A SOCIEDADE DE RISCO NA ERA DIGITAL: A EXPANSÃO DOS ESTELIONATOS VIRTUAIS E SEUS IMPACTOS NA SOCIEDADE BRASILEIRA

Ana Luiza Mendonça Castro[1]
Yan Silva Carneiro[2]
Cristiane Ingrid de Souza Bonfim[3]

RESUMO

O presente trabalho analisa o crime de estelionato virtual, com foco nas fraudes bancárias, considerando a evolução tecnológica e as vulnerabilidades do ambiente digital. Fundamentado na Teoria da Sociedade de Risco, o estudo demonstra como o avanço tecnológico intensifica incertezas e desafios na segurança cibernética. O objetivo geral é compreender os mecanismos utilizados pelos criminosos, os impactos para as vítimas e o papel do ordenamento jurídico na repressão e prevenção dessas condutas. Os objetivos específicos incluem a identificação das principais estratégias empregadas nas fraudes bancárias digitais, analisando a sofisticação dos métodos utilizados. Além disso, busca-se avaliar os impactos para as vítimas, considerando tanto os prejuízos financeiros quanto os danos psicológicos. Também se examina a evolução das normas penais aplicáveis ao estelionato virtual, com destaque para a Lei n.º 14.155/2021, que trouxe mudanças relevantes na tipificação e punição desses delitos. A pesquisa adota metodologia baseada em estudos doutrinários, legislativos e jurisprudenciais, além da análise de estatísticas sobre o crescimento dos golpes bancários e os desafios enfrentados pelos órgãos de persecução penal. Os resultados indicam que, apesar dos avanços normativos, persistem dificuldades na efetividade das medidas de combate ao estelionato virtual, especialmente devido à transnacionalidade dos crimes e à sofisticação das fraudes. Conclui-se que a repressão penal deve ser complementada por estratégias preventivas, como o aprimoramento da segurança digital e a conscientização dos usuários, aliadas a políticas públicas em parceria com instituições financeiras e autoridades.

PALAVRAS-CHAVE: Estelionato Virtual. Fraudes Bancárias. Sociedade de Risco. Fighting.

INTRODUÇÃO

Este estudo explora o crescente fenômeno do estelionato virtual, com foco específico nas fraudes bancárias, um tipo de crime cada vez mais prevalente no Brasil. O avanço tecnológico e a digitalização da sociedade têm proporcionado uma série de benefícios, mas, ao mesmo tempo, têm dado origem a novas modalidades criminosas, como o estelionato virtual. Tais crimes, caracterizados por sua sofisticação e dificuldade de detecção, representam um desafio significativo para as vítimas e para o sistema de justiça. A relevância dessa temática é notável, pois oferece uma reflexão crítica sobre as causas e consequências desse tipo de crime, além de levantar questões sobre a eficácia das normas jurídicas na **prevenção** e repressão, inclusive para o meio acadêmico. A pesquisa visa, assim, contribuir para o entendimento das

[1] Graduanda em Direito pela Faculdade Evangélica Raízes, Anápolis, Goiás, analuiza.castro23@hotmail.com
[2]Graduando em Direito pela Faculdade Evangélica Raízes, Anápolis, Goiás, yan.ccarneiro@gmail.com. [3]Especialista em Direito Penal e Processo Penal, Mestrado (Universidade Evangélica de Goiás - UniEVANGÉLICA), advogada e professora, Faculdade Evangélica Raízes, Anápolis, Goiás, cristiane.bonfim@docente.faculdaderaizes.edu.br.

vulnerabilidades do ambiente digital, das práticas utilizadas pelos criminosos e das dificuldades enfrentadas pelas autoridades no combate a esse tipo de fraude.

O objetivo principal da pesquisa é analisar o estelionato virtual, com ênfase nas fraudes bancárias, à luz da teoria da sociedade de risco. A proposta é investigar os mecanismos utilizados pelos criminosos, os efeitos desse crime nas vítimas e a resposta do sistema jurídico, procurando compreender as limitações e os avanços da legislação e das políticas públicas no combate a essas práticas ilícitas. Quanto aos objetivos específicos, busca-se, compreender as diferentes formas de estelionato virtual, como phishing e clonagem de dados bancários; analisar a evolução das normas legais relacionadas a esse tipo de crime, destacando os avanços trazidos pela Lei n.º 14.155/2021; e discutir a efetividade das medidas adotadas para prevenir e punir tais fraudes.

