contrapartida, o Código Penal traz em seu artigo 154-A, incluído pela Lei Carolina Dieckmann, a criminalização da invasão de dispositivo informático com o fim de obter dados ou informações sem autorização expressa do usuário do dispositivo, com aumento de pena de um a dois terços em caso de divulgação desses dados ou informações obtidas.

Isto posto, é possível chegar às seguintes conclusões: Apesar de o *bug bounty* ser uma prática vantajosa à diversas empresas, no Brasil não é tão simples assim, sendo necessário ter autorização expressa dos usuários e da organização, com o fim de garantir a atuação dos

pesquisadores de segurança de maneira ética. O *bug bounty* não é ilegal, mas precisa ser realizado com regulamentação específica e autorização explícita. Isso nos leva ao caso do Banco Neon. Apesar da boa intenção de diversos pesquisadores de segurança, chamados de "hackers do bem", para a prática não ser considerada crime no Brasil, é necessário permissão formal do banco para a realização de testes, o que não foi o caso do hacker do Banco Neon. Outro ponto foi que, o hacker afirmou não ter entregue a falha encontrada para a instituição bancária, o que impediu o banco de realizar as medidas corretivas para garantir a segurança dos clientes. Além disto, a agravante que definitivamente tira o caso do Banco Neon de ser um *bug bounty*, é que após o banco ter negado o pagamento ao hacker que encontrou a falha, este realizou o compartilhamento de dados dos clientes em fórum hacker, configurando o aumento de pena tipificado no artigo 154-A, parágrafo 4º do Código Penal.

Apesar da intenção do hacker do banco Neon na divulgação dos dados, fosse chamar a atenção das empresas acerca das falhas no sistema e a falta de remuneração ou recompensa dos pesquisadores que gastam tempo procurando-as, ele nos trouxe outro ponto a ser discutido, tema central desta pesquisa. O vazamento de dados sensíveis de clientes do Banco Neon não foi um caso isolado. No ano de 2025 foram registrados vazamentos de dados em empresas como Banco XP, Correios, e até mesmo o Conselho Nacional de Justiça. Isso evidencia a vulnerabilidade e falhas na segurança digital em empresas que possuem milhões de clientes.

O vazamento de dados em si é um dano considerado de primeiro nível, conforme determina Peck (2021), o risco, na verdade, mora na natureza dessas informações vazadas. A depender do tipo da informação, elas podem gerar um efeito cascata que geram diversos danos aos clientes e a própria reputação da empresa.

Nos últimos anos, diversos estudos têm explorado o tema da segurança de dados e a responsabilidade das instituições financeiras em caso de vazamento de dados, tem ganhado novas abordagens e contribuições significativas. Estudos recentes, como os de Patrícia Peck (2021), trouxeram avanços ao discutir a necessidade de uma cultura de segurança proativa nas empresas. Além disso, pesquisas conduzidas por Pedro Augusto Zaniolo (2021) exploraram a dificuldade de tipificação dos novos crimes cibernéticos, enfatizando a importância de mecanismos de rastreabilidade. De acordo com Cueva e Frazão (2021), a relevância do tema tem sido intensificada por incidentes de segurança em bancos digitais, o que reflete uma lacuna na literatura jurídica e regulatória. Esses estudos destacam a crescente atenção ao tema, demonstrando sua importância para o direito digital, especialmente no que diz respeito à defasagem da legislação frente à inovação tecnológica.

As teorias discutidas ao longo deste trabalho têm sido amplamente aplicadas em processos judiciais contra instituições financeiras. No campo jurídico, autores como Cueva e Frazão (2021) discutem como a teoria do risco da atividade é aplicada em casos de fraudes e vazamento de dados de clientes, auxiliando na resolução de disputas sobre a responsabilidade objetiva do fornecedor. Além disso, a aplicação dessa teoria pode ser observada em decisões da ANPD e do Poder Judiciário, em que, conforme aponta Peck (2021), a responsabilidade das empresas é avaliada com base na adequação de suas medidas técnicas. A conexão entre teoria e prática é fundamental para entender como o arcabouço legal brasileiro se mostra insuficiente, como adverte Zaniolo (2021) ao tratar da agilidade dos crimes digitais.

