LIGA DE ENSINO DO RIO GRANDE DO NORTE
CENTRO UNIVERSITÁRIO DO RIO GRANDE DO NORTE
CURSO DE GRADUAÇÃO EM DIREITO

THIAGO VINICIUS DE SOUZA PINHEIRO SOARES

DESAFIOS E PERSPECTIVAS DA PREVENÇÃO E INVESTIGAÇÃO DO ESTELIONATO ONLINE

NATAL/RN
2024

THIAGO VINICIUS DE SOUZA PINHEIRO SOARES

DESAFIOS E PERSPECTIVAS DA PREVENÇÃO E INVESTIGAÇÃO DO ESTELIONATO ONLINE

Trabalho de Conclusão de Curso apresentado ao Centro Universitário do Rio Grande do Norte (UNI-RN) como requisito final para obtenção do título de Graduação em direito.

Orientador: Prof. Dr. Sandresson de Menezes Lopes.

NATAL/RN

2024

Catalogação na Publicação – Biblioteca do UNI-RN
Setor de Processos Técnicos

Soares, Thiago Vinicius de Souza Pinheiro.
Desafios e perspectivas da prevenção e investigação do estelionato online / Thiago Vinicius de Souza Pinheiro Soares. – Natal, 2024.
47 f.

Orientador: Prof. Dr. Sandresson de Menezes Lopes.
Monografia (Graduação – Curso de Direito) – Centro Universitário do Rio Grande do Norte.

1. Estelionato digital – Monografia. 2. Crimes cibernéticos – Monografia. 3. Prevenção de fraudes – Monografia. 4. Segurança digital – Monografia. 5. Legislação – Monografia. I. Lopes, Sandresson de Menezes. II. Título.

RN/UNI-RN/BC CDU 34

Larissa Inês da Costa (CRB 15/657)

THIAGO VINICIUS DE SOUZA PINHEIRO SOARES

DESAFIOS E PERSPECTIVAS DA PREVENÇÃO E INVESTIGAÇÃO DO ESTELIONATO ONLINE

Trabalho de Conclusão de Curso apresentado ao Centro Universitário do Rio Grande do Norte (UNI-RN) como requisito final para obtenção do título de Graduação em direito.

Aprovado em: 17/12/2024

BANCA EXAMINADORA

_____

Prof. Dr. Sandresson de Menezes Lopes.

Orientador

_____

Prof. Me. João Victor Gomes Bezerra Alencar.

Membro

_____

Profa. Dra. Stefani Leite Cavalcanti.

Membro

RESUMO

O crime cibernético tem crescido rapidamente no Brasil, especialmente o estelionato digital, causando sérios prejuízos às vítimas e afetando negativamente a interação no meio digital. Este trabalho investiga os desafios e oportunidades para prevenir e combater essas fraudes, avaliando a eficácia das medidas legais e práticas atualmente adotadas. Com base em uma análise de legislações, como o Marco Civil da Internet e a Lei nº 14.155/2021, e em estudos de caso, a pesquisa mostra como o anonimato, a globalização da internet e falhas nas leis tornam difícil identificar e responsabilizar os criminosos. Diante disso, destaca-se a importância de ações conjuntas entre governo, setor privado e sociedade, priorizando políticas públicas mais eficazes, modernização das leis e campanhas que conscientizem e preparem a população para lidar com esse problema crescente.

Palavras-chave: Estelionato Digital, Crimes Cibernéticos, Prevenção De Fraudes, Segurança Digital, Legislação.

ABSTRACT

Cybercrime has grown rapidly in Brazil, especially digital fraud, causing serious harm to victims and affecting new experiences and interaction in the digital environment. This work investigates the challenges and opportunities to prevent and combat these frauds, evaluating the effectiveness of legal and practical measures currently adopted. Based on an analysis of legislation, such as the Marco Civil da Internet and Law nº 14,155/2021, and case studies, research shows how anonymity, the globalization of the internet and flaws in laws make it difficult to identify and hold criminals accountable. In view of this, the importance of joint actions between government, private sector and society stands out, prioritizing more effective public policies, modernization of laws and campaigns that raise awareness and prepare the population to deal with this growing problem.

Keywords: Digital Theft, Cybercrime, Fraud Prevention, Digital Security, Legislation.

SUMÁRIO

1 INTRODUÇÃO

O estelionato no Brasil, especialmente em sua forma digital, tem se tornado um fenômeno preocupante. Recentemente, as estatísticas mostram que estados como o Rio Grande do Norte têm registrado elevadas taxas de vítimas de crimes cibernéticos, como o clonamento de cartões, golpes online e insegurança em contas bancárias. Números como esses não refletem apenas os danos materiais, mas também impactos emocionais, uma vez que as pessoas buscam informações para o dia a dia em uma sociedade onde a interação no espaço digital é parte fundamental da vida.

Ao falar de estelionato, é importante entendermos como esses crimes funcionam e qual a importância de adotar medidas que possam preveni-los e combatê-los de maneira mais eficaz no futuro. Com o crescimento da tecnologia, os golpes também se tornaram mais sofisticados, expondo vulnerabilidades significativas que a legislação ainda não consegue abordar adequadamente, além da ignorância de parte da população sobre as falhas e riscos no ambiente digital.

Portanto, esse debate vai além de alertar as pessoas sobre os perigos; é necessário buscar soluções para proteger os indivíduos contra os golpes virtuais e promover maior segurança nas interações online. Um dos crimes mais prevalentes associados ao estelionato nos últimos anos é a fraude digital, onde criminosos utilizam informações falsas para obter patrimônio ou direitos financeiros de outra pessoa. Exemplos disso incluem o clonamento de cartões, fraudes em plataformas online, entre outros.

2 REFERENCIAL TEORICO

O estelionato, em sua forma tradicional e digital, é um crime tipificado no artigo 171 do Código Penal Brasileiro, caracterizado pela obtenção de vantagem ilícita mediante fraude. Esse delito, historicamente associado à exploração da boa-fé em transações econômicas, adquiriu novas nuances no ambiente digital, expondo vulnerabilidades das relações mediadas pela tecnologia (CUNHA, 2019).

O advento da internet e o crescimento das interações virtuais criaram um cenário propício para o surgimento do estelionato digital, modalidade que utiliza ferramentas online para enganar as vítimas e obter benefícios ilícitos. Golpes como phishing, clonagem de aplicativos e fraudes financeiras tornaram-se mais sofisticados, aproveitando-se da lacuna legislativa e da falta de conscientização da população (OLIVEIRA; BRITO; FERREIRA JÚNIOR, 2024).

A legislação brasileira, representada pelo Marco Civil da Internet (Lei nº 12.965/2014) e pela Lei nº 14.155/2021, busca regular o uso da tecnologia e endurecer as punições para crimes cibernéticos. Contudo, lacunas jurídicas, aliadas à globalização da internet e ao anonimato proporcionado pelo meio digital, dificultam a responsabilização dos agentes criminosos (CABRAL; BARRETO, 2024).

Além disso, a evolução tecnológica impõe desafios à investigação. Métodos tradicionais tornam-se insuficientes diante da complexidade das fraudes digitais, que frequentemente envolvem servidores localizados no exterior e o uso de redes privadas virtuais (VPNs). Isso exige um esforço coordenado entre governos, setor privado e organismos internacionais para implementar tecnologias de rastreamento e fortalecer políticas públicas de segurança digital (BARRETO & BRASIL, 2016).

Dessa forma, o referencial teórico desta pesquisa fundamenta-se na análise das legislações existentes, no estudo de casos práticos e na literatura especializada sobre segurança digital e crimes cibernéticos. O objetivo é compreender, de forma aprofundada e sensível, as peculiaridades do estelionato digital, enquanto se busca caminhos práticos e eficazes para fortalecer a prevenção e melhorar a investigação desses crimes no Brasil.

3 OBJETIVO

O presente trabalho tem como objetivo principal realizar uma análise aprofundada dos desafios e perspectivas relacionados à prevenção e à investigação do crime de estelionato online no Brasil. Busca-se compreender as características distintivas desse delito no ambiente virtual, destacando os fatores que facilitam sua prática, como o anonimato, a globalização das interações digitais e a insuficiência de regulamentações específicas.

Adicionalmente, objetiva-se investigar as dificuldades enfrentadas pelos órgãos de segurança pública, como a identificação e responsabilização dos autores, os limites tecnológicos e jurídicos, bem como a escassez de recursos especializados. Outro foco será avaliar a eficácia das legislações vigentes e a necessidade de aprimoramento normativo, considerando as transformações tecnológicas e sociais.

Por fim, o trabalho visa propor estratégias e soluções viáveis para otimizar os mecanismos de prevenção e repressão ao estelionato online, promovendo a proteção dos direitos das vítimas e o fortalecimento da segurança digital no Brasil.

4 RELEVÂNCIA

A relevância deste trabalho reside na crescente incidência do estelionato online, um fenômeno que tem desafiado os sistemas de segurança pública e as instituições jurídicas no Brasil e no mundo. A expansão das interações digitais, impulsionada pelo avanço tecnológico e pela popularização da internet, criou um ambiente propício para práticas ilícitas que impactam diretamente a economia, a confiança nos meios digitais e os direitos fundamentais dos cidadãos.

O estudo sobre os desafios e perspectivas da prevenção e investigação do estelionato online é indispensável, pois trata de um tema atual e relevante, que afeta não apenas indivíduos, mas também empresas e instituições públicas. Ao abordar as dificuldades enfrentadas pelos órgãos de investigação e a insuficiência de instrumentos legais e tecnológicos para o combate a esse tipo de crime, este trabalho contribui para um debate crítico sobre a necessidade de fortalecimento das políticas públicas de segurança digital.

Além disso, a pesquisa tem potencial para propor soluções práticas e viáveis, auxiliando na construção de um sistema mais eficiente e adequado à realidade tecnológica contemporânea. Assim, o estudo pretende fomentar discussões acadêmicas e subsidiar decisões no âmbito legislativo, policial e judicial, promovendo avanços significativos no combate ao estelionato online.

5 METODOLOGIA

A metodologia aplicada à pesquisa incluiu a análise de revistas científicas e documentos, compostos por artigos científicos, livros, relatórios do Ciberlab e da Polícia Federal, bem como de outras organizações especializadas.

Dentro dessa etapa, foi realizada uma análise das legislações reguladoras, como o Marco Civil da Internet e a Lei nº 14.155/2021. No entanto, ao invés de apenas compreender a aplicabilidade tradicional dessas normas,estudou-se detalhadamente as lacunas que permanecem no combate ao estelionato online.

Para aprofundar essa etapa, estudos de caso e exemplos práticos foram explorados, os quais revelaram as dificuldades reais encontradas no trabalho de investigar e prevenir o crime em questão.

Adicionalmente, a pesquisa foi estendida com a análise de relatórios internacionais, permitindo relacionar o cenário em debate com as práticas existentes em outras nações, para uma comparação e adaptação do cenário brasileiro.

A combinação entre legislação, análise de revistas e dados de fontes primárias possibilitou uma visão mais profunda e conectada à prática, de forma que as propostas elaboradas visam fortalecer políticas públicas no combate ao estelionato digital por meio de mecanismos públicos mais eficazes.

6 ASPECTOS CONCEITUAIS E FUNDAMENTOS DO CRIME DE ESTELIONATO

O estelionato foi criado como uma forma de proteger relações comerciais que emergiram entre sociedades mais complexas e interconectadas. Quando as trocas comerciais e financeiras se tornaram um pilar fundamental da organização social, os casos de fraude que exploravam a relação de confiança entre as partes também aumentaram. Portanto, a forma como o crime se manifestava evidencia a importância da proteção do princípio fundamental da boa-fé, que era utilizado como um instrumento comum de ganho ilícito.

Em nosso país, o estelionato foi tipificado pela primeira vez no Código Penal de 1940, época em que a sociedade reconheceu que certas práticas fraudulentas já constituíam crimes. Com sua abrangente conceituação, esse Código visava combater o golpe tradicional, que consistia na falsificação de documentos, manipulação de contratos e promessas falsas feitas às vítimas, geralmente caracterizadas pela ingenuidade ou falta de discernimento. A inclusão do estelionato no Código Penal demonstrava claramente a preocupação do Estado em recuperar um ambiente econômico mais seguro e confiável, proporcionando maior confiança na economia financeira de nossos cidadãos.