A abordagem metodológica adotada neste estudo foi baseada em uma pesquisa que envolveu a análise doutrinária, legislativa e jurisprudencial. A pesquisa procurou examinar a evolução das leis relacionadas ao estelionato, identificar as falhas na implementação de políticas públicas e sugerir possíveis melhorias na resposta institucional a esse tipo de delito.

Para embasar a análise, foram utilizados diversos teóricos, sendo Ulrich Beck um dos principais autores, cujas ideias sobre a sociedade de risco ajudam a compreender como o avanço tecnológico contribui para o surgimento de novas formas de criminalidade no ambiente digital. A revisão da literatura também inclui contribuições de estudiosos das áreas jurídica e de segurança cibernética, que fornecem uma base sólida para a compreensão das implicações legais e sociais do estelionato virtual.

O estudo está organizado em três seções principais. A primeira parte explora a relação entre a sociedade de risco, a digitalização e a evolução tecnológica, destacando as vulnerabilidades do ambiente digital. A segunda seção investiga a ascensão dos crimes cibernéticos, com foco nas práticas fraudulentas, como o estelionato virtual. Por fim, a terceira seção aborda as estratégias de combate ao estelionato virtual, analisando a legislação vigente, as políticas públicas e as inovações tecnológicas aplicadas ao combate a esse crime.

1. A SOCIEDADE DE RISCO NA ERA DIGITAL E A EVOLUÇÃO TECNOLÓGICA: UMA PERSPECTIVA SOCIOLÓGICA E JURÍDICA.

Inicialmente na década de oitenta, o sociólogo alemão Ulrich Beck, desenvolveu a teoria da sociedade de risco, é um conceito que se refere à análise dos perigos e incertezas aos

quais estamos expostos no mundo contemporâneo. Esses riscos afetam todas as pessoas, sejam indivíduos, organizações privadas ou públicas, e são avaliados por meio de ferramentas científicas e tecnológicas. Porém, essas mesmas ferramentas, que deveriam oferecer segurança, estão se mostrando insuficientes diante da complexidade e da magnitude dos desafios que enfrentamos diariamente.

Inicialmente em suas primeiras publicações, a teoria foi analisada sob a ótica ambiental, no contexto da época em que surgiam novos avanços na tecnologia agrícola e analisando o período dos avanços tecnológicos na agricultura que apesar de benéficos, afetariam o meio ambiente e a sociedade, os principais riscos enfrentados pela sociedade moderna são, em grande parte, frutos das próprias ações humanas. Beck (2010, p. 96/97) acrescenta que,

> A urgência dos perigos ambientais descritos, no que diz respeito à vida de plantas, animais e seres humanos, "legitima" os autores, com a boa consciência da moral ecológica, a recorrer a uma linguagem na qual pululam expressões como "controle", "sanção oficial" e "monitoramento governamental". Tipicamente, em função da gravidade dos danos ambientais, são arrogados mecanismos e direitos gradativamente abrangentes de intervenção, planejamento e controle.

Em sua teoria Beck destaca que os avanços tecnológicos, como a industrialização e a globalização, geram novos tipos de riscos que são diferentes daqueles enfrentados no passado, principalmente porque envolvem incertezas e consequências imprevisíveis. Esses riscos, não podem ser totalmente compreendidos ou controlados, e muitas vezes surgem de processos que antes eram considerados seguros ou controláveis, como o uso de tecnologias nucleares, biotecnologia, e o impacto ambiental.

O conceito de ambivalência foi introduzido para descrever esses riscos, indicando que, por um lado, as tecnologias trazem benefícios e avanços, mas, por outro, geram consequências imprevistas e potencialmente perigosas. Em outras palavras, a própria modernização e inovação, em vez de oferecerem segurança, criam novos desafios e ameaças que são difíceis de prever e medir com precisão.