Em síntese, o referencial teórico com base em Peck (2021), Zaniolo (2021), e Cueva e Frazão (2021), oferece uma base para a compreensão crítica do tema da responsabilidade do setor financeiro frente a incidentes de segurança. As teorias discutidas foram fundamentais para esclarecer a obrigação legal das empresas em proteger dados, mas também para expor a precariedade da lei diante de novos avanços da tecnologia como a IA e *deepfakes* em fraudes bancárias. As contribuições trazidas pelos autores reforçam a relevância deste estudo e a tese de que a legislação brasileira caminha a passos lentos comparados a tecnologia.

Com o intuito de reunir e analisar conhecimentos produzidos sobre a responsabilidade das instituições financeiras em vazamento de dados, adotou-se a pesquisa bibliográfica. De acordo com Gil (2008), isso implicou o levantamento de publicações sobre o tema, buscando analisar as contribuições teóricas existentes.

Serviram-nos como fontes a Biblioteca Digital Brasileira de Teses e Dissertações, o Banco de Teses e Dissertações da Universidade Unicesumar, além dos bancos eletrônicos SciELO, Google Scholar. As obras chaves de Peck (2021), Zaniolo (2021), e Cueva e Frazão (2021) foram os pilares para a estrutura desta pesquisa.

A pesquisa desenvolvida, organizou-se ao redor da palavra-chave “vazamento de dados” e “responsabilidade penal”, presente nos títulos, resumos e palavras-chave.

O conjunto de materiais encontrados nos levou a organizar sua divisão em três agrupamentos. No primeiro, reunimos pesquisas que oferecem um panorama geral sobre as consequências financeiras e reputacionais para os bancos. Em seguida, trazemos a literatura que versa sobre a temática da negligência na gestão de segurança de dados sensíveis. Por último, analisaremos a problemática da aplicação precária das sanções da LGPD e do Marco Civil frente à agilidade das inovações tecnológicas em fraudes financeiras.

2.2 Consequências dos Vazamentos de Dados no Setor Financeiro

Os vazamentos de dados no setor financeiro brasileiro têm assumido proporções alarmantes, gerando consequências que transcendem os prejuízos monetários imediatos. O caso mais emblemático ocorreu em 2025, quando o ataque cibernético contra a empresa C&M Software resultou no desvio de valores estimados em mais de R$3 bilhões, configurando-se como o maior cibercrime financeiro já registrado no país.

As consequências reputacionais representam um dos aspectos mais devastadores desses incidentes. Como observado por Peck (2021), a confiança do consumidor constitui elemento crucial para a sustentabilidade do setor bancário, e a incapacidade de assegurar proteção adequada pode resultar na migração massiva de clientes. O vazamento de 46 milhões de chaves Pix em julho de 2025, que afetou mais de 11 milhões de pessoas através do sistema Sisbajud do CNJ, demonstrou como falhas na segurança digital podem abalar a confiança no sistema financeiro nacional.

No aspecto financeiro, o impacto é igualmente severo. Segundo dados recentes, o custo médio de um vazamento de dados no Brasil atingiu R$6,7 milhões por incidente em 2024. Este valor contempla não apenas os custos diretos de recuperação técnica, mas também despesas com notificação de clientes, investimentos emergenciais em segurança, custos de imposições penais relacionadas à LGPD e perda de receita durante os períodos de inatividade. As instituições financeiras, além desses custos, enfrentam multas regulatórias que podem alcançar 2% do faturamento bruto anual, limitadas a R$50 milhões por infração.