Com o passar dos anos, o estelionato foi se adaptando às mudanças sociais e tecnológicas. O que antes era realizado, em grande parte, de forma presencial devido ao limitado alcance da comunicação, foi impulsionado pelo crescimento da tecnologia, permitindo que o crime se expandisse além das fronteiras territoriais. O estelionato digital é um exemplo disso, mostrando que, apesar das novas ferramentas e métodos, a essência do crime, que é enganar para obter vantagem ilícita, se mantém atual, adaptando-se às novas dinâmicas da sociedade e das épocas.

A expressão jurídica "estelionato" advém de termos gregos, que originalmente designavam um tipo de lagarto capaz de mudar de cor para enganar e impedir que seus inimigos alimentassem sua presa. Assim, a raiz da palavra reflete a ação do agente que fere outra pessoa utilizando métodos fraudulentos (RIBEIRO, 2019).

O crime de estelionato, comum no mundo contemporâneo, foi intensificado pela pandemia de COVID-19, que agravou a prática dessa modalidade criminosa, especialmente no âmbito digital. Nesse contexto, a prática do estelionato passou a ser mais predominante no ambiente virtual, gerando um número crescente de vítimas e prejudicando muitas pessoas, que foram exploradas de forma cruel e ilícita.

O ambiente digital oferece maior comodidade para os criminosos, tornando a prática das fraudes mais facilitada em comparação às fraudes presenciais. De acordo com o Código Penal Brasileiro, o estelionato está tipificado no Capítulo IV, entre os crimes contra o patrimônio, da seguinte forma:

Art. 171 - Obter, para si ou para outra pessoa, benefício ilícito em prejuízo de terceiros, induzindo ou mantendo alguém em erro, por meio de artifício, ardil ou outro expediente fraudulento. Pena - reclusão de um a cinco anos e multa, de quinhentos mil réis a dez contos de réis (BRASIL, 1940).

Trata-se de um crime patrimonial, no qual a legislação busca resguardar a inviolabilidade do patrimônio, punindo atos destinados a enganar a vítima e beneficiar o agente (CUNHA, 2019). Essa infração ocorre por meio de engano ou fraude, onde o criminoso manipula a vítima com uma narrativa fictícia para obter vantagem ilícita, causando danos emocionais ou financeiros, muitas vezes irreparáveis.

É importante destacar que o estelionato não envolve violência física ou ameaças graves, sendo essa a principal distinção entre ele e o crime de extorsão (Art. 158 do CP). No caso do estelionato, a vítima, convencida, entrega voluntariamente algo ao criminoso após ser induzida ao erro. Já na extorsão, a perda do patrimônio ocorre contra a vontade da vítima, que é submetida a violência ou ameaças.

6.1 SUJEITO ATIVO E SUJEITO PASSIVO DO ESTELIONATO

O estelionato é um crime comum, não exigindo qualquer característica ou condição especial do autor. Assim, qualquer pessoa pode ser o sujeito ativo. Da mesma forma, o sujeito passivo também é comum, pois qualquer cidadão pode sofrer perdas patrimoniais devido a atividades fraudulentas (RAMOS JÚNIOR, 2020).

No entanto, para que o crime se configure, a vítima deve ter capacidade de discernimento, ou seja, ser capaz de ser enganada. Caso não possua essa capacidade, o crime será enquadrado no abuso de incapazes (Art. 173 do CP). Além disso, a vítima precisa ser identificável, pois, se for incerta, o crime poderá ser enquadrado em outros artigos legais, como o Art. 2º, XI, da Lei nº 1.521/1951, que trata, por exemplo, de adulteração de taxímetros, balanças ou bombas de combustível (CUNHA, 2019)

No direito brasileiro, há duas correntes de interpretação sobre o estelionato. A primeira acredita que, quando há fraude bilateral, ou seja, ambas as partes têm

intenção de obter vantagem ilícita, o crime não se configura. Essa visão sustenta que o patrimônio só deve ser protegido quando usado para fins legítimos. A segunda corrente, amplamente aceita, argumenta que o crime ocorre independentemente da boa-fé da vítima. Segundo essa posição, a intenção do golpista é o fator determinante, sendo irrelevante a motivação ou conduta da vítima (CAPEZ, 2020).

No entanto, é indispensável que a vítima participe ativamente, entregando a vantagem ao criminoso de maneira espontânea. Caso contrário, o crime pode ser classificado como roubo (Art. 157 do CP) ou extorsão (Art. 158 do CP) (SALES, 2023).

7 ASPECTOS DEFINIDORES E ELEMENTOS CARACTERÍSTICOS DO ESTELIONATO VIRTUAL

O estelionato, previsto no artigo 171 do Código Penal Brasileiro, é um crime que consiste na obtenção de vantagem ilícita, geralmente de natureza financeira, por meio de engano. A prática envolve o uso de artifícios, fraudes ou mentiras que induzem a vítima ao erro, resultando em prejuízo. A essência do estelionato está na manipulação da confiança alheia, explorando a credibilidade e boa-fé das pessoas para alcançar objetivos ilícitos (LUDGERO, 2023).

crime que consiste na obtenção de vantagem ilícita, geralmente de natureza financeira, por meio de engano. A prática envolve o uso de artifícios, fraudes ou mentiras que induzem a vítima ao erro, resultando em prejuízo. A essência do estelionato está na manipulação da confiança alheia, explorando a credibilidade e boa-fé das pessoas para alcançar objetivos ilícitos (LUDGERO, 2023).

A tipificação do estelionato como crime reflete a necessidade de proteger as relações de confiança, especialmente em sociedades onde as interações econômicas são frequentes e diversas. Esse tipo de fraude já era reconhecido historicamente, mas sua formalização no ordenamento jurídico brasileiro ocorreu com o Código Penal de 1940, buscando coibir práticas prejudiciais ao patrimônio e à integridade social. Desde então, o estelionato abrange uma ampla gama de condutas fraudulentas, desde golpes presenciais até fraudes em contratos e documentos (MENEZES, 2016).

Com o avanço da tecnologia, o estelionato passou a se manifestar de forma significativa no ambiente digital, resultando no chamado "estelionato digital". Essa modalidade utiliza a internet como ferramenta para aplicar golpes, explorando vulnerabilidades como falta de conhecimento técnico dos usuários ou a ausência de mecanismos de segurança robustos. Golpes como phishing, falsas promoções e fraudes financeiras online são exemplos de como a evolução tecnológica ampliou as oportunidades para esse tipo de crime (OLIVEIRA; BRITO; FERREIRA JÚNIOR, 2024).

Diante da crescente incidência do estelionato, especialmente no meio digital, torna-se essencial não apenas a conscientização da população sobre os riscos, mas também o fortalecimento de mecanismos de proteção. A legislação vem sendo aprimorada para acompanhar a complexidade dos golpes modernos, como o projeto de lei que tipifica o estelionato digital com penas específicas. A prevenção depende

de um esforço conjunto entre governos, empresas e cidadãos, visando educar a sociedade, aprimorar tecnologias de segurança e garantir a punição dos responsáveis (LUDGERO, 2023).

Com o avanço da transformação digital, o estelionato tradicional expandiu-se para o ambiente online, impulsionado pela popularização da internet e das plataformas de e-commerce e aplicativos financeiros. Essas ferramentas, apesar de trazerem conveniência, também criaram oportunidades para fraudes, permitindo que criminosos utilizem tecnologias sofisticadas para enganar vítimas de forma rápida e, muitas vezes, difícil rastrear (LUDGERO, 2023).

O estelionato digital é uma adaptação moderna do crime de estelionato, utilizando meios virtuais para enganar vítimas e obter vantagens ilícitas. Entre as práticas mais comuns estão os golpes de phishing, nos quais os criminosos induzem os usuários a fornecerem informações pessoais e financeiras confidenciais, a falsificação de identidades em redes sociais e fraudes em transações financeiras. Essas ações exploram tanto vulnerabilidades técnicas, como a falta de segurança em sistemas digitais, quanto humanas, como a confiança excessiva nas interações online (OLIVEIRA; BRITO; FERREIRA JÚNIOR, 2024).

Nos últimos anos, o crescimento do estelionato digital tem sido alarmante. A facilidade de acesso a dados pessoais e financeiros, somada à crescente dependência de transações online, tem contribuído para o aumento desse tipo de crime. Dados alarmantes apontam para um número crescente de vítimas, muitas vezes com prejuízos significativos, tanto financeiros quanto emocionais. A rapidez com que os golpistas se adaptam a novas tecnologias e criam esquemas fraudulentos é um dos maiores desafios no combate a esse tipo de atividade criminosa (MENEZES, 2016).

A dificuldade em identificar e punir os responsáveis é uma das principais barreiras enfrentadas pelas autoridades. No ambiente digital, os criminosos frequentemente utilizam técnicas de anonimato, como redes privadas virtuais (VPNs) e identidades falsas, tornando o rastreamento e a coleta de provas ainda mais complicados. Além disso, a ausência de uma legislação clara e específica para crimes digitais em muitos países contribui para a impunidade, incentivando a perpetuação das fraudes online (LUDGERO, 2023).

Diante desse cenário, é fundamental fortalecer os mecanismos de combate ao estelionato digital, tanto por meio de avanços na legislação quanto pelo

aprimoramento das tecnologias de segurança. Além disso, a conscientização dos usuários desempenha um papel crucial na prevenção de golpes. Medidas como desconfiar de ofertas muito vantajosas, verificar a autenticidade de sites e proteger informações pessoais são passos simples, mas eficazes, para reduzir os riscos. A união de esforços entre governos, empresas e cidadãos é essencial para criar um ambiente digital mais seguro e resiliente contra fraudes (OLIVEIRA; BRITO; FERREIRA JÚNIOR, 2024).

Diante da crescente complexidade e do aumento exponencial dos casos de estelionato digital, a legislação brasileira tem buscado se adaptar para enfrentar os desafios impostos por esse tipo de crime. Recentemente, a Comissão de Constituição e Justiça (CCJ) do Senado aprovou um projeto de lei que propõe a inclusão do estelionato digital como uma tipificação específica no Código Penal. Essa iniciativa reflete a necessidade de atualizar o ordenamento jurídico para contemplar as peculiaridades dos crimes cometidos no ambiente virtual (ARAÚJO, 2024).

O projeto estabelece penas que variam de quatro a oito anos de reclusão para aqueles que utilizam plataformas digitais para aplicar golpes. Essa pena é similar à prevista para crimes de fraude eletrônica, indicando a seriedade com que o tema vem sendo tratado. Ao criar um enquadramento específico para o estelionato digital, a proposta busca não apenas punir os responsáveis, mas também atuar como um mecanismo de dissuasão, visando reduzir a incidência dessas práticas criminosas (ARAÚJO, 2024).

Além disso, o texto do projeto de lei aborda situações como o uso de notoriedade em redes sociais para promover esquemas fraudulentos, demonstrando preocupação com novas formas de atuação criminosa no ambiente online. Essa abordagem amplia a responsabilidade para influenciadores e outros indivíduos que, de forma intencional, utilizam sua posição para lesar economicamente seus seguidores ou promover atividades ilegais (ARAÚJO, 2024).

A aprovação desse tipo de legislação é um marco importante na proteção dos usuários da internet, especialmente em um cenário de crescente digitalização das relações econômicas e sociais. No entanto, a eficácia dessa medida dependerá de uma aplicação rigorosa, bem como da capacitação das autoridades para investigar e combater o estelionato digital de maneira eficiente (ARAÚJO, 2024).

O avanço legislativo, portanto, é um passo significativo, mas precisa ser acompanhado de esforços complementares, como campanhas de conscientização

pública e investimento em tecnologia de rastreamento e segurança. A união entre legislação robusta, educação digital e fortalecimento de mecanismos de investigação é essencial para enfrentar os desafios apresentados pelo estelionato digital e proteger os direitos dos cidadãos no ambiente virtual (LUDGERO, 2023).

