ESTELIONATO ELETRÔNICO NO DIREITO DIGITAL

Alana Nagashima de Lima[1]
Bianca e Silva Caires[2]
Carlos Eduardo da Silva Costa Junior[3]
Filipe Borges Marra[4]
Lucas Felipe Machado Silva[5]
Miguel Nardi Coral[6]
Samara Adriele Fernandes Martins Matos[7]
Sarah Emanuelle de Souza Silva[8]
Tayná Cesar Justino de Mello[9]
Vivian Carvalho Santos[10]

RESUMO

A presente pesquisa teórica foi realizada com o objetivo de embasar a atividade extensionista que será realizada no âmbito da disciplina “Direito Digital”, sob orientação do Prof. Dr. Henrique Savonitti Miranda. Concentra-se no estudo do estelionato eletrônico, um crime virtual que afeta principalmente grupos vulneráveis, como idosos e pessoas de baixa renda, que possuem menos domínio dos meios digitais. O estudo destaca a relevância do tema na conscientização e prevenção de golpes cibernéticos, buscando promover o acesso a informações que possibilitem maior segurança na interação digital e reduzir os danos causados por essas práticas ilícitas, que têm se intensificado com o avanço da tecnologia e a popularização da internet no país.

[1] Graduanda em Direito pelo Centro Universitário UniProcessus.
[2] Graduanda em Direito pelo Centro Universitário UniProcessus.
[3] Graduando em Direito pelo Centro Universitário UniProcessus.
[4] Graduando em Direito pelo Centro Universitário UniProcessus.
[5] Graduando em Direito pelo Centro Universitário UniProcessus.
[6] Graduando em Direito pelo Centro Universitário UniProcessus.
[7] Graduanda em Direito pelo Centro Universitário UniProcessus.
[8] Graduanda em Direito pelo Centro Universitário UniProcessus.
[9] Graduanda em Direito pelo Centro Universitário UniProcessus.
[10] Graduanda em Direito pelo Centro Universitário UniProcessus.

1. INTRODUÇÃO

O Direito Digital entra na história para suprir demandas que envolvem princípios e violações dentro do mundo digital, isso é, das relações sociais, contratuais, financeiras, enfim, dos fatos jurídicos que são possíveis e ocorrem por meio da internet. Como aduz Pinheiro (2021), *in verbis:*

> O Direito Digital consiste na evolução do próprio Direito, abrangendo todos os princípios fundamentais e institutos que estão vigentes e são aplicados até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas (Direito Civil, Direito Autoral, Direito Comercial, Direito Contratual, Direito Econômico, Direito Financeiro, Direito Tributário, Direito Penal, Direito Internacional etc.) (PINHEIRO, 2021, p. 71).

No Brasil, atualmente, pode-se perceber um aumento dos crimes de fraude digital, especialmente no que concerne às transações bancárias on-line. Neste trabalho, discorremos sobre o gênero do qual o “golpe do PIX”, por exemplo, é uma das espécies: o estelionato eletrônico, digital ou virtual, ou, em um termo técnico do Direito, a fraude eletrônica.

O Estelionato Eletrônico é uma forma qualificada do crime de Estelionato comum (Art. 171 do CP). Foi inserido no Código Penal Brasileiro pela Lei Federal 14.155/21, nos § 2º-A e § 2º-B do art. 171, sendo intitulado por Fraude Eletrônica.

O estelionato é um golpe em que o criminoso induz uma pessoa, por vontade própria, a lhe fornecer dados e informações pessoais, os quais serão usados para obtenção de vantagem financeira em prejuízo da vítima. Quando esse golpe é praticado através de redes sociais, telefone, e-mail ou qualquer outro meio digital, ocorre então o Estelionato Eletrônico. (TJDFT, 2024).

Como em qualquer crime em que um dos influenciadores da causa é o fator oportunidade, no Estelionato Digital não é diferente. À medida que a sociedade se moderniza com o avanço da internet, inclusive após a adaptação global provocada pela pandemia do COVID-19, amplia-se o espaço para atuação de criminosos pelos meios digitais. (VEJA, 2024).

Além disso, o conforto, a agilidade e a segurança da atuação em âmbito remoto também incentiva a prática dos delitos digitais, já que nesses casos o crime pode ser

cometido de qualquer lugar do mundo, com anonimato e sem exposição física, minimizando quase que absolutamente um possível confronto do criminoso com a polícia e até mesmo com a vítima. (CONSULTOR JURÍDICO, 2024).

Enquanto o Estelionato comum possui pena de reclusão de 1 a 5 anos, a modalidade eletrônica funciona como qualificadora, cuja pena é de 4 a 8 anos, além de multa, nos dois casos. Pode haver ainda um aumento dessas penas caso o crime seja praticado utilizando-se de servidor mantido em território internacional.

Vejamos como a definição do crime consta no Código Penal (BRASIL, 1940):

> **Estelionato**
> Art. 171. Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
> Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis. (Vide Lei nº 7.209, de 1984)
> § 1º - Se o criminoso é primário, e é de pequeno valor o prejuízo, o juiz pode aplicar a pena conforme o disposto no art. 155, § 2º.
> **Fraude eletrônica**
> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. (Incluído pela Lei nº 14.155, de 2021)
> § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional. (Incluído pela Lei nº 14.155, de 2021).

Com efeito, o atual grande sucesso dos crimes cometidos na esfera digital é também fruto da insuficiente educação digital sobre os métodos eficientes de prevenção e proteção virtual.