As consequências operacionais, incluindo a perda de clientes, manifestam-se de forma particularmente severa no setor financeiro. Conforme documentado em casos judiciais, a vulnerabilidade dos consumidores frente às fraudes resulta não apenas em perdas financeiras diretas, mas também em danos morais decorrentes da angústia e insegurança geradas. A ausência de medidas efetivas por parte das instituições configura falha grave na prestação de serviços, acarretando responsabilização civil objetiva conforme estabelece o Código de Defesa do Consumidor.

2.3 Análise Custo-Benefício: O Paradoxo do Investimento Preventivo

A análise econômica dos investimentos em segurança digital versus os custos de incidentes revela um paradoxo alarmante no setor financeiro brasileiro. Enquanto um teste de penetração (pentest) custa em média R$15 mil, o custo médio de um vazamento de dados atinge

R$6,7 milhões. Esta disparidade representa um retorno sobre investimento (ROI) extraordinário: para cada R$1 investido em pentest, uma empresa pode economizar potencialmente R$447 em custos de violação.

Casos reais no setor bancário ilustram tragicamente essa equação. O BTG Pactual, por exemplo, teve 8.032 chaves Pix expostas devido a falhas pontuais em seus sistemas. Embora a instituição tenha negado invasão de sistemas, o incidente evidenciou vulnerabilidades que poderiam ter sido identificadas preventivamente através de auditorias de segurança adequadas.

No contexto brasileiro, estudos com 450 empresas paulistas revelaram que pequenas e médias empresas são as mais vulneráveis, utilizando estratégias básicas de phishing que poderiam ser facilmente mitigadas através de treinamentos e protocolos de segurança adequados.

A análise teórica desta disparidade, conforme apontado por Cueva e Frazão (2021), revela que a implementação de programas de compliance robustos não apenas mitiga riscos, mas também demonstra a adoção do princípio da *accountability* previsto na LGPD. O investimento preventivo em segurança representa apenas 0,22% do custo médio de um vazamento, tornando inexplicável a resistência de algumas instituições em adotar medidas proativas.

2.4 Responsabilidade Civil e Caracterização de Negligência

A ausência de medidas de segurança robustas nas instituições financeiras tem sido consistentemente caracterizada pelos tribunais brasileiros como negligência e imprudência. A jurisprudência consolidada do Superior Tribunal de Justiça, através da Súmula 479, estabelece que "as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias".

A teoria do risco da atividade, amplamente adotada pelos tribunais, determina que aquele que exerce atividade econômica assume os riscos inerentes. No contexto das instituições financeiras, conforme observado por Zaniolo (2021), a digitalização dos serviços bancários criou novos vetores de risco que exigem medidas de segurança proporcionais. A falha em implementar tais medidas configura inadimplemento contratual, atraindo responsabilidade indenizatória independentemente da demonstração de culpa.

Casos paradigmáticos demonstram como a negligência é caracterizada. Alguns tribunais têm reconhecido que instituições que tiveram dados de clientes vazados, falharam ao não implementar adequadamente camadas de segurança para cadastro de usuários e mecanismos de

prevenção a fraudes. A decisão enfatizou que não é aceitável afastar a responsabilidade do banco por culpa exclusiva do consumidor quando existem vulnerabilidades técnicas nos sistemas.

A responsabilização civil, segundo Peck (2021), transcende a mera aplicação de penalidades, constituindo um incentivo econômico para que as instituições invistam adequadamente em segurança, estabelecendo um ciclo virtuoso de prevenção e proteção.

2.5 Legislação Brasileira Acerca da Proteção de Dados

A Lei Geral de Proteção de Dados (LGPD), vigente desde 2020, representa o marco regulatório mais significativo na proteção de dados pessoais no Brasil. A legislação estabelece princípios fundamentais como finalidade, necessidade e segurança, impondo às instituições financeiras o dever de implementar medidas técnicas e organizacionais adequadas. Contudo, conforme evidenciado pelos crescentes incidentes, a lei apresenta limitações práticas na sua aplicação ao setor financeiro.