Beck observa que, na sociedade moderna, o conhecimento científico e técnico, que poderia servir como base para decisões informadas, muitas vezes é insuficiente ou não abrange toda a complexidade dos riscos emergentes. Ele enfatiza que esses riscos tendem a ser globais, afetando não apenas uma sociedade específica, mas a humanidade como um todo. Isso torna ainda mais difícil para os indivíduos, governos e organizações tomarem decisões

que levem em conta todas as variáveis possíveis, o que cria um ambiente de incerteza crescente. Beck (2010, p. 94) expõe que,

> Quando os riscos da modernização são "reconhecidos" e isto quer dizer muito, não apenas o conhecimento a respeito deles, mas o conhecimento coletivo a respeito deles, a crença neles e a exposição política das cadeias de causas e efeitos com eles associadas, eles desenvolvem uma dinâmica política sem precedentes.

O avanço tecnológico, embora traga benefícios significativos, também contribui para a criação de novos e mais amplos riscos. Por exemplo, os impactos ambientais decorrentes do uso indiscriminado da tecnologia agrícola, os danos à saúde mental, como ansiedade, depressão, estresse e problemas físicos, como dores crônicas, estão entre as consequências de um mundo cada vez mais digitalizado e acelerado. Além disso, o modelo capitalista exacerbado reforça esse cenário, promove um consumo desenfreado e intensifica as desigualdades sociais. Em sua obra, Lima, (2022, p. 18), descreve que,

> A tecnologia é apenas o resultado da manipulação dos recursos materiais da natureza para atender a necessidades sociais. Na era digital, o ápice da servidão do trabalho ao capital se expressa na exploração sutil no campo virtual e no autocontrole exercido pelo trabalhador, experimentado pela função móvel das tecnologias digitais, de maneira a lhe extrair mais tempo de trabalho e saúde.

Uma das características mais marcantes da sociedade de risco é a crescente preocupação com o futuro e a busca por segurança, que paradoxalmente alimenta ainda mais a percepção de vulnerabilidade. Essa sensação de incerteza, associada tanto aos riscos concretos já existentes quanto aos potenciais, faz com que as pessoas e as instituições vivam em um estado permanente de alerta, moldando comportamentos e decisões em escala global.

Os riscos tecnológicos são diversos e podem surgir de diferentes circunstâncias: acidentes de trânsito, transporte de materiais perigosos, colapso de estruturas, rompimentos de barragens, acidentes industriais, emergências radiológicas, incêndios, ataques hacker, cyber crimes, vazamento de dados entre outros. Esses eventos são reflexos de uma sociedade em constante transformação, que nem sempre prioriza a prevenção e a segurança Diante disso a sociedade contemporânea se vê diante do desafio de lidar com riscos que não são apenas técnicos, mas também sociais, éticos e políticos, exigindo novas formas de governança e gestão de riscos, que reconheçam a limitação do conhecimento e a necessidade de ações preventivas diante de incertezas profundas. “Cabe ao governo e cientistas reformularem o conceito de controle e vigilância, sabendo sempre que nem assim as pessoas que estão no

poder estão em condições de definir ou controlar os riscos de forma racional.” (Beck, 2010, p. 92)

É evidente que nos últimos anos o avanço da tecnologia propiciou a evolução e popularização do uso de smartphones em todo o mundo, trazendo uma infinidade de benefícios e soluções, facilitando a vida proporcionando celeridade para as interações humanas, mensagens que antes levariam semanas para chegar através de um envelope postal hoje cruzam o oceano e o espaço em uma fração de segundos, vão e voltam sem parar, imagens e vídeos são enviados, arte é criada, tudo é registrado.

Um exemplo desse avanço tecnológico, são os bancos, a evolução dos serviços financeiros na era digital cresce a cada dia, bancos 100% digitais são uma realidade hoje em dia, é natural que o crime também tenha evoluído para era digital, foi se a era das fraudes antigas, com falsificação de documentos físicos, cheques sem fundo, golpes de bilhete premiado, pirâmides financeiras e venda de terrenos inexistentes agora as contas podem ser liquidadas e o dinheiro é transferido de qualquer lugar do mundo através de uma pequena tela.