Considerando que grande parte da sociedade brasileira tem acesso à internet, podemos destacar entre eles a parte mais vulnerável dessa grande massa, que são os idosos, que, pelo maior desconhecimento dos meios virtuais, tornam-se alvos fáceis dos criminosos que utilizam as ferramentas oferecidas pela tecnologia para realizar diversos tipos de cibercrimes, em diferentes contextos e usando várias técnicas.

O ambiente virtual tornou-se frequentemente mais vantajoso para os delinquentes, pois apresenta menores riscos, conforme apontam Diniz, Cardoso e Puglia (2022, p. 24 -25):

> Hoje em dia, o pensamento do criminoso, como já mencionado, é no sentido de que é muito mais vantajoso permanecer em casa e aplicar golpes via internet utilizando-se do anonimato do que sair para as ruas e roubar. Dá mais dinheiro, se a prática criminosa for descoberta, a pena é menor, pois ausentes a violência e a grave ameaça, e o risco de ser morto em um confronto com a polícia ou até mesmo com a própria vítima é praticamente zero.

Segundo o Fórum Brasileiro de Segurança Pública, o aumento alarmante dos estelionatos e fraudes eletrônicas no Brasil tem sido uma preocupação crescente, conforme evidenciado no Anuário Brasileiro de Segurança Pública de 2023. Definido no artigo 171 do Código Penal, o crime de estelionato consiste em obter vantagem ilícita em prejuízo de outrem, utilizando-se de artifícios fraudulentos. A crescente digitalização da sociedade brasileira, impulsionada pela pandemia de Covid-19, resultou em um aumento expressivo dessas práticas criminosas, principalmente em meios eletrônicos (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2023, p. 84).

O documento cita que, em 2021, foi introduzida a tipificação específica para fraudes eletrônicas, que abrange crimes cometidos por meio de redes sociais, aplicativos de mensagens e e-mails fraudulentos. Esse movimento legislativo foi uma resposta ao aumento expressivo desses crimes, que cresceram 326,3% entre 2018 e 2022, atingindo 1.819.409 registros no último ano, uma média de 207,7 casos por hora. Esse aumento é particularmente preocupante, uma vez que muitos casos podem não ser registrados, o que sugere que o cenário real pode ser ainda mais grave (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2023, p. 93).

Além disso, os estudos destacam que o isolamento social durante a pandemia ampliou as oportunidades para criminosos virtuais, que se aproveitaram da vulnerabilidade das pessoas e da crescente dependência das redes digitais para realizar atividades cotidianas. A engenharia social, técnica usada para induzir vítimas a fornecer informações confidenciais, tem sido amplamente empregada, diversificando os métodos de ataque e ampliando o alcance dos golpes (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2023, p. 93).

Ainda de acordo com o Anuário, um exemplo notório de estelionato eletrônico é o "golpe do amor", onde os criminosos estabelecem relações afetivas virtuais com as vítimas para obter vantagens financeiras. Casos como o de uma idosa que perdeu

208 mil reais para um golpista que se passava por uma celebridade são emblemáticos do impacto devastador dessas fraudes (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2023, p. 94).

Quando aludimos golpes digitais, podemos salientar que existem várias formas, dentre eles: o golpe do PIX; o golpe do falso emprego; o golpe do empréstimo; o golpe do precatório; o golpe do link falso; o golpe da falsa central de atendimento; o golpe do falso boleto; o golpe do sequestro de dados e o estelionato sentimental.

O estelionato eletrônico tem se destacado como uma das principais formas de crime cibernético, explorando vulnerabilidades humanas e tecnológicas para obter vantagens financeiras ilícitas. Dentre as modalidades mais comuns desse tipo de fraude, incluem-se phishing, vishing, golpes no comércio eletrônico e técnicas de engenharia social. Além de descrever o funcionamento dessas práticas criminosas, apresentam-se estratégias de proteção para indivíduos e organizações, ressaltando a importância da conscientização e do uso de ferramentas de segurança digital. (TJDFT, 2024).

2. DESENVOLVIMENTO DO TEMA PESQUISADO

2.1 Modalidades do Estelionato Eletrônico

Da análise do livro Cibersegurança para Leigos, do autor Joseph Steinberg (2020), extraiu-se conceitos desses principais tipos de fraudes eletrônicas, como o phishing, que é uma técnica de fraude cibernética que consiste em enganar uma pessoa ao se passar por uma entidade confiável, induzindo-a a realizar uma ação, como fornecer informações pessoais.

Por exemplo, um golpista pode enviar um e-mail que parece ser de um banco renomado, solicitando ao destinatário que clique em um link para redefinir sua senha devido a uma suposta violação de segurança. Ao clicar no link, a vítima é direcionada para um site que imita o site oficial do banco, mas que, na verdade, é controlado pelo criminoso. Este, então, coleta as credenciais de login da vítima, como nome de usuário e senha, para acessar sua conta bancária (STEINBERG, 2020, p. 52).

O spear phishing é uma variante mais direcionada do phishing, em que os ataques são personalizados para atingir uma pessoa, empresa ou organização específica. Criminosos que utilizam essa técnica geralmente pesquisam minuciosamente seus alvos, aproveitando informações obtidas em redes sociais e outras fontes públicas para criar mensagens fraudulentas altamente convincentes. Ao contrário do phishing convencional, que é mais genérico, o spear phishing é projetado para parecer uma comunicação legítima, aumentando a probabilidade de sucesso (STEINBERG, 2020, p. 52-53).

A fraude do CEO é uma forma específica de spear phishing em que o criminoso se passa pelo CEO ou outro executivo sênior de uma empresa. Nesse tipo de golpe, o objetivo é induzir um funcionário, muitas vezes do departamento financeiro, a realizar ações como transferir fundos para uma conta controlada pelo criminoso ou enviar documentos sensíveis. O impacto desse tipo de fraude pode ser significativo, resultando em perdas financeiras substanciais e, frequentemente, em consequências graves para os funcionários envolvidos, como a demissão (STEINBERG, 2020, p. 53-54).