O Marco Civil da Internet (Lei 12.965/2014) complementa esse arcabouço ao regular questões processuais criminais referentes à preservação de provas digitais. O artigo 15 estabelece o dever de guarda e retenção de registros de acesso sob sigilo, criando instrumental probatório essencial para investigações de crimes cibernéticos. No entanto, como observa Zaniolo (2021), a legislação não acompanha a agilidade das inovações tecnológicas utilizadas por criminosos.

A Lei Carolina Dieckmann (Lei 12.737/2012), primeira lei brasileira a tipificar crimes cibernéticos, inseriu no Código Penal o crime de invasão de dispositivo informático. Atualizada pela Lei 14.155/2021, aumentou as penas de detenção de três meses a um ano para reclusão de um a quatro anos. Apesar dos avanços, especialistas apontam sua generalidade como principal limitação, faltando especificação técnica adequada para enfrentar os crimes modernos.

A análise específica dos artigos sobre responsabilidade revela insuficiências estruturais. O artigo 52 da LGPD prevê sanções administrativas que incluem multas de até 2% do faturamento, limitadas a R$50 milhões por infração, conforme já demonstrado. Contudo, muitas vezes essas multas vêm em valores extremamente abaixo do limite legal, demonstrando tímida aplicação do poder sancionatório.

No contexto das instituições financeiras, a Resolução 347/2023 do Banco Central estabelece obrigações mais rígidas que a própria LGPD para comunicação de incidentes envolvendo dados do PIX. A norma exige comunicação aos titulares mesmo quando não há

risco relevante, contrastando com a LGPD que só obriga comunicação em casos de risco efetivo.

A insuficiência das sanções torna-se evidente quando confrontada com a magnitude dos prejuízos. Como observado por Cueva e Frazão (2021), a ausência de regulamentação efetiva compromete a dissuasão necessária para transformar comportamentos corporativos.

A análise do panorama regulatório brasileiro revela uma característica preocupante: a legislação é fundamentalmente reativa, respondendo a crises ao invés de antecipar desenvolvimentos tecnológicos. Como argumenta Peck (2021), esta postura reativa cria janelas de vulnerabilidade que são sistematicamente exploradas por criminosos cibernéticos.

Conforme documenta Zaniolo (2021), enquanto crimes digitais mostram-se extremamente atrativos (baixo risco físico, poucos envolvidos, altos valores), a legislação penal ainda prevê penas de 1 a 5 anos, contrastando com mais de 15 anos para crimes presenciais como o assalto ao Banco Central de Fortaleza em 2005. Esta disparidade punitiva incentiva a migração criminosa para o ambiente digital.

A velocidade da inovação tecnológica supera consistentemente a capacidade regulatória. A introdução do PIX, lançado em 2020, já registrou múltiplos incidentes de segurança sem que houvesse tempo hábil para o desenvolvimento de arcabouço regulatório adequado. Tecnologias emergentes como inteligência artificial e *deepfakes* em fraudes bancárias permanecem em zona cinzenta regulatória, criando brechas sistematicamente exploradas. Como observam Cueva e Frazão (2021), a ausência de punições efetivas perpetua um ciclo de complacência corporativa que mantém vulnerabilidades sistêmicas.

Esta análise sustenta inequivocamente a tese de que a legislação atual é precária diante da rápida evolução tecnológica. As brechas regulatórias não são acidentes isolados, mas consequência estrutural de um sistema jurídico que prioriza respostas pontuais sobre estratégias preventivas abrangentes. O setor financeiro permanece vulnerável devido a este atraso entre progresso tecnológico e adequação regulatória.

A modernização urgente do arcabouço legal, incluindo harmonização entre diferentes esferas regulatórias, a maior eficiência das penalidades e criação de mecanismos preventivos específicos para o setor financeiro, constitui uma necessidade não apenas jurídica, mas de segurança nacional na era da economia digital.