7.1 MÉTODOS COMUNS DE FRAUDE VIRTUAL

Os tipos de golpes cibernéticos incluem a clonagem de WhatsApp, em que o golpista duplica a conta da vítima e solicita dinheiro aos contatos; o boleto fraudulento, no qual o código de barras de um boleto legítimo é alterado para redirecionar o pagamento; as fraudes em instituições financeiras, como o falso funcionário, o falso motoboy e o phishing, que visam roubar dados ou realizar transações indevidas; o golpe de sites falsos de e-commerce, onde o consumidor é enganado por lojas virtuais fictícias; o golpe do falso leilão, envolvendo sites fraudulentos que simulam leilões online; o ransomware, que sequestra dados e exige resgate financeiro para desbloqueá-los; o golpe do amor, em que criminosos exploram relações virtuais para obter dinheiro; a sextorsão, que utiliza ameaças de divulgar conteúdo íntimo para extorquir vítimas; e os golpes envolvendo PIX, que exploram descuidos no uso do sistema de pagamento instantâneo (POLÍCIA CIVIL DE SÃO PAULO, s.d).

Na Clonagem de WhatsApp, o esquema ocorre da seguinte maneira: o golpista entra em contato por ligação ou mensagem, fingindo ser funcionário de um site de compras ou instituição bancária, alegando que enviará um código promocional ou de confirmação. Ele solicita que a vítima informe esse código, que, na realidade, é a verificação do WhatsApp. Com esse dado, o estelionatário consegue duplicar a conta da vítima. Após a clonagem, ele passa a enviar mensagens aos contatos da pessoa lesada, fingindo ser ela, solicitando dinheiro. As justificativas para pedir o valor emprestado variam, sendo os principais alvos os familiares e amigos próximos, que, confiando na mensagem, realizam depósitos ou transferências para a conta fornecida pelo golpista (POLÍCIA CIVIL DE SÃO PAULO, s.d).

Já o Boleto Fraudulento, o golpe acontece assim: o boleto bancário é um instrumento de quitação em que o emissor, denominado "Beneficiário", recebe o valor correspondente a um produto ou serviço em sua conta. O criminoso, utilizando técnicas de engenharia social ou links maliciosos, modifica o código de barras do

boleto, direcionando o pagamento para a conta de um integrante da quadrilha (POLÍCIA CIVIL DE SÃO PAULO, s.d).

As fraudes bancárias mais comuns incluem: Falso funcionário ou falsa central de atendimento: o golpista se passa por um colaborador do banco e informa problemas no cadastro ou irregularidades na conta. A vítima, ao fornecer

seus dados, possibilita que o criminoso realize transações indevidas (POLÍCIA CIVIL DE SÃO PAULO, s.d). Falso motoboy: membros da quadrilha ligam para a vítima, alegando ser da central de atendimento da instituição financeira. Eles informam problemas com o cartão e pedem que a senha seja digitada no telefone. Em seguida, enviam um motoboy para recolher o cartão, que, junto com a senha, é utilizado para realizar operações fraudulentas (POLÍCIA CIVIL DE SÃO PAULO, s.d). Phishing: o golpista envia mensagens com links por e-mail ou SMS, explorando emoções como curiosidade, urgência ou medo, induzindo a vítima a clicar em links que roubam dados ou a fornecer informações confidenciais (POLÍCIA CIVIL DE SÃO PAULO,s.d).

Sobre os Sites de Comércio Eletrônico Falsos, essa prática criminosa tem como alvo consumidores de e-commerce. O estelionatário cria uma página virtual que imita o site original, enganando a vítima a acreditar que está realizando uma compra legítima. Após selecionar os produtos e concluir o pagamento, a vítima não recebe a mercadoria, percebendo então que foi enganada. Para aumentar o sucesso, o golpista utiliza estratégias como envio de e-mails em massa, oferta de produtos com preços muito abaixo do mercado e anúncios patrocinados. Empresas e indivíduos que têm seus dados usados de forma indevida para criar os sites ou “empresas fictícias” também são prejudicados (POLÍCIA CIVIL DE SÃO PAULOs,d).

No Golpe do Falso Leilão ou Empréstimo Fraudulento, é realizado por meio da criação de sites fraudulentos, com imagens de veículos para simular um leilão online. A vítima, ao fazer um lance, é informada que ganhou o leilão e recebe um documento com orientações para pagamento e retirada do veículo. Após a transferência do valor, o contato com a “empresa” é interrompido. Em muitos casos, os golpistas utilizam informações reais de leiloeiros, sem que estes tenham conhecimento, e oferecem veículos a preços extremamente baixos para atrair vítimas (POLÍCIA CIVIL DE SÃO PAULO).

Ransomware (Sequestro de Dados): Nesse golpe, um software malicioso, conhecido como ransomware, bloqueia o acesso aos dados da vítima até que um resgate seja pago. Normalmente, a invasão ocorre à noite ou de madrugada, quando

o criminoso instala o vírus que criptografa as informações do dispositivo. Ao tentar acessar seus dados, a vítima recebe uma mensagem informando que
eles só serão liberados mediante o pagamento, geralmente exigido em bitcoins (POLÍCIA CIVIL DE SÃO PAULO, s.d).

Depois da série “o golpista do TInder” lançado pela Netflix, ficou muito conhecido o Golpe do Amor / Golpe Sentimental. Nessa fraude, pessoas que buscam relacionamentos em plataformas digitais são alvos de golpistas que criam perfis falsos. Após conquistar a confiança da vítima com declarações e promessas de amor, o criminoso inventa histórias para obter vantagens financeiras, como pedir dinheiro para comprar passagens ou pagar taxas de envio de supostos presentes (POLÍCIA CIVIL DE SÃO PAULO, s.d).

Pela primeira vez em 2013, surgiu o termo "fraude sentimental", mencionado no acórdão proferido pela 5ª Turma Cível do Tribunal de Justiça do Distrito Federal. Nesse caso, confirmou-se a sentença do 1º grau que condenou o ex-namorado da autora a ressarcir as dívidas contraídas durante o período em que mantinham um relacionamento amoroso. Ficou comprovado que o ex-namorado (réu) se aproveitou da relação afetiva para enganar a autora, visando obter vantagens ilícitas. O que gerou a seguinte jurisprudência:

> PROCESSO CIVIL. TÉRMINO DE RELACIONAMENTO AMOROSO. DANOS MATERIAIS COMPROVADOS. RESSARCIMENTO. VEDAÇÃO AO ENRIQUECIMENTO SEM CAUSA. ABUSO DO DIREITO. BOA FÉ OBJETIVA. PROBIDADE. SENTENÇA MANTIDA.
>
> 1. Deve ser mantida a sentença a quo eis que, da documentação carreada para os autos, consubstanciados em sua maior parte por mensagens trocadas entre as partes, depreendendo-se que a autora/apelada efetuou continuadas transferências ao réu; fez pagamentos de dívidas em instituições financeiras em nome do apelado/réu; adquiriu bens móveis tais como roupas, calcados e aparelho de telefonia celular; efetuou o pagamento de contas telefônicas e assumiu o pagamento de diversas despesas por ele realizadas, assim agindo embalada na esperança de manter o relacionamento amoroso que existia entre os ora demandantes. Corrobora-se, ainda e no mesmo sentido, as promessas realizadas pelo varão-réu no sentido de que, assim que voltasse a ter estabilidade financeira, ressarciria os valores que obteve de sua vítima, no curso da relação [...].

> [5ª TURMA CÍVEL Classe : APELAÇÃO N. Processo : 20130110467950APC (0012574-32.2013.8.07.0001) Apelante(s) : SERGIO ANTONIO PINHEIRO DE OLIVEIRA Apelado(s) : SUZANA OLIVEIRA DEL BOSCO TARDIM Relator Desembargador CARLOS RODRIGUES Revisor : Desembargador ANGELO PASSARELI Acórdão N. : 866800]

Conforme constatado no referido julgado, a 5ª Turma Cível do Tribunal de Justiça do Distrito Federal caracterizou como "fraude sentimental" o ato de tirar proveito da confiança estabelecida dentro de um relacionamento amoroso para obter ganhos patrimoniais que, de outra forma, não seriam alcançados. Essas vantagens são obtidas por meio da quebra da boa-fé da vítima, que acreditava plenamente na veracidade do relacionamento em que estava envolvida.

Em casos mais recentes, a jurisprudência apresenta uma definição do "estelionato sentimental" como situações em que uma das partes do relacionamento abusa da confiança e do afeto do parceiro amoroso com o intuito de conseguir vantagens patrimoniais.

> APELAÇÃO CRIMINAL. ESTELIONATO SENTIMENTAL OU AFETIVO. MATERIALIDADE E AUTORIA COMPROVADAS. CONJUNTO PROBATÓRIO SUFICIENTE. PALAVRA DA VÍTIMA. CONDENAÇÃO MANTIDA. DOSIMETRIA. PENA-BASE. FRAÇÃO NORTEADORA. MANUTENÇÃO. AGRAVANTE. FRAÇÃO DE 1/6 (UM SEXTO). APLICAÇÃO. DANO MORAL E DANO MATERIAL. MANUTENÇÃO. PRISÃO PREVENTIVA. ADEQUAÇÃO. I - Incabível
> a absolvição quando os elementos probatórios indicam com a certeza necessária a prática do crime de estelionato em contexto de violência doméstica e familiar contra a mulher, notadamente quando a vítima apresenta relatos firmes e coerentes, corroborados pelos depoimentos dos informantes e das testemunhas, sob o crivo do contraditório e da ampla defesa, os quais revelam que durante relacionamento afetivo mantido com a vítima, o réu obteve vantagem econômica ilícita, ao induzi-la em erro, por meio de artifício e ardil.[...].
>
> (Acórdão 1435207, 07070233720218070005, Relator: NILSONI DE FREITAS CUSTODIO, 3ª Turma Criminal, data de julgamento: 30/6/2022, publicado no PJe: 12/7/2022. Pág.: Sem Página Cadastrada.)

No primeiro caso, que trata de um processo civil, a 5ª Turma Cível do Tribunal de Justiça do Distrito Federal manteve a sentença que condenou o réu a ressarcir a autora por danos materiais decorrentes de um relacionamento amoroso. O réu se aproveitou da confiança criada dentro do relacionamento para que a autora realizasse várias transferências financeiras e assumisse dívidas em seu nome, acreditando que o relacionamento continuaria. A decisão considerou a boa-fé objetiva, probidade e a promessa de restituição feita pelo réu, o que justificou o ressarcimento para evitar o enriquecimento sem causa.

No segundo caso, referente a uma apelação criminal, o réu foi condenado por estelionato sentimental em contexto de violência doméstica e familiar contra a mulher. A vítima apresentou relatos firmes e coerentes, reforçados por depoimentos de testemunhas, sobre como o réu obteve vantagens econômicas ilícitas ao induzi-la em erro durante o relacionamento afetivo. A condenação

incluiu tanto a reparação por dano material quanto por dano moral, e o tribunal considerou a especial valorização da palavra da vítima em situações de violência doméstica. Além disso, foram estabelecidas diretrizes para arbitrar o valor da indenização por danos morais, levando em conta diversas circunstâncias envolvidas.

Ambas as jurisprudências convergem na ideia de que o estelionato sentimental ocorre quando uma das partes se aproveita do relacionamento amoroso para obter vantagens patrimoniais indevidas. As decisões ressaltam a importância de considerar a boa-fé, a confiança e a promessa de restituição feita pelo réu como elementos fundamentais na análise do caso. Além disso, a palavra da vítima ganha destaque em ambos os casos, enfatizando sua relevância probatória, especialmente em situações de violência doméstica.

Tem-se, também a sextorsão, é a ameaça de divulgar imagens ou vídeos íntimos com o objetivo de forçar a vítima a fazer algo, seja para obter dinheiro, vingança ou causar humilhação. As imagens podem ser obtidas por meio de invasão de dispositivos, falsas promessas de emprego ou manipulação emocional. Após conseguir o material, o criminoso exige mais fotos, encontros presenciais ou pagamentos para não divulgar o conteúdo (POLÍCIA CIVIL DE SÃO PAULO).