Smishing é uma variação do phishing que utiliza mensagens de texto (SMS) como meio de ataque. Assim como no phishing tradicional, o objetivo é obter informações pessoais ou induzir a instalação de malware no dispositivo da vítima. Essa técnica se aproveita da confiança que muitos usuários depositam em mensagens de texto, especialmente quando parecem ser enviadas por instituições financeiras ou serviços conhecidos (STEINBERG, 2020, p. 54-55).

Vishing, ou phishing por voz, é uma técnica em que os golpistas utilizam chamadas telefônicas para enganar as vítimas. Embora hoje muitas dessas chamadas sejam realizadas via sistemas de voz sobre IP (VoIP), os criminosos ainda utilizam linhas telefônicas tradicionais para se passar por representantes de empresas ou instituições governamentais, convencendo as vítimas a fornecer informações confidenciais (STEINBERG, 2020, p. 55).

Whaling é uma forma de spear phishing direcionada a executivos de alto nível ou funcionários públicos. Esse tipo de ataque é altamente sofisticado e visa a obtenção de informações críticas ou a execução de transações financeiras significativas. Devido ao perfil das vítimas, os ataques de whaling exigem uma

preparação minuciosa e são frequentemente mais difíceis de detectar (STEINBERG, 2020, p. 55).

Em alguns casos, os criminosos não buscam interromper as operações de uma organização, mas sim explorá-las para obter ganhos financeiros. Isso é feito por meio da adulteração de dados, que pode ocorrer durante a transmissão ou enquanto os dados estão armazenados nos sistemas da organização. Por exemplo, um golpista pode interceptar uma transação bancária e alterar os detalhes da conta destinatária para desviar os fundos. Alternativamente, o criminoso pode invadir um sistema e modificar informações críticas, como os detalhes de pagamento de um fornecedor, para que os pagamentos sejam direcionados para uma conta fraudulenta.

Tem-se que a prática de compartilhar senhas e credenciais de acesso com outras pessoas é identificada como uma vulnerabilidade significativa. Nesse sentido, a obra Cibersegurança para Leigos enfatiza a importância de estabelecer credenciais únicas para cada sistema e de utilizar ferramentas de gerenciamento de senhas. Adicionalmente, o autor aborda a necessidade de utilizar as redes sociais de forma consciente, evitando o compartilhamento excessivo de informações pessoais que possam ser utilizadas por cibercriminosos para fins maliciosos (STEINBERG, 2020, p. 220).

Continuando, o autor afirma que a crença de ser um alvo potencial para ataques cibernéticos induz o indivíduo a adotar comportamentos mais seguros, como a verificação da autenticidade de e-mails e a proteção de credenciais de acesso (STEINBERG, 2020, p. 243). Cita-se a relevância da realização de backups regulares e da utilização de senhas robustas para mitigar os riscos associados à perda de dados e à invasão de contas (STEINBERG, 2020, p. 340-341).

Sintetizando as principais recomendações para a proteção de dados em um ambiente digital cada vez mais hostil, segundo Steinberg (2020), tem-se dez medidas de baixo custo que podem ser implementadas por qualquer usuário. Dentre as estratégias apresentadas pelo autor, destaca-se a importância da conscientização sobre as ameaças cibernéticas, a adoção de softwares de segurança atualizados e a criptografia de dados sensíveis (STEINBERG, 2020, p. 462).

Demonstra-se, dessa forma, que a adoção de medidas de segurança simples e eficazes pode contribuir significativamente para a proteção de dados pessoais e corporativos em um cenário de crescente complexidade e sofisticação das ameaças cibernéticas. As recomendações apresentadas neste estudo podem servir como um guia para indivíduos e organizações que buscam fortalecer sua postura de segurança da informação.

2.2 Aspectos Legais e Regulatórios do Estelionato Eletrônico

O estelionato eletrônico, fenômeno crescente no cenário digital contemporâneo, exigiu, com o passar dos anos, a construção de um entendimento jurisprudencial e de uma legislação específica para que o regulamentasse. Com a evolução das fraudes virtuais, surgiu a necessidade de um aprofundamento das normas que visam combater essas práticas ilícitas e proteger os usuários da internet.

Anteriormente a uma regra específica, o Código Penal brasileiro, embora elaborado em 1940, muito antes da criação da internet, oferecia dispositivos que pudessem ser aplicados a situações e crimes que hoje são classificados como estelionato eletrônico. O crime de estelionato, como demonstrado acima, vem previsto no art. 171 do Código Penal. Somente em maio de 2021, é que o artigo foi alterado pela Lei n. 14.155, que introduziu, nos §§ 2º-A e 2º-B, a figura da “fraude eletrônica” (BRASIL, 2021).

Conforme os novos dispositivos, se o crime for cometido com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo, a pena é de reclusão, de quatro a oito anos, e multa. Se for praticada por meio da utilização de servidor mantido fora do território nacional, considerada a relevância do resultado gravoso, a pena é aumentada de um terço a dois terços.

A inovação legislativa deu-se em grande medida em resposta ao momento vivido, durante a pandemia de Covid-19. Pelo distanciamento social e a maior utilização de grande parte da população dos meios digitais para a realização das

atividades pessoais e profissionais, o número de fraudes virtuais havia aumentado muito no Brasil.

Silva e Carvalho, no entanto, sugerem que a aplicação dessa norma ao contexto digital exige uma interpretação que considere as especificidades dos crimes cibernéticos, dado o caráter dinâmico e inovador das fraudes virtuais (SILVA; CARVALHO, 2022, p. 55).