3 APRESENTAÇÃO DOS DADOS (RESULTADOS)

A visão socioeconômica apresentada no **primeiro agrupamento**, traz justamente uma identificação das profundas consequências, tanto financeiras quanto reputacionais, que o vazamento de dados impõe às instituições financeiras. Falar sobre as consequências do vazamento de dados implica, necessariamente, compreender a perda de confiança do consumidor, os custos altíssimos para remediação, e a escolha economicamente irracional em não investir em uma segurança preventiva.

No **segundo agrupamento**, os trabalhos que abordam mais profundamente as questões da responsabilidade civil e da negligência corporativa, isso implica reconhecer a consolidação de um entendimento jurídico que atribui o risco da atividade ao próprio negócio. Desse modo, evidenciam um conjunto de conceitos, ideias e valores implícitos que posicionam a segurança de dados não como um custo opcional, mas como um dever intrínseco à prestação de serviços financeiros na era digital, cuja falha configura imprudência e gera o dever de indenizar.

Por fim, no **terceiro agrupamento**, procuramos mostrar que o arcabouço legal brasileiro, embora robusto em seus princípios, é reativo e lento em sua aplicação prática. As investigações em Direito Digital apresentadas figuram apenas os primeiros passos de estudos exploratórios sobre um universo que demanda atenção. No que se refere à efetividade da legislação de proteção de dados no setor financeiro, são ainda numerosas as questões a perscrutar. Entre elas, podemos analisar primeiramente o crescimento da utilização de Inteligência Artificial e *deepfakes* em fraudes bancárias e a iminente necessidade de novas abordagens na tipificação de crimes digitais nessa vertente, trazendo mais clareza e especificidade legislativa na atribuição da responsabilidade. Outro ponto a ser analisado, é como o ordenamento jurídico pode se antecipar às novas ameaças cibernéticas, ao invés de apenas reagir a elas, promovendo assim, um ambiente de inovação seguro com uma regulamentação mais adequada. E por fim, algo de extrema importância para uma efetividade maior da legislação de proteção de dados, poderia ser a colaboração entre órgãos reguladores - como Banco Central e ANPD - e o Poder Judiciário, para uma aplicação de sanções previstas nas leis de proteção de dados de forma mais célere e eficaz.

CONCLUSÃO

Em suma, desenvolver um enfoque sobre a responsabilidade penal por vazamento de dados, a partir do caso do Banco Neon, significa avaliar a ineficácia da legislação atual frente aos crimes cibernéticos. O panorama da produção científica acerca do tema aponta para a necessidade do empreendimento de estudos sobre a real capacidade dissuasória das sanções, que nos permitam conhecer suas falhas e propor aprimoramentos.

O presente artigo buscou abordar a responsabilização de empresas e gestores por vazamentos de dados, questionando se as leis vigentes, como a LGPD, são eficazes para promover uma mudança real na segurança digital. A pesquisa revelou que, apesar de legislação específica sobre o tema, sua aplicação é reativa e branda. A responsabilidade civil é consolidada, mas a responsabilização penal ainda enfrenta desafios práticos, o que reduz o poder de intimidação da lei.

Este trabalho contribui para a literatura ao conectar a teoria do risco da atividade com a governança de dados, reforçando que a falha em investir em segurança constitui uma negligência juridicamente punível. Os resultados desta pesquisa têm implicações práticas para gestores, que devem tratar a segurança como pilar estratégico, e para operadores do Direito, que precisam aplicar as normas com maior rigor para refletir a gravidade dos danos.

Apesar das contribuições, o estudo apresenta algumas limitações, como a análise de um caso hipotético, o que impede o acompanhamento de um processo judicial real e seus desdobramentos concretos. Pesquisas futuras podem explorar o impacto de novas tecnologias em fraudes, como IA e *deepfakes*, e analisar de forma comparativa a eficácia das sanções aplicadas pela ANPD e pelo Judiciário.