Há também os golpes que envolvem o PIX, sendo os cuidados para evitar fraudes nesse serviço semelhantes aos aplicados a outros, como TED e DOC. Recomenda-se não acessar sites ou baixar aplicativos desconhecidos, realizar cadastros e transações apenas em sites ou aplicativos oficiais das instituições

financeiras, confirmar o cadastro de chaves em duas etapas e evitar compartilhar códigos de confirmação enviados por SMS ou e-mail. Em caso de dúvidas, é importante consultar diretamente a instituição financeira por meio de seus canais oficiais (POLÍCIA CIVIL DE SÃO PAULO, s.d).

7.2 BARREIRAS JURÍDICAS E OPERACIONAIS

A investigação e punição de crimes de estelionato virtual representam desafios no cenário da segurança pública moderna. O estelionato virtual, uma forma de fraude perpetrada por meio digital, é caracterizado pelo uso da internet para enganar e obter vantagens indevidas das vítimas. A globalidade da rede, o anonimato e a capacidade de disseminação rápida de informações tornam esses

crimes particularmente difíceis de investigar e punir. Barreto e Brasil (2016) destacam que a sofisticação das técnicas empregadas pelos criminosos e a constante adaptação dessas práticas dificultam a identificação e responsabilização dos autores.

Um dos principais entraves jurídicos na responsabilização de estelionatários virtuais é a localização de servidores fora do Brasil. O Marco Civil da Internet (Lei nº 12.965/2014) impõe aos provedores de serviços com atuação no Brasil o dever de respeitar a legislação local, mas muitas empresas de tecnologia sediadas no exterior invocam leis de seus países de origem para não cumprir ordens judiciais brasileiras (Barreto, 2015). Esse conflito de legislações prejudica a coleta de evidências e a continuidade das investigações.

A exigência de utilizar tratados de cooperação jurídica, como o MLAT (Mutual Legal Assistance Treaty), agrava a situação. Esses tratados são frequentemente burocráticos e demoram meses para serem concluídos, um tempo que pode ser crucial em investigações que exigem rapidez (Barreto & Wendt, 2015). Como consequência, os investigadores se deparam com dificuldades para acessar dados em tempo hábil, o que compromete a eficácia das ações policiais e pode resultar na impunidade dos infratores.

A legislação brasileira, representada pelo Marco Civil da Internet, busca garantir a aplicação de suas normas a empresas que oferecem serviços no país, mesmo que seus servidores estejam no exterior (Brasil, 2014). No entanto, a aplicação dessa legislação enfrenta desafios práticos, principalmente quando os provedores se

recusam a fornecer dados sob a alegação de que seus dados estão sujeitos a leis de outros países (Barreto, 2015).

A morosidade na resposta às solicitações de dados é outro problema crítico. Investigações criminais, por natureza, exigem celeridade e precisão, e o tempo é um fator determinante para o sucesso ou fracasso da apuração dos fatos. Como apontam Cabral e Barreto (2024), a falta de agilidade na obtenção de informações telemáticas pode fazer com que evidências se tornem obsoletas e ineficazes.

A criação de delegacias especializadas em crimes cibernéticos é uma medida que vem sendo discutida para superar esses desafios. Barreto (2018) ressalta a necessidade de setores capacitados e bem equipados para lidar com a complexidade das investigações cibernéticas. A capacitação de agentes e a utilização de técnicas de investigação digital são fundamentais para melhorar a coleta de evidências e a identificação de autores (Barreto & Brasil, 2016).

A cooperação internacional é uma peça-chave para a investigação eficaz de crimes cibernéticos, dada a natureza transnacional desses delitos. Contudo, a falta de uniformidade nas legislações de diferentes países sobre privacidade e proteção de dados impede a fluidez da troca de informações (Barreto & Wendt, 2015). Sem um mecanismo global harmonizado, as investigações ficam limitadas e as ações judiciais podem ser ineficazes.

A investigação de estelionato virtual muitas vezes requer o uso de técnicas modernas, como a análise de tráfego de rede e ferramentas de inteligência de dados. Segundo Caselli et al. (2015), essas metodologias têm se mostrado eficazes em coletar informações e rastrear criminosos. No entanto, sua implementação depende de recursos e treinamento adequado, que ainda são limitados em muitas regiões do Brasil.

Outro fator complicador é a utilização de tecnologias que permitem o anonimato, como redes privadas virtuais (VPNs) e serviços de VOIP. Esses recursos dificultam a identificação do autor do crime, uma vez que a localização real e outros detalhes podem ser mascarados (Caselli et al., 2015). A rápida evolução tecnológica requer que os investigadores estejam sempre atualizados e prontos para adotar novas abordagens.

A jurisprudência brasileira já reconheceu que a aplicação do MLAT não deve ser a única via para obtenção de dados. O Tribunal Regional Federal da 2ª Região decidiu que as empresas que oferecem serviços no Brasil devem cumprir a legislação

nacional, independentemente de onde seus servidores estão localizados. Essa decisão reafirma a soberania do país sobre o cumprimento das leis dentro de seu território.

A resistência de empresas em cumprir ordens judiciais é uma barreira que deve ser enfrentada com firmeza. Como observado por Barreto (2015), a negativa de fornecer informações sob o pretexto de leis estrangeiras ameaça transformar o Brasil em um "paraíso cibernético", onde os criminosos se aproveitam da ineficácia na aplicação da lei. É essencial que as autoridades busquem meios de garantir que a legislação nacional seja respeitada.

A falta de integração entre as forças policiais e a ausência de um canal unificado para comunicação entre agências agravam as dificuldades na

investigação de estelionatos virtuais. Cabral e Barreto (2024) apontam que, sem uma colaboração adequada, ocorre duplicidade de investigações e desperdício de recursos. A criação de protocolos padronizados e bancos de dados compartilhados pode ajudar a otimizar os esforços e evitar redundâncias.

Outro ponto importante é a necessidade de proteger a privacidade dos cidadãos enquanto se combate o crime cibernético. A legislação deve encontrar um equilíbrio entre garantir a segurança pública e respeitar os direitos individuais. O Marco Civil da Internet tenta traçar essa linha, mas sua aplicação prática muitas vezes gera conflitos (Barreto, 2015).

A atuação do Ministério da Justiça e Segurança Pública, por meio de iniciativas como o Ciberlab, tem sido uma resposta relevante aos desafios dos crimes cibernéticos. Esses esforços visam promover a capacitação e a integração de dados entre diferentes órgãos de segurança pública, aumentando a eficiência nas investigações (Cabral & Barreto, 2024).

A educação e conscientização da população sobre segurança digital também desempenham um papel crucial na prevenção de estelionatos virtuais. Barreto e Brasil (2016) enfatizam que muitos crimes poderiam ser evitados com práticas de segurança básicas, como o uso de senhas fortes e a autenticação de dois fatores. No entanto, a falta de conhecimento ainda é um ponto fraco significativo.

O avanço tecnológico requer que as leis sejam atualizadas constantemente para acompanhar novas ameaças e metodologias de crime. Segundo Cabral e Barreto (2024), a inovação e a adaptação das forças policiais às novas realidades digitais são imperativas para que as investigações sejam bem-sucedidas.

Barreto e Brasil (2016) apresentam uma abordagem prática e técnica para conduzir investigações cibernéticas, enfatizando a importância da conformidade com a legislação vigente para garantir a validade e a eficácia dos procedimentos investigativos.

Uma das contribuições mais significativas de Barrerto e Brasil (2016) é a explicação dos métodos de coleta e preservação de evidências digitais, procedimentos fundamentais para a integridade das provas em processos judiciais. Os autores também discutem desafios técnicos e legais enfrentados por investigadores, como o anonimato proporcionado por redes privadas e a encriptação de dados, que dificultam a identificação de criminosos cibernéticos. Barreto e Brasil (2016) ainda abordam questões práticas relacionadas ao rastreamento de atividades suspeitas, técnicas de investigação forense digital e estratégias de colaboração entre autoridades e provedores de serviços. A obra serve como um guia essencial para compreender os aspectos legais e processuais de investigar crimes na era digital, destacando a importância da coordenação entre diferentes agentes e do uso de tecnologia avançada para combater atividades ilícitas na internet.

Além de fornecer conhecimentos técnicos, Barreto e Brasil sublinham a relevância de uma abordagem ética e legal no combate aos crimes cibernéticos, promovendo a proteção dos direitos individuais e a preservação da privacidade, ao mesmo tempo em que se busca a responsabilização dos infratores. Este livro é, portanto, um recurso valioso para profissionais que atuam na interseção entre direito, tecnologia e segurança pública.

Para enfrentar os desafios da investigação de estelionatos virtuais, é necessário investir em tecnologia, treinamento e colaboração internacional. A resistência ao cumprimento de ordens judiciais por empresas de tecnologia não pode ser um empecilho permanente. É preciso que medidas sejam adotadas para assegurar que o país tenha os recursos necessários para combater crimes digitais com eficiência (Barreto, 2015).

8 A EVOLUÇÃO LEGISLATIVA E OS DESAFIOS DO DIREITO DIGITAL

A trajetória da legislação de informática no Brasil começou nos anos 1980, quando as tecnologias de informação e comunicação começaram a ter um impacto mais perceptível na vida das pessoas e na economia. Nesse contexto, foi necessário criar um conjunto de leis que acompanhasse o avanço tecnológico e garantisse a proteção de direitos em um cenário cada vez mais digitalizado.

O ponto de partida dessa regulamentação foi a Lei de Informática (Lei nº 7.232/1984), criada para organizar o setor de tecnologia no país e estimular o crescimento da indústria nacional de informática. Essa lei buscava proteger o mercado interno, oferecendo incentivos fiscais e impondo barreiras à entrada de tecnologias estrangeiras, numa tentativa de reduzir a dependência tecnológica do Brasil e incentivar a inovação local.

No entanto, com a abertura econômica nos anos 1990 e o fim da política de reserva de mercado, a Lei de Informática precisou ser atualizada para refletir a nova realidade de globalização e inovação tecnológica. Nesse período, a popularização dos computadores e o surgimento da internet trouxeram à tona desafios inéditos, exigindo ajustes no arcabouço legal.

Décadas depois, um marco significativo nesse campo foi a criação do Marco Civil da Internet (Lei nº 12.965/2014). Considerado uma “Constituição da Internet” no Brasil, esse documento estabeleceu direitos e deveres tanto para usuários quanto para provedores de serviços, abordando temas como neutralidade da rede, privacidade e liberdade de expressão online. Essa lei foi uma resposta às novas demandas de uma sociedade hiperconectada, tentando equilibrar liberdade digital, proteção de dados pessoais e responsabilidade na disseminação de informações.

Outro passo importante foi dado com a Lei Geral de Proteção de Dados Pessoais (LGPD, Lei nº 13.709/2018), que trouxe regras rigorosas para o tratamento de dados no Brasil. Inspirada na legislação europeia GDPR, a LGPD obrigou empresas e organizações a serem mais transparentes e cuidadosas no uso das informações pessoais, o que demandou grandes adaptações tanto do setor público quanto do privado.

Apesar desses avanços, o Brasil ainda enfrenta desafios significativos na regulamentação de novas questões no direito digital, como inteligência artificial,

criptomoedas e a segurança contra crimes cibernéticos. Tecnologias como blockchain e IA têm provocado debates sobre como equilibrar inovação e ética no uso dessas ferramentas.

Hoje, um dos principais desafios no campo do direito digital é encontrar formas de proteger direitos fundamentais, como a privacidade e a não discriminação, em meio à complexidade das novas tecnologias. Além disso, o combate a crimes virtuais exige esforços conjuntos entre governo, setor privado e sociedade civil, envolvendo políticas públicas eficazes e colaboração.

8.1 O MARCO CIVIL DA INTERNET

O Marco Civil da Internet, instituído pela Lei 12.965/2014, é uma das legislações mais importantes no cenário brasileiro para regulamentação do uso da internet. Criada para garantir direitos e estabelecer responsabilidades no ambiente digital, a lei é frequentemente considerada a “Constituição da Internet” no Brasil (CARVALHO, 2017).