O Marco Civil da Internet (Lei nº 12.965/2014) complementa o Código Penal ao estabelecer princípios e regras para o uso da internet no Brasil, com foco na proteção da privacidade, na neutralidade da rede e na responsabilidade dos provedores de aplicações.

Essa legislação representa um marco na regulamentação do uso da internet no Brasil. Ao estabelecer um conjunto de normas para o ambiente digital, a lei visa garantir a privacidade dos usuários, limitando a coleta e o uso de dados pessoais. Além disso, o Marco Civil assegura a liberdade de expressão, desde que exercida dentro dos limites legais, combatendo a censura e promovendo a diversidade de opiniões. Dessa forma, a legislação busca promover um ambiente virtual mais seguro e democrático para todos os usuários (GONÇALVES; HENRIQUES; 2024, p. 6).

A Lei do Marco Civil da Internet é estruturada em três princípios fundamentais: neutralidade da rede, liberdade de expressão e proteção à privacidade. A neutralidade garante que o tráfego de dados na internet não sofra discriminação baseada em conteúdo, origem, ou destino, enquanto a liberdade de expressão assegura o direito de manifestação no ambiente digital, equilibrando-o com a proteção à intimidade e honra das pessoas. Já a privacidade dos usuários é tratada de forma abrangente, introduzindo a proteção de dados no sistema jurídico brasileiro. Apesar da relevância da legislação, sua eficácia depende de uma fiscalização rigorosa por parte do Estado e da sociedade, para garantir que a liberdade de expressão e a privacidade sejam preservadas. Entretanto, o alcance da lei é limitado, exigindo uma abordagem internacional mais robusta para enfrentar as violações de direitos no ambiente digital (LEITE, 2016, p. 159).

A Lei Geral de Proteção de Dados (LGPD), sancionada em 2018 e em vigor desde 2020, constitui um avanço significativo na proteção de dados pessoais no

Brasil. Nela são estabelecidos princípios rigorosos para o tratamento de dados, conferindo aos seus titulares maior controle sobre as informações pessoais e impondo às empresas a responsabilidade de garantir a segurança desses dados (BRASIL, 2018).

A lei foi criada para proteger direitos fundamentais relacionados à liberdade, privacidade e ao desenvolvimento pessoal. Seu objetivo é definir normas para a gestão e proteção de dados pessoais de indivíduos e entidades empresariais, assegurando os direitos dos cidadãos e regulando o processamento de dados por instituições públicas e privadas. A principal motivação para a criação dessa lei é prevenir abusos da privacidade dos usuários, salvaguardando seus direitos e evitando o uso indevido de suas informações pessoais (HENRIQUES; GONÇALVES, 2024, p.6).

No entanto, conforme destacam Santos e Sotero, a implementação da LGPD ainda é um processo em curso e os desafios persistem. A adaptação das empresas aos novos padrões de proteção de dados tem sido gradual, e a vulnerabilidade dos dados continua sendo uma preocupação. A lei, embora seja um avanço significativo, ainda precisa ser aprimorada para acompanhar a rápida evolução do ambiente digital. A necessidade de reformulações legislativas e de um compromisso constante com a inovação jurídica é evidente para garantir a segurança e a privacidade dos dados dos cidadãos em um mundo cada vez mais conectado (2024, p. 10-11).

A responsabilidade das plataformas digitais em relação aos crimes de estelionato eletrônico é um tema complexo que envolve considerações legais, técnicas e éticas. Segundo o Marco Civil da Internet, a responsabilidade dos provedores de aplicações de internet, como redes sociais e marketplaces, é, em princípio, subjetiva e depende do descumprimento de uma ordem judicial específica para a remoção de conteúdo ilegal (BRASIL, 2014). Essa estrutura foi estabelecida para equilibrar a liberdade de expressão na internet com a necessidade de proteger os usuários de abusos.

Contudo, a aplicação desse modelo de responsabilidade tem sido considerada insuficiente para combater crimes como o estelionato eletrônico, caracterizado por fraudes que induzem a vítima a entregar valores ou informações sensíveis. Como destaca Alves, a regulamentação da responsabilidade das plataformas deve

demandar o desenvolvimento de planos de segurança robustos, que garantam medidas precisas de combate à fraude e rapidez na exclusão do conteúdo malicioso. A colaboração entre governos, empresas e organizações da sociedade civil é fundamental para um combate pleno e eficaz aos crimes virtuais (ALVES, 2023, p.37).

A jurisprudência brasileira também reconhece a responsabilidade de plataformas que falham em adotar medidas de segurança adequadas para evitar fraudes, como observado no acórdão do Tribunal de Justiça do Distrito Federal e Territórios (TJDFT), no qual o Facebook Brasil (responsável pelo aplicativo WhatsApp) foi condenado por demora no bloqueio de uma conta clonada, facilitando a aplicação de golpes. O tribunal concluiu que, ao não agir prontamente, a plataforma contribuiu para a perpetuação da fraude e, portanto, foi responsabilizada por danos morais. Assim, as plataformas digitais podem ser co-responsáveis pelos prejuízos causados quando não adotam medidas eficazes de segurança, conforme os parâmetros do Código de Defesa do Consumidor (TJDFT, 2021).