O impacto desta pesquisa se dá no campo do Direito Digital, ao evidenciar a defasagem entre a velocidade do avanço tecnológico criminoso e a lentidão da resposta legislativa e judicial. Em síntese, este trabalho demonstrou que a proteção de dados no Brasil, embora bem fundamentada em princípios, carece de efetividade sancionatória. Conclui-se, portanto, que a segurança dos cidadãos depende de uma aplicação da lei mais ágil e rigorosa.

REFERÊNCIAS

ALEXANDRE, Brenda Cristina; ARAÚJO, Giulianna Martins; orientador RABELO, Cesar Leandro de Almeida. **A evolução dos crimes cibernéticos e os desafios da legislação brasileira**. Revista Finitude do Trabalho (Revista FT), v. 2, n. 1, 2023. DOI: 10.5281/zenodo.10223548. Disponível em: https://revistaft.com.br/a-evolucao-dos-crimes-ciberneticos-e-os-desafios-da-legislacao-brasileira/. Acesso em: 16 set. 2025.

BANCO Neon: **vazamento de dados expõe informações de clientes**. DPO Expert, 2025. Disponível em: https://dpoexpert.com.br/vazamento-dados-banco-neon/. Acesso em: 16 set. 2025.

BRASIL**. Lei nº 12.737**, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nş 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Lei Carolina Dieckmann. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 16 set. 2025.

BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Marco Civil da Internet. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 16 set. 2025.

BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. Dispőe sobre a proteção de dados pessoais e altera a Lei nş 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 16 set. 2025.

BUGHUNTERS. **Google**. Disponível em: https://bughunters.google.com/. Acesso em: 16 set. 2025.

CASO NEON: **banco revela primeiros detalhes de roubo de dados**. Tecnoblog, 15 fev. 2025. Disponível em: https://tecnoblog.net/noticias/caso-neon-em-novo-email-banco-revela-primeiros-detalhes-sobre-roubo-de-dados/. Acesso em: 16 set. 2025.

COMETTI, Marcelo Tadeu. **Vazamento de dados bancários**: responsabilidades jurídicas e medidas. Legale, 2025. Disponível em: https://legale.com.br/blog/vazamento-de-dados-bancarios-responsabilidades-juridicas-e-medidas/. Acesso em: 16 set. 2025.

CRIMES cibernéticos: **a evolução da tecnologia da informação**. JusBrasil, 2023. Disponível em: https://www.jusbrasil.com.br/artigos/crimes-ciberneticos-a-evolucao-da-tecnologia-da-informacao/1166686576. Acesso em: 16 set. 2025.

FRAZÃO, Ana (Coord.); CUEVA, Ricardo Villas Bôas (Coord.). **Compliance e políticas de proteção de dados**. São Paulo: Revista dos Tribunais, 2021.

FURTADO, Marina. **Packet Switching**: o pilar da transmissão de dados em redes. Conceitos Tech. Disponível em: https://conceitos.tech/redes-e-infraestrutura/tecnologias-de-rede/packet-switching/. Acesso em: 16 set. 2025.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008.
GRS ADVOCACIA. Proteção de dados em 2025: o panorama atual da LGPD no Brasil. GRS Advocacia, 2025. Disponível em: https://grsadv.com.br/protecao-de-dados-em-2025-o-panorama-atual-da-Igpd-no-brasil/. Acesso em: 16 set. 2025.

HISTÓRIA da World Wide Web. **Wikipédia, a enciclopédia livre.** Disponível em: https://pt.wikipedia.org/wiki/Hist%C3%B3ria_da_World_Wide_Web. Acesso em: 16 set. 2025.

INFORME. **O que se sabe até agora sobre o maior cibercrime financeiro já registrado no Brasil.** InfoMoney, 2025. Disponível em: https://www.infomoney.com.br/brasil/o-que-se-sabe-ate-agora-sobre-o-maior-cibercrime-financeiro-ja-registrado-no-brasil/. Acesso em: 16 set. 2025.