A premissa do Art. 19 é evitar o que se chama de “censura privada” por parte das plataformas digitais. Ao exigir que a remoção de conteúdo se dê apenas após decisão judicial, o artigo protege o direito à liberdade de expressão, evitando que conteúdos sejam retirados sem justificativa judicial. Este dispositivo jurídico se fundamenta na necessidade de assegurar a liberdade de expressão dos usuários, princípio basilar de qualquer sociedade democrática (SOUZA, 2018). No entanto, ele levanta a questão: a proteção desse direito à expressão deve sobrepor-se a outros direitos fundamentais, como a privacidade e a dignidade humana?

O Art. 19 reflete uma escolha legislativa explícita em dar primazia à liberdade de expressão. Em um ambiente digital onde a informação flui em larga escala e com grande rapidez, o legislador buscou proteger o debate público de uma censura excessiva, que poderia ser imposta por pressões sociais ou políticas. Assim, o artigo visa a evitar que as plataformas digitais adotem uma postura de remoção de conteúdo por simples notificações extrajudiciais, o que poderia criar uma situação de autocensura prejudicial à livre circulação de ideias (MACIEL, 2023).

Por outro lado, a exigência de uma ordem judicial para que os provedores removam conteúdo gerado por terceiros impõe um ônus significativo sobre as vítimas de conteúdos abusivos. Indivíduos que tenham sua honra, privacidade ou dignidade

lesada são obrigados a acionar o Judiciário para obter a remoção de conteúdos ofensivos. Esse processo pode ser demorado, deixando a vítima desprotegida por um longo período e, em muitos casos, perpetuando o dano (CARVALHO, 2017).

Essa teoria, entretanto, divide-se em duas abordagens, dependendo do ponto de partida para responsabilizar o provedor de aplicação pelo conteúdo gerado por terceiros. Esse ponto inicial pode ser: (i) a notificação feita pelo

próprio usuário, utilizando os canais disponibilizados pelo provedor; ou (ii) uma notificação judicial, acionada após a intervenção do Poder Judiciário pela parte que se sente lesada.

A jurisprudência do Superior Tribunal de Justiça, em um primeiro momento, adotava a primeira abordagem, considerando que o simples conhecimento inequívoco do conteúdo ofensivo, sem a devida remoção em um prazo razoável, tornaria o provedor responsável. Esse entendimento é exemplificado em decisões anteriores, como o julgado mencionado (REsp 1.406.448/RJ, Terceira Turma, DJe 21/10/2013).

No entanto, devido a diversas considerações, o Marco Civil da Internet opta expressamente pela segunda abordagem, estabelecendo que o provedor de aplicação só será responsabilizado caso descumpra uma ordem judicial, conforme determinado no artigo 19, caput, dessa legislação.

A Constituição Federal de 1988 assegura a dignidade da pessoa humana como um dos fundamentos do Estado Democrático de Direito. Esse princípio é violado quando conteúdos que afetam a honra ou privacidade permanecem online durante o longo tempo que a judicialização do processo pode levar. Assim, enquanto o Art. 19 busca garantir a liberdade de expressão, ele também é criticado por não proporcionar proteção eficaz e célere a outros direitos fundamentais de grande relevância constitucional (SOUZA, 2018).

Outro ponto relevante na análise da constitucionalidade do Art. 19 é o princípio da proporcionalidade, que orienta a ponderação entre direitos fundamentais conflitantes. Ao atribuir peso excessivo à liberdade de expressão, o artigo compromete a proteção de outros direitos, como privacidade e dignidade, o que representa um desequilíbrio no tratamento desses direitos fundamentais (CARVALHO, 2017).

Em termos práticos, o princípio da proporcionalidade sugere que a lei deve buscar soluções que considerem igualmente todos os direitos envolvidos, ajustando suas exigências conforme a relevância e os impactos.

Muitos estudiosos do direito argumentam que o Art. 19 representa um retrocesso na proteção de direitos fundamentais. Isso se deve à criação de uma situação em que a liberdade de expressão é elevada acima de outros direitos, desconsiderando a necessidade de proteger a dignidade humana e a privacidade dos usuários (SOUZA, 2018). Em uma sociedade plural, a legislação

deve garantir que esses direitos não sejam ameaçados por práticas ou interpretações que permitam abusos e violações.

Ao manter conteúdos prejudiciais acessíveis até a ordem judicial ser proferida, o Art. 19 pode agravar o dano à vítima, principalmente em situações de difamação, ofensa à honra, ou exposição não consentida. O atraso imposto pelo processo judicial reduz a eficácia da proteção e gera uma sensação de impunidade, que contradiz o objetivo de proteção constitucional à dignidade humana e à segurança jurídica (SOUZA, 2018).

Outro aspecto importante a ser considerado é o papel das plataformas digitais na curadoria de conteúdo. Diferente de distribuidores de informação tradicionais, essas plataformas controlam o fluxo de informações, impactando diretamente o que é visto e compartilhado por milhões de usuários. Com isso, elas deixam de ser apenas intermediárias e passam a atuar como curadoras de conteúdo, o que implica uma responsabilidade maior pela repercussão e impacto dos conteúdos que hospedam (MACIEL, 2023).

Há argumentos de que o Art. 19 beneficia desproporcionalmente as grandes plataformas, as chamadas Big Techs, ao garantir a elas uma posição segura contra a responsabilização direta, o que reduz incentivos para uma postura de maior controle sobre o conteúdo nocivo (CARVALHO, 2017). Essas empresas, que geram lucros a partir do engajamento de seus usuários, não estariam obrigadas a reprimir conteúdos que promovam desinformação, ódio ou violência, a menos que haja uma ordem judicial específica.

Nesse contexto, o princípio do “pro homine” — que orienta a aplicação da norma que melhor protege o ser humano — é muitas vezes invocado para contestar a constitucionalidade do Art. 19. Os críticos sustentam que, ao privilegiar os interesses das plataformas em detrimento da proteção de direitos individuais, a lei falha em aplicar o princípio do “pro homine”, que deveria guiar a interpretação e aplicação das normas para proteção máxima dos direitos humanos (SOUZA, 2018).

É importante destacar que o Art. 19 não se aplica a todos os tipos de conteúdo. No caso de conteúdos relacionados a cenas de nudez ou violência sexual, por exemplo, a remoção pode ser feita sem ordem judicial, o que demonstra uma preocupação específica do legislador com essas situações extremas (CARVALHO, 2017). No entanto, essa exceção não atende a todos os cenários onde a dignidade e privacidade do usuário estão em risco, deixando uma lacuna de proteção que pode ser interpretada como falha constitucional.

8.2 MARCO CIVIL E A LGPD

Outro argumento a favor da constitucionalidade do Art. 19 é que ele se baseia no princípio da “inafastabilidade da jurisdição”. Essa abordagem busca evitar que conflitos de direitos sejam resolvidos fora do sistema judiciário, promovendo segurança jurídica e impedindo que plataformas adotem políticas arbitrárias de remoção de conteúdo (MACIEL, 2023). No entanto, a aplicação rígida desse princípio pode ignorar a necessidade de resposta rápida em casos onde há clara violação de direitos fundamentais.

Para compreender plenamente o Marco Civil da Internet e a LGPD, é essencial considerar o contexto em que essas leis foram criadas. O Marco Civil da Internet, instituído pela Lei 12.965 de 2014, foi a primeira legislação específica voltada para regulamentar o uso da internet no Brasil. Seu principal objetivo é estabelecer princípios, garantias e deveres tanto para os usuários quanto para os provedores de serviços na rede, delineando as diretrizes de atuação do Estado nesse ambiente digital. Com essa estrutura, o Marco Civil abordou aspectos essenciais como a neutralidade da rede, a privacidade dos usuários e a liberdade de expressão online, criando uma base fundamental para a regulamentação da internet (Cardoso; Régis, 2024).

Em 2018, com a promulgação da LGPD, o cenário de proteção de dados no Brasil ganhou novos contornos. A LGPD, Lei 13.709, trouxe um enfoque mais específico e abrangente sobre o tratamento de dados pessoais, aplicando-se tanto ao setor público quanto ao privado. A legislação visa proteger os direitos fundamentais de liberdade e privacidade dos indivíduos, estabelecendo princípios e regras claras para o tratamento de dados pessoais.

A LGPD exige que as organizações adotem práticas transparentes e seguras no manejo de dados, limitando a coleta apenas ao necessário e garantindo que esses dados sejam usados para finalidades legítimas e específicas. Além disso, a LGPD introduziu sanções rigorosas para o descumprimento dessas normas, um ponto que o Marco Civil da Internet não aborda com tanta profundidade (Rocha, 2022).

As duas leis se complementam em diversos aspectos, mas também possuem diferenças significativas. Enquanto o Marco Civil da Internet estabelece diretrizes gerais para o uso da internet e menciona a proteção de dados como um de seus princípios fundamentais, a LGPD apresenta uma regulamentação detalhada sobre a coleta, armazenamento e tratamento de dados pessoais. A LGPD adiciona um nível de proteção e responsabilidade para as organizações, reforçando os direitos dos indivíduos sobre suas informações pessoais e, com isso, respondendo aos novos desafios trazidos pela era digital. A interação entre o Marco Civil e a LGPD reflete o avanço da regulamentação digital no Brasil, que busca garantir um ambiente online seguro e transparente para os usuários (Rocha, 2022).

Para Cardoso e Régis (2024), essas legislações, embora distintas em sua abordagem, se interconectam ao buscar um equilíbrio entre a liberdade e segurança no ambiente digital. O Marco Civil da Internet, ao priorizar a liberdade de expressão e o acesso à informação, estabelece um terreno fundamental para a comunicação e compartilhamento de informações na rede. No entanto, sua abordagem à proteção de dados é limitada, deixando espaço para a necessidade de uma norma mais detalhada. A LGPD surge exatamente para preencher essa lacuna, focando na privacidade e nos direitos dos titulares de dados.

Dessa forma, a LGPD amplia o escopo de proteção ao exigir que todas as atividades de tratamento de dados, sejam elas realizadas online ou offline, sigam princípios de transparência, segurança e responsabilidade, proporcionando uma regulamentação mais robusta e específica.

Portanto, a relação entre as duas leis também revela a evolução do sistema jurídico brasileiro em adaptar-se aos avanços tecnológicos e às novas demandas sociais. Ao complementar o Marco Civil com a LGPD, o Brasil fortalece a proteção dos usuários e estabelece um padrão de segurança que acompanha as práticas internacionais de proteção de dados.

Essa dupla camada de regulamentação reflete uma abordagem moderna e preventiva, onde a internet é não só um espaço de liberdade, mas também um

ambiente protegido contra abusos e usos indevidos de dados pessoais. Assim, o Marco Civil e a LGPD, juntos, visam criar um equilíbrio essencial para que o ambiente digital seja seguro, respeitoso e em conformidade com os direitos fundamentais de cada cidadão.

O principal ponto de interseção entre o Marco Civil e a LGPD é a proteção da privacidade. Enquanto o Marco Civil estabelece o direito à privacidade como um dos princípios para o uso da internet, a LGPD amplia essa proteção, determinando que os dados pessoais só podem ser tratados mediante consentimento do titular ou outra base legal adequada. Segundo Maciel (2023), o Marco Civil pode ser considerado a base normativa inicial para a proteção de dados pessoais no Brasil, mas a LGPD traz especificações e garantias mais robustas.

Além disso, ambos estabelecem obrigações para os provedores de internet e demais agentes envolvidos no tratamento de dados. No Marco Civil, o artigo 19 trata da responsabilidade dos provedores, prevendo que só serão civilmente responsáveis caso não retirem conteúdo ilegal após ordem judicial. Essa medida visa proteger a liberdade de expressão, evitando remoções arbitrárias (Carvalho, 2017). Na LGPD, a responsabilidade é expandida para abranger o dever de tratamento adequado dos dados, com a implementação de medidas de segurança para proteger as informações dos usuários.