Além disso, a responsabilidade civil, tradicionalmente associada às teorias da culpa e do risco, tem sido adaptada no contexto digital para lidar com as peculiaridades da internet. No Direito Digital, a teoria do risco, que dispensa a prova de culpa, é mais aplicável devido à natureza global e dinâmica da rede. A Lei do Marco Civil da Internet introduziu novos parâmetros, isentando os provedores de conexão de responsabilidade sobre o conteúdo que trafega em suas redes, enquanto os provedores de aplicação só são responsabilizados após ordem judicial. Essa mudança visa preservar a liberdade de expressão, mas impõe um custo maior à vítima que, ao ver seu conteúdo ofensivo na rede, só pode solicitar sua remoção mediante decisão judicial, aumentando o tempo e o impacto dos danos sofridos. (PINHEIRO, 2024, p. 527-538)

Pinheiro (2024, p. 527-538) cita ainda que a lei prioriza a liberdade de expressão, mas levanta questões sobre a proteção da honra e da privacidade dos usuários. Antes do Marco Civil, a vítima podia solicitar a remoção de conteúdo diretamente ao provedor, o que acelerava a resolução do problema. Agora, essa dinâmica mudou, e a remoção só ocorre após intervenção judicial, o que pode gerar prejuízos adicionais à vítima devido à demora. Ao mesmo tempo, é necessário um

equilíbrio, para evitar que a remoção arbitrária de conteúdo interfira na liberdade de expressão, criando um desafio para o Judiciário ao aplicar essas novas regras.

Portanto, embora o Marco Civil da Internet estabeleça um marco regulatório inicial, há uma crescente demanda por uma responsabilidade mais proativa das plataformas digitais em prevenir e combater o estelionato eletrônico. A complexidade e a rápida evolução dos crimes digitais exigem que tanto a legislação quanto a atuação das plataformas sejam constantemente atualizadas para enfrentar esses desafios de maneira eficaz.

2.3 Prevenção e Combate ao Estelionato Eletrônico

Como visto, a ocorrência dos crimes virtuais aumentou significativamente com a crescente digitalização de serviços e a expansão do acesso à internet. De acordo com relatórios de segurança cibernética, as fraudes online estão entre as principais causas de perda financeira em todo o mundo. A situação no Brasil também é semelhante: os casos de estelionato eletrônico têm aumentado com frequência no país, causando grande preocupação aos profissionais do direito e à sociedade em geral.

Em 2022, os casos de estelionato no Brasil atingiram um recorde de 1.819.409 ocorrências, o que equivale a uma média de 207,7 casos registrados por hora. Em relação a 2021, houve um aumento de 37,9% no total de registros de estelionato no país. O panorama dos crimes eletrônicos é ainda mais alarmante. Apenas em 2022, os estelionatos eletrônicos somaram 200.322 casos, mesmo sem dados de cinco estados populosos (BA, CE, RJ, RS e SP) e do Rio Grande do Norte. Esse número representa um crescimento de 65,2% em relação a 2021, ano em que o crime foi tipificado (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2023, p.94).

Essas estatísticas reforçam a necessidade urgente de medidas mais eficazes de combate a esses crimes, como campanhas de conscientização e o fortalecimento das investigações digitais. Embora a Lei nº 14.155/2021 tenha elevado as penas para o estelionato eletrônico, o aumento contínuo nos casos revela que os criminosos estão se aproveitando de situações específicas, como o uso crescente da internet para trabalho e compras, além de técnicas de engenharia social, que tornam a população

mais vulnerável. O relatório aponta para a necessidade de ações mais rigorosas para proteger a sociedade e reduzir a crescente incidência desses crimes (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2023, p.95).

Para combater esse tipo de crime de forma eficaz, é necessária uma abordagem integrada que inclua medidas preventivas e reativas. O método mais eficaz é, sem dúvida, a prevenção, pois visa reduzir as chances de o crime ocorrer. No entanto, para que a prevenção seja eficaz, ela precisa ser compreendida de uma perspectiva ampla, incluindo a criação de tecnologias de segurança e o fomento da conscientização e educação digital.

A conscientização é um poderoso instrumento para evitar fraudes eletrônicas. As campanhas educacionais são essenciais para capacitar os usuários a identificar e a evitar golpes. Diversas entidades e agências governamentais têm feito campanhas de conscientização para uma variedade de públicos, reconhecendo que as vulnerabilidades mudam com o conhecimento da tecnologia.

Por exemplo, a Receita Federal do Brasil realiza regularmente campanhas de esclarecimento sobre fraudes relacionadas a impostos de renda para alertar os contribuintes sobre e-mails falsos e sites clonados que tentam obter informações sigilosas. Estas iniciativas têm demonstrado ser eficazes na redução do número de incidentes, ao mesmo tempo em que incentivam a educação continuada sobre segurança digital (BRASIL, 2024).

Além de campanhas públicas, a educação digital deve ser incorporada ao currículo escolar. Isso ajudará a preparar as futuras gerações para enfrentar os desafios e as ameaças do mundo virtual. A introdução de disciplinas sobre segurança digital nos currículos das escolas e universidades pode contribuir significativamente para formar cidadãos mais conscientes e preparados para lidar com o mundo digital de forma segura.

Outra parte essencial da prevenção e combate ao estelionato eletrônico é a tecnologia. A autenticação de dois fatores (2FA) é uma medida crucial para aumentar a segurança de suas contas. Ela exige uma segunda forma de verificação, além da senha, o que cria uma camada extra de proteção. Dessa forma, mesmo que um atacante consiga suas credenciais, o acesso ainda será bloqueado (ROSA; MALIMPENSA; CARDOSO, 2023, p.8).

A criptografia é uma ferramenta essencial para a proteção de dados, pois transforma a informação original em uma forma oculta, garantindo sua segurança. Desde a década de 1970, o termo abrange um conjunto de técnicas matemáticas utilizadas para proteger informações em diversas aplicações. A cifração de dados se destaca como uma das principais técnicas, preferida ao termo “criptografia de dados” por evitar ambiguidades. Além da cifração, outras técnicas como o resumo criptográfico (hash) e assinaturas digitais são fundamentais para atender aos requisitos de segurança em sistemas modernos (Dahab, R, 2024, p.15).