KASZNAR LEONARDOS. **Banco Central publica Resolução sobre incidentes de segurança da informação envolvendo dados pessoais no sistema do Pix**. 4 out. 2023. Disponível em: https://www.kasznarleonardos.com/banco-central-publica-resolucao-sobre-incidentes-de-seguranca-da-informacao-envolvendo-dados-pessoais-no-sistema-do-pix/. Acesso em: 16 set. 2025.

L.O. BAPTISTA ADVOGADOS. **ANPD não multou empresas por violação da LGPD em 2024**. Pessoa e Pessoa, 4 fev. 2025. Disponível em: https://pessoaepessoa.com.br/imprensa/anpd-nao-multou-empresas-por-violacao-da-igpd-em-2024/. Acesso em: 16 set. 2025.

LEINER, Barry M.; CERF, Vinton G.; CLARK, David D.; KAHN, Robert E.; KLEINROCK, Leonard; LYNCH, Daniel C.; POSTEL, Jon; ROBERTS, Larry G.; WOLFF, Stephen. **A brief history of the Internet**. Internet Society, 1997. Disponível em: https://www.internetsociety.org/internet/history-internet/brief-history-internet/. Acesso em: 16 set. 2025.

MORAES, Helio Ferreira. **O hacker do bem e as invasões de sistemas no Brasil**. Migalhas, 2025. Disponível em: https://www.migalhas.com.br/depeso/425037/o-hacker-do-bem-e-as-invasoes-de-sistemas-no-brasil. Acesso em: 16 set. 2025.

NAKAGAWA, Fernando. **Análise**: Vazamento de dados do Pix preocupa o Banco Central. CNN Brasil, 22 jul. 2025. Disponível em: https://www.cnnbrasil.com.br/blogs/fernando-nakagawa/economia/macroeconomia/analise-vazamento-de-dados-do-pix-preocupa-o-banco-central/. Acesso em: 16 set. 2025.

NASCIMENTO, Bruna Laís Campos do; SILVA, Edilene Maria da. **Lei Geral de Proteção de Dados (LGPD) e repositórios institucionais**: reflexões e adequações. Em Questão, Porto Alegre, v. 29, e-127314, 2023. Disponível em: https://doi.org/10.1590/1808-5245.29.127314. Acesso em: 16 set. 2025.

OLIVEIRA. **Crimes cibernéticos**: da ineficácia da Lei Carolina Dieckmann na prática de crimes virtuais. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 9, n. 11, p. 354-369, 2025. DOI: 10.51891/rease.v9i11.12291. Disponível em: https://periodicorease.pro.br/rease/article/view/12291. Acesso em: 16 set. 2025.

PAYSÃO, Felipe. **‘Eu que vazei os dados de clientes do Banco Neon’**: uma conversa com um hacker. TecMundo, 12 fev. 2025. Atualizado em 12 fev. 2025. Disponível em: https://www.tecmundo.com.br/seguranca/402487-eu-que-vazei-os-dados-de-clientes-do-banco-neon-uma-conversa-com-um-hacker.htm. Acesso em: 16 set. 2025.

PINHEIRO, Patrícia Peck; SLEIMAN, Cristina; ROCHA, Henrique; LOTUFO, Larissa; BISSOLI, Leandro. **Segurança digital**: proteção de dados nas empresas. 1. ed. São Paulo: Atlas, 2020.

SANTOS, Marco Aurelio Fernandes dos. **Crimes cibernéticos no sistema financeiro**: análise jurídica e desafios. Migalhas, 2025. Disponível em: https://www.migalhas.com.br/depeso/439640/crimes-ciberneticos-no-sistema-financeiro-analise-juridica-e-desafios. Acesso em: 16 set. 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Súmula n° 479**: As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias. Brasília, 26 jun. 2012. Disponível em: https://scon.stj.jus.br/SCON/sumstj/toc.jsp?livre=%27479%27.num.&O=JT. Acesso em: 16 set. 2025.

ZANIOLO, Pedro Augusto. **Crimes modernos**: o impacto da tecnologia no Direito. 4. ed., rev., ampl. e atual. Salvador: JusPODIVM, 2021.