Contudo, há um debate sobre a eficácia do artigo 19 do Marco Civil no que tange à proteção de direitos fundamentais. Parte da doutrina critica esse artigo por priorizar a liberdade de expressão em detrimento da proteção da dignidade e privacidade, o que pode resultar em vulnerabilidade para os usuários que buscam a remoção de conteúdos ofensivos (Godoy, 2018). A LGPD busca equilibrar essa lacuna ao exigir que os dados sejam tratados de forma transparente e responsável, possibilitando um maior controle por parte dos titulares de dados.

Outro ponto importante é o princípio da proporcionalidade, abordado tanto no Marco Civil quanto na LGPD. No Marco Civil, o princípio da liberdade de expressão é equilibrado com a proteção de outros direitos, porém, segundo Souza (2018), a LGPD intensifica a proteção, aplicando o princípio da necessidade para assegurar que apenas os dados essenciais sejam tratados, evitando excessos e riscos de exposição.

Para desenvolver uma análise aprofundada entre a LGPD e o Marco Civil da Internet, é essencial observar como cada legislação aborda temas cruciais como privacidade, liberdade de expressão e responsabilidade civil dos provedores. Essas

leis, embora complementares, possuem diferentes enfoques e objetivos regulatórios no ambiente digital.

A LGPD, promulgada em 2018, surge como uma resposta à necessidade crescente de regulamentação sobre o tratamento de dados pessoais no Brasil. Esse marco legal prioriza a proteção dos dados dos cidadãos, estipulando normas claras para a coleta, uso e armazenamento de informações pessoais, com o objetivo de salvaguardar a privacidade dos indivíduos e estabelecer parâmetros de segurança na era digital (Carvalho, 2017). O Marco Civil da Internet, por outro lado, aprovado em 2014, é muitas vezes descrito como uma "Constituição da Internet," por se concentrar na garantia de princípios gerais como a liberdade de expressão e a neutralidade de rede, além de regulamentar a responsabilidade dos provedores de internet.

Em relação à privacidade, ambos os dispositivos legais possuem objetivos que convergem. A LGPD impõe obrigações rigorosas a organizações públicas e privadas para proteger a privacidade dos usuários, estabelecendo que o consentimento do titular é essencial para a coleta e tratamento de seus dados, salvo em exceções legais. O Marco Civil, embora trate da privacidade de forma indireta, apresenta princípios como o direito à proteção de dados pessoais no ambiente digital, mas sua aplicação é mais focada na regulamentação dos provedores em termos de transparência e neutralidade da rede, visando a manutenção de um espaço livre para o fluxo de informações (Oliveira, 2023).

No campo da liberdade de expressão, o Marco Civil desempenha um papel mais direto. Conforme apontado por Maciel (2023), o artigo 19 do Marco Civil prioriza a liberdade de expressão ao estabelecer que os provedores de aplicações de internet só podem ser responsabilizados pela manutenção de conteúdos prejudiciais após uma ordem judicial. Isso é uma tentativa de evitar a censura privada e garantir que a internet continue sendo um espaço de livre expressão. Em contraste, a LGPD não lida diretamente com a liberdade de expressão, mas protege a exposição de dados pessoais de forma abusiva, o que, em última instância, apoia a privacidade e a dignidade pessoal.

Um aspecto controverso da relação entre essas leis está na questão da responsabilidade dos provedores de internet. O Marco Civil estipula que os provedores são responsabilizados apenas após descumprirem uma ordem judicial para remover conteúdo, o que implica uma proteção adicional para a liberdade de

expressão, mas que pode limitar a proteção imediata para usuários que se sentem lesados (Carvalho, 2017).

A LGPD, por sua vez, responsabiliza diretamente os agentes de tratamento que violam os direitos dos titulares, impondo uma responsabilização mais direta e incisiva. Em uma decisão do Tribunal de Justiça de Mato Grosso do Sul no Agravo de Instrumento nº 1406382-48.2022.8.12.0000, interposto por Twitter Brasil Rede de Informação Ltda., confirmou a obrigatoriedade de ocultação de conteúdos potencialmente ofensivos postados por usuários específicos contra o professor Alessandro Martins Prado, conforme determinado pela decisão inicial.

O professor relatou que os ataques, feitos por uma aluna e sua mãe, envolviam expressões difamatórias que comprometiam sua honra e dignidade. Ele solicitou a remoção dos conteúdos no Twitter e em outras redes sociais e o pagamento de indenização por danos morais.

> AÇÃO DE OBRIGAÇÃO DE NÃO FAZER C/C INDENIZAÇÃO POR DANOS MORAIS – OCULTAÇÃO DE PUBLICAÇÕES NO TWITTER COM CONTEÚDO POTENCIALMENTE OFENSIVO POSTADAS POR USUÁRIOS – PREENCHIMENTO DOS REQUISITOS PARA A CONCESSÃO DA TUTELA ANTECIPADA (ART. 300, DO CÓDIGO DE PROCESSO CIVIL/2015)– MANUTENÇÃO DA DECISÃO RECORRIDA – AGRAVO DE INSTRUMENTO CONHECIDO E
> IMPROVIDO. 1. Discute-se no presente recurso o preenchimento dos requisitos para concessão da tutela antecipada no sentido de determinar que a ré Twitter Brasil Rede de Informação Ltda oculte conteúdos potencialmente ofensivos publicados por usuáiros identificados. 2. A Lei nº 12.965, de 23/04/2014, conhecida como "Marco Civil da Internet", estabelece em seu artigo 19 que "com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário", sendo que "o juiz, inclusive no procedimento previsto no § 3º , poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação" (§ 4º, do art. 19, da Lei nº 12.965, de 23/04/2014). 3. Na espécie, verificando-se que a parte autora indicou claramente na inicial os conteúdos que pretende ver excluídos do "twitter", os quais foram devidamente indicados no decisum recorrido, tendo, ainda, sido fornecido os endereços (URLs) nos quais estão postados os textos tidos por ofensivos, não há razão para a parte agravante se eximir da obrigação de excluir as postagens feitas por seus usuários da rede social por ela gerenciada. 4. Agravo de Instrumento conhecido e improvido (TJMS, 2022).

A decisão do Tribunal de Justiça de Mato Grosso do Sul, no caso do Twitter Brasil, tem a ver com duas leis importantes: o Marco Civil da Internet e a LGPD, que regulam o que as plataformas podem fazer e protegem os direitos das pessoas na internet. O Marco Civil diz que redes sociais, como o Twitter, só podem ser responsabilizadas por posts ofensivos de terceiros se, depois de uma ordem judicial, elas não fizerem nada para tirar esses conteúdos do ar.

No caso, o tribunal mandou o Twitter ocultar postagens ofensivas contra um professor, lembrando que é dever da plataforma seguir a decisão da justiça para evitar problemas legais. Em resumo, o Marco Civil tenta equilibrar a liberdade de expressão das pessoas com o dever de proteger quem sofre ataques online.

Já a LGPD cuida da privacidade e proteção dos dados das pessoas, o que é importante quando alguém usa informações pessoais para prejudicar outra pessoa. Se esses dados são usados de maneira abusiva, como nas postagens que atacaram o professor, isso pode ir contra a LGPD, que dá direito à privacidade e ao respeito. Assim, as duas leis trabalham juntas: o Marco Civil define quando uma plataforma deve agir e a LGPD protege as pessoas de terem suas informações usadas de forma ofensiva ou prejudicial.

Outra diferença significativa é a abordagem de cada lei em relação ao princípio da proporcionalidade. A LGPD aplica este princípio ao exigir que o tratamento de dados seja limitado ao mínimo necessário para atingir seus fins, reforçando a proteção do titular (Carvalho, 2017). Já o Marco Civil usa a proporcionalidade como critério para evitar uma responsabilização excessiva dos provedores de internet, de modo que apenas uma decisão judicial pode determinar a remoção de conteúdo considerado ilícito, o que evita a atuação arbitrária dos provedores.

A seguir, há um e mandado de segurança questiona a legalidade de um ato judicial que deferiu a quebra de sigilo de dados telemáticos, delimitada por parâmetros de localização e tempo, com o objetivo de localizar agentes criminosos responsáveis pelo furto de oitenta armas de um estabelecimento comercial. A medida, fundamentada nos artigos 7º, inciso II, e 22 da Lei Federal nº 12.965/2014 (Marco Civil da Internet), atende a todos os requisitos legais, tendo sido justificada pelo grave risco à segurança pública.

MANDADO DE SEGURANÇA – APONTADO ATO COATOR CONSISTENTE NO DEFERIMENTO DE MEDIDA CAUTELAR DE QUEBRA DE SIGILO DE DADOS TELEMÁTICOS ESTÁTICOS DELIMITADA POR PARÂMETROS

> DE PESQUISA EM DETERMINADA REGIÃO E POR PERÍODO DE TEMPO – TENTATIVA DE LOCALIZAÇÃO DE AGENTES CRIMINOSOS QUE SUBTRAÍRAM OITENTA ARMAS DE UM ESTABELECIMENTO COMERCIAL – MEDIDA QUE ENCONTRA AMPARO NOS ARTIGOS 7º, INCISO II E 22 DA LEI FEDERAL N. 12.965/2014 (MARCO CIVIL DA INTERNET)– CUMPRIMENTO DE TODOS OS REQUISITOS LEGAIS E JUSTIFICADA NO GRAVE RISCO À SEGURANÇA PÚBLICA – FUNDADOS INDÍCIOS DA PRÁTICA DELITIVA – JUSTIFICADA A UTILIDADE DA MEDIDA, EIS QUE OUTROS MEIOS PROBATÓRIOS RESTARAM INEFICAZES, SENDO POSSÍVEL, A PARTIR DOS REGISTROS TELEMÁTICOS, A OBTENÇÃO DE DADOS SOBRE OS INDIVÍDUOS QUE CIRCULAREM NO LOCAL NO MOMENTO DA PRÁTICA DELITIVA – EXATA IDENTIFICAÇÃO DO PERIODO DESEJADO - DISPENSABILIDADE DE INDICAÇÃO DE QUALQUER ELEMENTO DE INDIVIDUALIZAÇÃO PESSOAL DOS ALVOS DA BUSCA - APURAÇÃO DE CRIME GRAVE E PATENTE RISCO À SEGURANÇA PÚBLICA COM A FALTA DE LOCALIZAÇÃO DAS ARMAS SUBTRAÍDAS, QUE PODEM SERVIR PARA A PRÁTICA DE OUTROS ILÍCITOS - VIOLAÇÃO À PRIVACIDADE E INTIMIDADE – DIREITOS QUE NÃO SÃO ABSOLUTOS E PODEM SER RESTRINGIDOS MEDIANTE DECISÃO JUDICIAL FUNDAMENTADA, SOBRETUDO QUANDO OBSERVADO RELEVANTE INTERESSE PÚBLICO, COMO NA HIPÓTESE EM APREÇO – DEVIDO RESPEITO AOS PRINCÍPIOS DA LEGALIDADE E DA PROPORCIONALIDADE - DECISÃO ADEQUADAMENTE FUNDAMENTADA NOS PRESSUPOSTOS PREVISTOS NO ARTIGO 22 DA LEI Nº 12.965/14 – INVIABILIDADE DE APLICAÇÃO DA LEI N. 9.296/96, QUE TRATA DAS INTERCEPTAÇÕES DAS COMUNICAÇÕES TELEFÔNICAS E DETÉM TRATAMENTO ESPECIALIZADO E MAIS RIGOROSO - PRECEDENTES DO SUPERIOR TRIBUNAL DE JUSTIÇA E DESTE TRIBUNAL – APONTADO ‘FISHING EXPEDITION’ (PESCARIA EXPLORATÓRIA) NÃO IDENTIFICADA NA HIPÓTESE EM ANÁLISE – INEXISTÊNCIA DE VIOLAÇÃO A APONTADO DIREITO LÍQUIDO E CERTO OU DE ABUSO DE PODER DA AUTORIDADE APONTADA COMO COATORA – VIABILIDADE DA MEDIDA CAUTELAR – SEGURANÇA CONHECIDA E DENEGADA (TJPR, 2023).