A tecnologia é uma aliada importante na prevenção de crimes cibernéticos, e os Sistemas de Detecção de Intrusos (SDI) desempenham um papel crucial nesse cenário. Esses sistemas, sejam de software ou hardware, automatizam o monitoramento de eventos em redes e computadores, identificando falhas de segurança, tentativas de intrusão, anomalias e abusos. Considerados uma solução inovadora, os SDIs são amplamente utilizados em empresas, instituições governamentais e redes acadêmicas, oferecendo uma ferramenta poderosa de suporte para administradores de segurança (SANTOS, GLENDA, 2003, p.15).

A proteção contra estelionato eletrônico também depende do uso de firewalls avançados e softwares de antivírus que bloqueiam o acesso de agentes mal-intencionados aos sistemas. A implementação de redes privadas virtuais (VPNs) é uma prática cada vez mais comum em muitas empresas que querem a proteção dos seus dados durante a transferência de dados. As VPNs criptografam os dados em trânsito e garantem que as informações trafeguem de maneira segura, mesmo em redes públicas (AKINSANYA, M. O; EKECHI, C. C.; OKEKE, 2024, p.1460).

Além das iniciativas educacionais e tecnológicas, a legislação desempenha um papel crucial na proteção contra o estelionato eletrônico. A Lei nº 12.737, de 2012, conhecida como Lei Carolina Dieckmann, estabelece no Art. 154-A que a invasão de dispositivos eletrônicos com o objetivo de obter, adulterar ou destruir dados, bem como a divulgação não autorizada desses dados, é considerada um crime. A pena

para tal violação inclui detenção de 3 (três) meses a 1 (um) ano, além de multa (BRASIL, 2002).

Complementarmente, a Lei nº 13.709, de 2018, ou Lei Geral de Proteção de Dados (LGPD), define regras rigorosas para a coleta, armazenamento e tratamento de dados pessoais. Essa legislação exige que as empresas implementem medidas de segurança robustas para proteger as informações de seus clientes. O Art. 9º da LGPD garante ao titular o direito ao acesso facilitado às informações sobre o tratamento de seus dados, que devem ser disponibilizadas de forma clara, adequada e ostensiva. Isso inclui a finalidade do tratamento, a forma e a duração do tratamento, a identificação e o contato do controlador, o uso compartilhado de dados e suas finalidades, as responsabilidades dos agentes de tratamento, e os direitos do titular conforme o Art. 18 da Lei (BRASIL, 2018).

Para prevenir práticas ilícitas e garantir que os criminosos cibernéticos sejam punidos, a implementação dessas leis é crucial. A colaboração entre os setores público e privado é vital, especialmente no que diz respeito à troca de informações sobre ameaças emergentes e à coordenação das respostas a incidentes de segurança.

Por fim, a prevenção e combate ao estelionato eletrônico requer uma abordagem multifacetada que inclua educação, conscientização, ferramentas tecnológicas avançadas e um arcabouço legal robusto. É necessário que todos os setores da sociedade colaborem para criar um ambiente digital mais seguro em que as pessoas possam aproveitar a tecnologia sem estar sempre sob a ameaça de fraude eletrônica. A cooperação contínua é necessária para proteger os direitos dos usuários no meio digital e reduzir a frequência desses crimes.

3. CONSIDERAÇÕES FINAIS

Uma abordagem legal e preventiva eficaz contra o estelionato eletrônico é indispensável para a proteção de indivíduos e empresas em um mundo cada vez mais digital. Uma resposta legal sólida, com legislação atualizada e rigorosa, é imprescindível para responsabilizar os criminosos e desencorajar futuras atividades fraudulentas. Além disso, medidas preventivas, como a educação em cibersegurança,

a implementação de sistemas eficazes de proteção de dados e a conscientização sobre práticas online seguras, são fundamentais para diminuir a ocorrência deste crime.

A combinação dessas estratégias legais e preventivas promove um ambiente digital mais seguro e confiável, protegendo a integridade financeira e pessoal dos cidadãos

A regulamentação do estelionato eletrônico no Brasil enfrenta sérios obstáculos em um cenário de transformação tecnológica acelerada e aumento da digitalização nas interações sociais e comerciais. Com a crescente dependência da internet para realizar transações financeiras e manter comunicações, crimes cibernéticos, como o estelionato eletrônico, tornaram-se mais frequentes e complexos.

Apesar dos avanços na legislação brasileira nos últimos anos, especialmente com a introdução do Marco Civil da Internet e da Lei Geral de Proteção de Dados (LGPD), é fundamental que o arcabouço legal continue a se adaptar para enfrentar as novas modalidades de fraudes e garantir a segurança dos cidadãos.

Um dos desafios centrais é a necessidade de uma cooperação mais eficaz entre as autoridades nacionais e internacionais, dado que muitos crimes cibernéticos têm origem em outros países.

Além disso, é fundamental capacitar as forças de segurança e o sistema judiciário para enfrentar a complexidade desses delitos, que frequentemente envolvem tecnologias sofisticadas e exigem conhecimentos especializados. A conscientização do público também é vital, pois a prevenção se destaca como uma das estratégias mais eficientes no combate ao estelionato eletrônico.

A forma como será regulado o estelionato eletrônico no Brasil no futuro estará atrelada à habilidade do país em inovar suas práticas legais e de prevenção, assim como em cultivar uma cultura de segurança cibernética entre seus cidadãos. Isso envolve o fortalecimento das colaborações entre o governo, o setor privado e a sociedade civil para a criação de estratégias mais completas e eficazes.