A decisão judicial que exige da Google uma varredura em dados de localização de todos os usuários em uma área geográfica específica levanta questões centrais sobre o princípio da proporcionalidade, com implicações tanto sob o Marco Civil da Internet quanto sob a LGPD. A LGPD enfatiza que o tratamento de dados deve ser limitado ao mínimo necessário para atingir seus fins, protegendo o titular contra excessos no uso de suas informações pessoais (Carvalho, 2017).

Neste caso, a ordem judicial de coletar dados de localização de muitos indivíduos não envolvidos no crime parece desrespeitar esse princípio, uma vez que amplia desnecessariamente o impacto da coleta de

dados, expondo dados sensíveis de pessoas inocentes sem justificativa direta e específica.

O Marco Civil da Internet, por outro lado, aplica a proporcionalidade para evitar uma responsabilização excessiva e arbitrária dos provedores de internet, exigindo que apenas uma decisão judicial específica determine a remoção de conteúdo ou acesso

a dados que envolvam a privacidade dos usuários. Isso assegura que a atuação dos provedores seja limitada e resguarde a privacidade do usuário (Rocha, 2022).

Dado o caráter coletivo e genérico da ordem, a decisão judicial parece ignorar essa limitação ao exigir uma "pescaria exploratória", que compromete a proteção da privacidade garantida pelo Marco Civil. Cardoso e Régis (2024) destacam que, em conflitos entre as normas, a LGPD deve prevalecer por ser mais recente e detalhada na proteção da privacidade, cobrindo aspectos que o Marco Civil não regula.

Assim, uma aplicação equilibrada e integrada dessas legislações ajudaria a respeitar a privacidade dos usuários, sem abrir precedentes de invasão desnecessária, mantendo os objetivos de ambas as leis.

A conciliação entre as exigências do Marco Civil da Internet e da LGPD é uma questão fundamental para garantir um ambiente digital que respeite tanto a liberdade de expressão quanto a privacidade dos usuários. Conforme aponta Rocha (2022), a solução eficaz para esse conflito envolve uma interpretação harmônica e sistemática das duas normas.

Isso significa aplicar as leis de maneira que se respeitem as particularidades de cada situação, ponderando os interesses em questão e buscando um equilíbrio entre eles. Com essa abordagem, a proteção da privacidade e dos direitos fundamentais é priorizada, cumprindo os objetivos de ambas as legislações.

Segundo Cardoso e Régis (2024) que também falam sobre a relação entre essas normas, em situações de conflito entre elas, a LGPD, sendo mais recente e abrangente, pode prevalecer, uma vez que cobre aspectos de privacidade com maior especificidade e exigência de responsabilidade direta por parte dos agentes de tratamento de dados.

A LGPD aborda questões que o Marco Civil não regulamenta detalhadamente, como a coleta de dados de menores, o compartilhamento de dados entre empresas, e o tratamento de dados sensíveis. Esse aspecto torna a LGPD um complemento necessário, que, por ser mais protetivo, deve orientar as decisões judiciais onde se busca maior segurança e transparência no uso de dados pessoais.

Um exemplo disso é a apelação, onde o Tribunal de Justiça de São Paulo (TJ-SP) analisou um caso em que um consumidor teve seu número de telefone compartilhado em um banco de dados sem ser informado previamente, e decidiu modificar a sentença que havia julgado a ação improcedente. O autor recorreu, alegando seu direito de não ter seus dados divulgados sem consentimento e pedindo

indenização por danos morais. O tribunal reconheceu que, independentemente de os dados divulgados serem considerados sensíveis ou não, o consumidor tem o direito de ser informado sobre o armazenamento e o compartilhamento de seus dados, podendo se opor a essa divulgação ou corrigir informações incorretas.

> APELAÇÃO – Compartilhamento de informações pessoais (número de telefone) em banco de dados – Ação julgada improcedente – Apelo do autor, insistindo no direito de não ter seus dados pessoais divulgados em banco de dados e na indenização por danos morais – Admissibilidade – Independentemente da natureza dos dados divulgados, se sensíveis ou não, o consumidor deve ser informado da abertura do cadastro, podendo se opor à respectiva divulgação, bem como retificar os dados incorretos, sob pena de violação aos artigos 5º, X, da CF, 43, § 2º, do CDC e art. 4º, § 4º, I, da Lei nº 12.414/2011 – Precedentes do STJ e desta Corte – Distinção do tema em julgamento (ausência de informação ao consumidor do armazenamento de dados) com o precedente vinculante do STJ (Tema 710 - Resp 1.419.697), que trata do sistema de cadastro positivo (credit score), prática comercial considerada lícita – Violação do dever de informação – Ocorrência de dano moral "in re ipsa" – Indenização fixada em R$10.000,00, quantia que se mostra adequada e suficiente a reparar o dano, sem representar enriquecimento sem causa da vítima – Sentença modificada – RECURSO PROVIDO (TJSP, 2023).

Nesse caso, a ausência de comunicação ao consumidor sobre o armazenamento dos dados configurou violação ao dever de informação, prevista na Constituição Federal (artigo 5º, X), no Código de Defesa do Consumidor (artigo 43, § 2º), e na Lei nº 12.414/2011, que regula cadastros de consumidores. A decisão se diferenciou do precedente do Superior Tribunal de Justiça (Tema 710), que trata da prática legal do cadastro positivo para fins de crédito, pois neste caso o foco estava na falta de informação ao consumidor. Considerando o dano moral "in re ipsa" (presumido pela violação dos direitos do autor), o tribunal fixou uma indenização de R$10.000,00, considerada adequada para reparar o dano sem enriquecimento indevido. Assim, o recurso foi provido e a sentença foi modificada.

Ainda segundo Cardoso e Régis (2024), a jurisprudência tem sido decisiva para moldar a aplicação conjunta dessas leis, especialmente nos casos que envolvem disputas de privacidade e segurança de dados. Decisões recentes dos tribunais brasileiros demonstram a tendência de aplicar a LGPD em casos que necessitam de proteção específica, como o tratamento de dados de menores ou a responsabilidade solidária das empresas de telecomunicações em incidentes de vazamento de dados. Assim, os tribunais e órgãos reguladores são encorajados a interpretar as duas normas de forma integrada, respeitando a complexidade do ambiente digital e

adaptando a aplicação das leis às exigências contemporâneas da segurança de dados e liberdade online.

Portanto, quando ocorrem divergências ou incompatibilidades entre o Marco Civil da Internet e a LGPD, torna-se essencial buscar uma solução que harmonize as duas legislações. Segundo Rocha (2022), tal solução pode ser obtida por meio de critérios bem estabelecidos na doutrina jurídica, como o critério cronológico, onde a norma mais recente prevalece sobre a anterior; o critério hierárquico, em que normas de diferentes hierarquias conferem prevalência à norma superior; e o critério da especialidade, que prioriza a aplicação da lei específica sobre a lei geral. Dentre esses critérios, a especialidade é particularmente relevante, visto que a LGPD é uma lei focada especificamente na proteção de dados pessoais, enquanto o Marco Civil da Internet regula de forma mais ampla o uso da internet no Brasil.

Segundo Cardoso e Régias (2024), com a promulgação da LGPD, certos dispositivos do Marco Civil foram considerados tacitamente revogados, pois não se alinham aos princípios mais rigorosos da nova legislação sobre proteção de dados. Por exemplo, a LGPD estipula a necessidade de consentimento explícito para a coleta, uso e armazenamento de dados pessoais, algo que o Marco Civil não exigia com o mesmo rigor. Além disso, a LGPD impõe regras específicas para o tratamento de dados pessoais sensíveis e prevê sanções mais elevadas em caso de descumprimento, um aspecto que pode sobrepor as disposições menos restritivas do Marco Civil. Essa evolução normativa permite maior proteção aos dados pessoais e exige que os provedores e empresas digitais adotem práticas mais transparentes e seguras.

Essas mudanças trazem importantes reflexões para o cenário jurídico e regulatório, destacando a necessidade de uma interpretação sistemática que permita a coexistência dos princípios de ambas as leis. A aplicação da LGPD nos casos de proteção de dados e privacidade representa um avanço na defesa dos direitos dos titulares, especialmente quando há risco de vazamento ou tratamento inadequado de informações pessoais. A atuação do Judiciário e da ANPD é fundamental para que a aplicação das sanções e das diretrizes de proteção de dados sigam uma linha consistente, assegurando que os direitos de privacidade dos indivíduos sejam respeitados e que o ambiente digital se torne mais seguro e transparente para todos os usuários.

A adoção de ambos os marcos legais reflete o esforço do Brasil para se alinhar aos padrões internacionais, especialmente aos modelos estabelecidos pela União Europeia com o GDPR, no caso da LGPD. Desse modo, a legislação brasileira busca garantir um ambiente digital seguro, em que direitos como privacidade e liberdade de expressão possam coexistir de maneira harmônica, protegendo tanto a integridade dos dados pessoais quanto o livre fluxo de informações (Bioni, 2019).

Portanto, a partir do que foi exposto, a coexistência do Marco Civil da Internet e da LGPD representa um avanço significativo para a proteção dos direitos dos usuários no ambiente digital brasileiro, ainda que com enfoques distintos e complementares. O Marco Civil prioriza a liberdade de expressão e a neutralidade de rede, garantindo a transparência e a responsabilidade dos provedores em situações de conteúdo gerado por terceiros. A LGPD, por sua vez, estabelece uma regulamentação rigorosa para o tratamento de dados pessoais, assegurando a privacidade e o controle dos usuários sobre suas informações.

8.3 ATUALIZAÇÃO NORMATIVA NO COMBATE AOS CRIMES VIRTUAIS

Os crimes cibernéticos são uma realidade cada vez mais presente em um mundo dominado pela digitalização e pelo uso intensivo da internet. Com o avanço tecnológico, surgiram novas modalidades de infrações que vão além das práticas criminosas convencionais, exigindo um aparato legal robusto e específico para lidar com essa nova realidade. Segundo Barreto (2016), a investigação de crimes cibernéticos requer uma abordagem técnica e especializada, uma vez que muitos dos crimes digitais são realizados por meio de métodos que dificultam a identificação dos criminosos, como o uso de criptografia e redes de anonimato.

A Constituição Federal de 1988 já estabelecia a proteção aos direitos fundamentais, incluindo a privacidade e a inviolabilidade de dados pessoais (Brasil,1988). No entanto, o crescente número de ataques cibernéticos levou à necessidade de legislações complementares que abordassem especificamente as infrações digitais. A Lei nº 12.965/2014 foi um marco importante, pois estabeleceu princípios, garantias, direitos e deveres para o uso da internet no Brasil, promovendo um ambiente mais seguro e regulamentado (Brasil, 2014).

A tipificação de crimes digitais também foi reforçada pela Lei nº 12.735/2012, que alterou o Código Penal para incluir condutas criminosas realizadas por meio

eletrônico (Brasil, 2012). Essa legislação busca abranger crimes que variam de ataques de phishing a invasões de sistemas bancários. Segundo a análise de Barreto e Brasil (2016), a investigação desses crimes exige não apenas uma compreensão técnica dos sistemas informáticos, mas também uma articulação entre diferentes autoridades e o uso de recursos tecnológicos avançados.

Os desafios para investigar crimes cibernéticos são amplos e incluem a falta de delegacias especializadas e a necessidade de formação técnica de investigadores. A análise da Lei Azeredo por Barreto (2018) ressalta a importância de criar setores especializados e bem treinados para lidar com as particularidades dos crimes informáticos. As delegacias de crimes cibernéticos são essenciais para a coleta e preservação de provas digitais, um aspecto fundamental para que o processo judicial seja eficaz e justo. Outro ponto importante é a abrangência dos crimes cibernéticos, que muitas vezes são interestaduais ou internacionais. A Lei nº 10.446/2002 e sua atualização pela Lei nº 13.642/2018 ampliaram as atribuições da Polícia Federal para incluir a investigação de crimes praticados por meio da internet, especialmente aqueles que difundem conteúdo misógino (Brasil, 2002; 2018).

Isso reflete a preocupação com a disseminação de ódio e a necessidade de repressão uniforme em crimes que ultrapassam fronteiras regionais.