Com o avanço contínuo da tecnologia, é fundamental que a legislação se mantenha dinâmica, antecipando-se, quando possível, às novas situações,

assegurando que a proteção dos cidadãos evolua juntamente com as mudanças no ambiente digital.

REFERÊNCIAS BIBLIOGRÁFICAS

AKINSANYA, M. O; EKECHI, C. C.; OKEKE. (2024). **REDES PRIVADAS VIRTUAIS (VPN): UMA REVISÃO CONCEITUAL DE PROTOCOLOS DE SEGURANÇA E SUA APLICAÇÃO EM REDES MODERNAS**. Engineering Science & Technology Journal , 5 (4), 1452-1472. Disponível em: https://doi.org/10.51594/estj.v5i4.1076. Acesso em: 11 Set. 2024.

ALVES, F. B. S. **Estelionato na internet: análise dos aspectos jurídicos e prevenção à criminalidade cibernética**. TCC (Bacharelado em Direito) - Universidade São Judas, São Paulo, 2023. Disponível em: https://repositorio.animaeducacao.com.br/items/0277af95-f38e-4f7f-9067-d944782d850e. Acesso em 04 set. 2024.

ARAÚJO, C. R. **Crimes virtuais: desafios e perspectivas**. Expert Editora, 2023. Disponível em: https://experteditora.com.br/wp-content/uploads/2023/07/Crimes-virtuais.pdf. Acesso em: 04 set. 2024.

BRASIL. **Anuário Brasileiro de Segurança Pública**. Fórum Brasileiro de Segurança Pública, 2023. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2023/07/anuario-2023.pdf. Acesso em: 04 set. 2024.

BRASIL. Código Civil. **Lei nº 10.406, de 10 de janeiro de 2002**. Diário Oficial da União, Brasília, DF, 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm?ref=blog.suitebras.com. Acesso em: 10/09/2024

BRASIL. Código Penal. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Diário Oficial da União, Brasília, DF, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848.htm. Acesso em: 04 set. 2024.

BRASIL. **Lei nº 14.155, de 27 de maio de 1921**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 04 set. 2024.

BRASIL. Lei Geral de Proteção de Dados. **Lei nº 13.709, de 14 de agosto de 2018**. Diário Oficial da União, Brasília, DF, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2018-2022/2018/lei/l13709.htm. Acesso em: 04 set. 2024.

BRASIL. Marco Civil da Internet. **Lei nº 12.965, de 23 de abril de 2014**. Diário Oficial da União, Brasília, DF, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 04 set. 2024.

BRASIL. Lei Carolina Dieckmann. **Lei nº 12.737/2012, de 30 de novembro de 2012**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 04 set. 2024.

BRASIL. Receita Federal. **Receita Federal alerta para o golpe do falso APP IRPF**. 2024. Disponível em: https://www.gov.br/receitafederal/pt-br/assuntos/noticias/2024/abril/receita-federal-alerta-nova-versao-do-golpe-do-erro-na-declaracao-do-imposto-de-renda-em-circulacao. Acesso em: 12 set. 2024.

BRASIL. Tribunal de Justiça do Distrito Federal e Territórios. TJDFT. **Acórdão 1351626**, 07157125920208070020, Relator: ANA CLAUDIA LOIOLA DE MORAIS MENDES, Segunda Turma Recursal dos Juizados Especiais do Distrito Federal, data de julgamento: 28/6/2021, publicado no DJE: 8/7/2021. Disponível em: https://pesquisajuris.tjdft.jus.br/IndexadorAcordaos-web/sistj?visaoId=tjdf.sistj.acordaoeletronico.buscaindexada.apresentacao.VisaoBuscaAcordao&controladorId=tjdf.sistj.acordaoeletronico.buscaindexada.apresentacao.ControladorBuscaAcordao&visaoAnterior=tjdf.sistj.acordaoeletronico.buscaindexada.apresentacao.VisaoBuscaAcordao&nomeDaPagina=resultado&comando=abrirDadosDoAcordao&enderecoDoServlet=sistj&historicoDePaginas=buscaLivre&quantidadeDeRegistros=20&baseSelecionada=BASE_ACORDAO_TODAS&numeroDaUltimaPagina=1&buscaIndexada=1&mostrarPaginaSelecaoTipoResultado=false&totalHits=1&internet=1&numeroDoDocumento=1351626. Acesso em 04 set. 2024.

BRASIL. Tribunal de Justiça do Distrito Federal e Territórios. TJDFT. **Estelionato**. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/estelionato-1#:~:text=A%20fraude%20eletr%C3%B4nica%20ocorre%20quando,cart%C3%A3o%20de%20cr%C3%A9dito%20ou%20d%C3%A9bito. Acesso em: 9 set. 2024.

BRETZ, W. **Organizações criminosas, crime de estelionato digital e a quebra de sigilo bancário sequencial**. Disponível em: https://www.conjur.com.br/2024-jan-12/organizacoes-criminosas-crime-de-estelionato-digital-e-a-quebra-de-sigilo-bancario-sequencial/. Acesso em: 9 set. 2024.

CARVALHO, G. C. **A Lei Geral de Proteção de Dados como instrumento jurídico no combate ao estelionato virtual**. Disponível em: https://www.jusbrasil.com.br/artigos/a-lei-geral-de-protecao-de-dados-como-instrumento-juridico-no-combate-ao-estelionato-virtual/2396725443. Acesso em: 04 set. 2024.

CERT.br. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de Segurança para Internet - Phishing e Vishing**. Disponível em: https://cartilha.cert.br/phishing/. Acesso em: 9 set. 2024.

DAHAB, R. (2024). **O papel basilar da Criptografia na segurança de dados.** Computação Brasil, (52), 14–21.Disponível em: https://doi.org/10.5753/compbr.2024.52.4598. Acesso em: 18 out. 2024

DINIZ, F. F.; CARDOSO, J. R.; PUGLIA, E. H. P. **O crime de estelionato e suas implicações na era contemporânea: o constante crescimento dos golpes via internet**. LIBERTAS DIREITO, [S. l.], v. 3, n. 1, 2022. Disponível em: https://periodicos.famig.edu.br/index.php/direito/article/view/215. Acesso em: 4 set. 2024.

FILHO, V. H. **Considerado o ‘crime da moda’, estelionato digital cresce no Brasil**. Disponível em: https://veja.abril.com.br/brasil/considerado-o-crime-da-moda-estelionato-digital-cresce-no-brasil. Acesso em: 9 set. 2024.

FREITAS, V. V. M. S. de; SANTOS, W. B. dos; CURY, L. V. M. **CRIMES VIRTUAIS: UM OLHAR SOB A ÓTICA DO DIREITO PENAL**. Revista Ibero-Americana de Humanidades, Ciências e Educação, [S. l.], v. 9, n. 5, p. 1285–1304, 2023. DOI: 10.51891/rease.v9i5.9868. Disponível em: https://periodicorease.pro.br/rease/article/view/9868. Acesso em: 5 set. 2024.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **18º Anuário Brasileiro de Segurança Pública**. São Paulo: Fórum Brasileiro de Segurança Pública, 2024. Disponível em: https://publicacoes.forumseguranca.org.br/handle/123456789/253. Acesso em: 11 set. 2024.

HENRIQUES, T. A.; GONÇALVES, S. M. **Crimes digitais: análise sobre o estelionato virtual**. Revista Eletrônica de Ciências Jurídicas, [S. l.], v. 14, n. 1, 2024. Disponível em: https://revista.fadipa.br/index.php/cjuridicas/article/view/567. Acesso em: 04 set. 2024.

KASPERSKY. **Engenharia Social e Suas Modalidades**. Disponível em: https://www.kaspersky.com. Acesso em: 9 set. 2024.

LEITE, F. P. A. **O exercício da liberdade de expressão nas redes sociais: e o Marco Civil da Internet**. Revista de Direito Brasileira. São Paulo, SP. v. 13. n. 6. p. 150 -166. jan./abr. 2016. Disponível em: https://www.indexlaw.org/index.php/rdb/article/view/2899. Acesso em: 04 set. 2024.

MENDES, F. **Enfrentando o estelionato virtual: análise da Lei 14.155/2021 e estratégias de proteção individual**. JusBrasil, 2021. Disponível em: https://www.jusbrasil.com.br/artigos/enfrentando-o-estelionato-virtual-analise-da-lei-14155-2021-e-estrategias-de-protecao-individual/2167131764. Acesso em: 04 set. 2024.

PINHEIRO, P. **Direito Digital**. Rio de Janeiro: Grupo GEN, 2021. E-book. ISBN 9786555598438. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555598438/. Acesso em: 04 set. 2024.

PORTAL G1. **Crimes virtuais: no auge da pandemia, fraudes cometidas no mundo digital aumentaram 175%**. Disponível em: https://g1.globo.com/profissao-reporter/noticia/2022/07/25/crimes-virtuais-no-auge-da-pandemia-fraudes-cometidas-no-mundo-digital-aumentaram-175percent.ghtml. Acesso em: 09 set. 2024.

ROSA, B. R.; MALIMPENSA, G. T.; CARDOSO, F. E. **Engenharia Social: o que é e como evitar esses ataques nas empresas**. SP, 2023. Trabalho de conclusão de curso. (Curso superior de tecnologia em gestão da Tecnologia da Informação). Faculdade de Tecnologia de Assis, Prof. Dr. José Luiz Guimarães. Assis, 2023. Disponível em: https://ric-cps.eastus2.cloudapp.azure.com/handle/123456789/15845. Acesso em 04. set. 2024.

SANTOS, GLENDA de LOURDES FERREIRA dos. **AUTOMATIC ANSWERS FOR IMPROVEMENT OF THE SECURITY IN DETECTION SYSTEMS OF INTRUDERS.**

2003. 82 f. Dissertação (Mestrado em Engenharia) - Universidade Federal do Maranhão, São Luis, 2003. Disponível em: http://tedebc.ufma.br:8080/jspui/handle/tede/366 Acesso em: 11 Set. 2014

SANTOS, L. R. dos; SOTERO, A. P. da S. **O estelionato virtual e a ineficácia da legislação brasileira para coibir o crime cibernético**. Cuadernos de Educación y Desarrollo, [S. l.], v. 16, n. 8, p. e5183, 2024. DOI: 10.55905/cuadv16n8-081. Disponível em: https://ojs.europubpublications.com/ojs/index.php/ced/article/view/5183. Acesso em: 04 set. 2024.

SILVA, M. A.; CARVALHO, U. R. **Análise sobre as dificuldades de investigação relacionadas aos crimes cibernéticos de estelionato na rede social WhatsApp**. Revista Científica UNIFAGOC, v. 7, n. 2, 2022. Disponível em: https://revista.unifagoc.edu.br/index.php/juridico/article/view/1120. Acesso em: 04 set. 2024.

STEINBERG, J. **Cibersegurança para leigos**. Rio de Janeiro: Editora Alta Books, 2020. E-book. ISBN 9786555204537. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555204537/. Acesso em: 04 set. 2024.