A atuação dos criminosos cibernéticos é facilitada pela falta de conhecimento da população sobre medidas básicas de segurança digital. Barreto (2016) aponta que muitos crimes, como a clonagem de cartões e invasão de contas, poderiam ser evitados com práticas simples, como o uso de senhas fortes e autenticação de dois fatores. No entanto, a educação digital ainda é um desafio no Brasil, com muitas pessoas desconhecendo os procedimentos corretos para se proteger online.

As legislações brasileiras, apesar de relevantes, ainda enfrentam desafios de aplicação e atualização.

O Projeto de Lei nº 4.614/2016 e o Projeto de Lei nº 5.202/2016 propõem medidas para incluir crimes cibernéticos no rol de infrações de repercussão interestadual, fortalecendo a capacidade de investigação e punição (Câmara dos Deputados, 2016). Essas iniciativas destacam a necessidade de políticas públicas mais eficazes e de uma colaboração entre setores públicos e privados para combater crimes que evoluem junto com a tecnologia.

Prevenir e combater crimes cibernéticos requer uma abordagem multidisciplinar que englobe não apenas a legislação, mas também a conscientização

e o envolvimento da sociedade. Prensky (2001) argumenta que as gerações mais jovens, chamadas de “nativos digitais”, têm mais facilidade em lidar com a tecnologia, mas isso não significa que estejam imunes a golpes e ataques. Portanto, a educação em segurança digital é tão crucial quanto as medidas legais.

A importância de uma estratégia nacional de segurança cibernética não pode ser subestimada. Segundo a Constituição e o Código Penal, a proteção dos cidadãos contra qualquer forma de crime é um dever do Estado (Brasil, 1940). A celeridade com que as tecnologias evoluem exige que as leis sejam frequentemente revisadas e que novas soluções sejam implementadas para mitigar riscos.

O papel das autoridades, como a Polícia Federal, é vital para a implementação das leis. A Lei nº 13.642/2018, que ampliou as atribuições dessa instituição, é um exemplo de como o Brasil tem buscado adaptar-se ao contexto digital (Brasil, 2018). No entanto, sem a formação técnica adequada e o aumento de recursos destinados a essa área, a eficácia das ações policiais continua limitada.

A sociedade também precisa estar ciente de seus direitos e deveres ao navegar na internet. A Lei nº 12.965/2014 garante a neutralidade da rede e a proteção de dados, mas é dever dos usuários tomar medidas proativas para proteger sua privacidade e segurança (Brasil, 2014). A combinação de legislação eficaz, práticas de segurança digital e consciência coletiva é a chave para enfrentar a crescente ameaça dos crimes cibernéticos.

Os desafios para o futuro incluem a adaptação contínua da legislação para enfrentar novas ameaças, como ataques de ransomware e crimes associados a tecnologias emergentes, como a inteligência artificial. Barreto e Brasil (2016) destacam que, embora os avanços legais sejam significativos, é necessária uma abordagem mais ampla e coordenada que inclua pesquisa, inovação e investimento em infraestrutura de segurança digital.

9 RESULTADOS E DISCUSSÕES

A presente pesquisa analisou os desafios e perspectivas relacionados à prevenção e investigação do estelionato digital no Brasil, com foco na eficácia das medidas legais e operacionais aplicadas. Os resultados encontrados refletem a crescente complexidade desse tipo de crime e as barreiras enfrentadas pelas instituições responsáveis pelo combate às fraudes digitais. Os dados analisados apontam que a globalização da internet, o anonimato proporcionado pelas redes digitais e as lacunas legislativas são fatores que dificultam a responsabilização dos criminosos. Apesar dos avanços proporcionados pelo Marco Civil da Internet (Lei nº 12.965/2014) e pela Lei nº 14.155/2021, ainda há entraves na aplicação prática dessas normas, especialmente em relação à cooperação internacional e ao acesso a dados armazenados fora do território nacional.

A pesquisa revelou que a rápida adaptação dos criminosos às novas tecnologias, como o uso de redes privadas virtuais (VPNs) e técnicas de engenharia social, aumenta a dificuldade de investigação. Casos frequentes de golpes como phishing, clonagem de aplicativos e fraudes em e-commerce mostram que as ferramentas digitais, apesar de facilitarem as interações sociais e comerciais, também potencializam as vulnerabilidades do sistema. Ademais, a ausência de delegacias especializadas e a morosidade no cumprimento de ordens judiciais por empresas de tecnologia sediadas no exterior comprometem a eficiência das investigações. Estudos de caso apresentados evidenciam que muitas vezes as vítimas ficam desamparadas, enquanto os criminosos permanecem impunes.

Outro ponto relevante discutido é a insuficiência de campanhas de conscientização sobre segurança digital no Brasil. A pesquisa destacou que uma parcela significativa da população desconhece medidas básicas de proteção, como autenticação em dois fatores e verificação de autenticidade de sites e links. Por fim, verificou-se a importância de uma abordagem integrada entre governo, setor privado e sociedade. Para avançar no enfrentamento ao estelionato digital, é imprescindível modernizar a legislação, adequando as normas à complexidade dos crimes digitais, com foco em penalidades específicas e atualizações frequentes. Também é necessário fortalecer políticas públicas, ampliando a estrutura de combate ao cibercrime, com a criação de delegacias especializadas e treinamento contínuo de agentes. Além disso, é fundamental promover educação digital, implementando

campanhas nacionais de conscientização sobre segurança cibernética, com orientações práticas para evitar fraudes.

Os resultados corroboram a necessidade de esforços conjuntos e contínuos para enfrentar o crescimento exponencial das fraudes digitais e garantir maior proteção ao patrimônio e à privacidade dos cidadãos no ambiente virtual.

10 CONCLUSÃO

Esta pesquisa buscou compreender os desafios e propor melhorias para a investigação e prevenção do estelionato digital no Brasil, crime que tem crescido rapidamente nos últimos anos. Foram analisadas as leis e práticas existentes, como o Marco Civil da Internet e a Lei nº 14.155/2021, e constatados avanços importantes, mas insuficientes diante da complexidade do problema.

A dificuldade em identificar e punir criminosos, agravada pelo anonimato e pela atuação transnacional, continua sendo um grande obstáculo. Além disso, a falta de conscientização sobre segurança digital faz com que muitas pessoas se tornem alvos fáceis. Contudo, com o uso de tecnologias avançadas, maior colaboração internacional e iniciativas de educação digital, é possível reduzir os impactos desse crime.

O estudo também destacou a necessidade de atualizar a legislação para acompanhar as constantes inovações tecnológicas e tornar as investigações mais eficazes. Golpes como phishing, clonagem de WhatsApp e fraudes envolvendo o PIX demonstram como os criminosos exploram não apenas ferramentas digitais, mas também o comportamento humano.

Campanhas de conscientização, parcerias entre governo, empresas e sociedade, e o uso estratégico de tecnologias como inteligência artificial e blockchain foram apontados como caminhos promissores. Apesar disso, a pesquisa teve limitações, como a ausência de dados empíricos ou relatos de especialistas e vítimas, que poderiam enriquecer a análise.

Apesar de focar na análise documental e bibliográfica, esta pesquisa trouxe contribuições relevantes ao debate sobre o estelionato digital, destacando desafios e apontando caminhos para sua prevenção e combate. A proposta de aprofundar estudos futuros, com entrevistas de especialistas e vítimas, bem como investigações sobre o papel de tecnologias emergentes, como inteligência artificial e blockchain, reforça a importância de um olhar contínuo sobre o tema. Essas perspectivas complementariam e enriqueceriam as reflexões apresentadas, ampliando as soluções práticas e estratégicas para enfrentar esse crime que afeta diretamente a sociedade moderna.

REFERÊNCIAS

ARAÚJO, Janaína. Aumento de pena para golpes virtuais segue para a CCJ. Senado Federal, 10 out. 2024. Disponível em: https://www12.senado.leg.br/radio/1/noticia/2024/10/10/aumento-de-pena-para-golpes-virtuais-segue-para-a-ccj. Acesso em: 20 nov. 2024.

ARRETO, Alesandro Gonçalves. BRASIL, Beatriz Silveira. Manual de Investigação Cibernética à Luz do Marco Civil da Internet. Rio de Janeiro: Ed. Brasport, 2016.

BARROSO, Luís Roberto. Curso de direito constitucional contemporâneo: os conceitos fundamentais e a construção do novo modelo. 2. ed. São Paulo: Saraiva, 2010.

BIONI, Bruno. Proteção de Dados Pessoais e o Legítimo Interesse. In: SEMINÁRIO DE DIREITO DIGITAL, 2019, São Paulo. Anais [...]. São Paulo: Editora Jurídica Digital, 2019. p. 30-45.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em: 20 nov. 2024.

BRASIL. Lei nº 10.446, de 08 de maio de 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10446.htm. Acesso em: 20 nov. 2024.

BRASIL. Lei nº 12.735, de 30 de novembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 20 nov. 2024.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 nov. 2024.

BRASIL. Lei nº 13.642, de 03 de abril de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13642.htm. Acesso em: 20 nov. 2024.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 20 nov. 2024.

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20 nov. 2024.

CARDOSO, Caroline; RÉGIS, Jonathan Cardoso. Direito Comparado: LGPD e o Marco Civil da Internet. Revista de Direito, v. 16, n. 01, p. 01-23, 2024.

CARVALHO, Patrícia Heloísa de. Marco Civil da Internet: Uma análise sobre a constitucionalidade do artigo 19. Revista da Faculdade de Direito do Sul de Minas,

Pouso Alegre, v. 33, n. 2, p. 228-244, 2017. Disponível em: https://revista.fdsm.edu.br/index.php/revistafdsm/article/view/140. Acesso em: 31 jul. 2022.

CAVALCANTI, Júlio. Princípio pro homine e os direitos dos consumidores no ambiente digital. Revista de Direito Digital, Brasília, 2019.

CHINELLATO, Silmara J. de A. Marco Civil da Internet e direito autoral: Responsabilidade civil dos provedores de conteúdo. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). Direito & Internet III – Tomo II: Marco Civil da Internet (Lei nº 12.965/2014). São Paulo: Quartier Latin, 2015.

DEMÉSIO, Nayume Pereira; LÔBO, Nágela Bitar. Regulação da internet: direito comparado entre a lei marco civil da internet brasileira e a lei argentina digital. Revista Mirante (ISSN 1981-4089), v. 11, n. 6, p. 58-69, 2018.

DONEDA, Danilo. O Marco Civil da Internet e a proteção de dados pessoais. In: SIMPÓSIO INTERNACIONAL DE DIREITO DIGITAL, 2015, São Paulo. Anais [...]. São Paulo: Revista de Direito Digital, 2015. p. 101-118.

GODOY, Carlos Eduardo. Potencialidade Danosa da Internet e Responsabilidade dos Provedores. São Paulo: Revista Jurídica de Direito Digital, 2018.

LIMA, Cintia Rosa Pereira de. A Importância da Autoridade Nacional de Proteção de Dados. In: CONGRESSO INTERNACIONAL DE DIREITO DIGITAL, 2019, Brasília. Anais [...]. Brasília: Revista de Direito e Tecnologia, 2019. p. 55-73.

LUDGERO, Paulo Ricardo. Desvendando o estelionato digital: desafios e estratégias para provar esse crime. JusBrasil, 2023. Disponível em: https://www.jusbrasil.com.br/artigos/desvendando-o-estelionato-digital-desafios-e-estrategias-para-provar-esse-crime/1881946688. Acesso em: 20 nov. 2024.

MACIEL, Rafael Fernandes. (In)Constitucionalidade do Artigo 19 do Marco Civil da Internet à Luz do Constitucionalismo Digital. SSRN Electronic Journal, 2023.
MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Eficácia dos direitos fundamentais nas relações privadas da internet: o dilema da moderação de conteúdo em redes sociais na perspectiva comparada Brasil-Alemanha. Revista de Direito Civil Contemporâneo-RDCC (Journal of Contemporary Private Law), v. 31, p. 33-68, 2022.

MENEZES, Elsio Gomes de Araujo. A prescrição no crime de estelionato previdenciário. Edunit, abril 2016. Disponível em: https://core.ac.uk/works/160940487/?t=94b042bed89ae9a809f3aab5fd1ec477..