Coincidentemente assim como a tecnologia, a teoria de Beck também evoluiu ao longo do tempo e passou a ser analisada e aplicada em diversas áreas das ciências sociais como sociologia, estudos ambientais, direito, economia, comunicação e tecnologia, o que nos traz até os dias de hoje, a nossa pesquisa buscou analisar a evolução das mídias sociais e dos bancos digitais. Essas evoluções foram benéficas, mas também tiveram um efeito colateral proporcionando o aumento dos crimes cibernéticos, dentre eles o mais notório nos dias de hoje é o crime de estelionato cibernético, popularmente conhecido como estelionato virtual ou fraude virtual, muitas vezes envolvendo instituições financeiras. Segundo Advogados Criminais (2023, p. 5):

> A fraude bancária online é um dos crimes cibernéticos mais recorrentes no Brasil. Esse crime é frequentemente praticado por meio de phishing, técnica em que o criminoso se passa por uma instituição financeira legítima para obter informações pessoais e financeiras da vítima. De posse desses dados, o fraudador pode realizar transações ilícitas na conta bancária da vítima.

Diante da análise que conecta a evolução tecnológica dos serviços financeiros é possível observar o crime de estelionato virtual sob a luz da teoria da sociedade de risco inserida no contexto da sociedade brasileira, houve um avanço tecnológico gigantesco com a invenção dos smartphones e sua popularização que atingiu a sociedade como um todo.

Segundo a Agência Estado (2024):

> Em 2023, 163,8 milhões de pessoas tinham aparelho de telefone celular para uso pessoal no País, o equivalente a 87,6% da população com 10 anos ou mais. Os dados são da Pesquisa Nacional por Amostra de Domicílios Contínua - Tecnologia da Informação e Comunicação 2023, a Pnad TIC, e foram divulgados pelo Instituto Brasileiro de Geografia e Estatística (IBGE) nesta sexta-feira, 16.

Ainda sobre o conceito de ambivalência internet funciona como uma faca de dois gumes, é o exemplo mais claro dessa evolução, ela abre um portal que te dá acesso ao mundo todo, mas em contrapartida o mundo todo tem acesso a você e isso traz uma certa vulnerabilidade. O uso massivo da internet e dos dispositivos móveis conecta indivíduos, mas também potencializa a disseminação de fraudes digitais. O crescimento de plataformas de e-commerce, redes sociais e aplicativos financeiros criou novas oportunidades para criminosos explorarem lacunas de segurança e a falta de conscientização dos usuários. Segundo Nalin (2024), "nove em cada dez brasileiros (92,9%) têm acesso à internet em casa, mostram novos dados da Síntese de Indicadores Sociais, estudo divulgado pelo IBGE nesta quarta-feira".

Portanto, a relação entre os avanços tecnológicos e a amplificação dos riscos contemporâneos, conforme apontado pela teoria da sociedade de risco de Ulrich Beck ao abordar os desdobramentos sociais, econômicos e digitais, evidencia-se a necessidade de analisar criticamente as transformações estruturais geradas pela modernização, com ênfase nos desafios impostos pela incidência crescente de crimes cibernéticos e pela vulnerabilidade das instituições financeiras.

2. A INTERNET E OS RISCOS DIGITAIS: A EVOLUÇÃO DOS CRIMES CIBERNÉTICOS E O IMPACTO DO ESTELIONATO VIRTUAL

A Internet foi criada por um grupo de cientistas em 1969, nos Estados Unidos, com o nome de ARPANET. Em seus primeiros anos foi utiliza para conectar universidades através do envio de e-mails, teve sua primeira demonstração pública em 1972 na International Conference on Computer Communications e em 1973 se expandiu para comunicações internacionais, sendo utilizada pelo governo americano para fins militares e científicos até que em 1983 foi dedicada inteiramente para fins científicos e outra rede foi criada para fins militares.

Foi só em 1987 que a troca de informações entre computadores foi liberada pela primeira vez para uso comercial, até então só era utilizada nos meios acadêmicos americanos, um ano depois em 1988 a internet chegou ao Brasil através de uma parceria entre a FAPESP - Fundação de Amparo à Pesquisa do Estado de São Paulo a UFRJ Universidade Federal do Rio de Janeiro e o LNCC (Laboratório Nacional de Computação Científica). E finalmente no ano de 1994 foi dado início a exploração comercial da internet no Brasil por meio de um projeto da Embratel que permitia o acesso a internet através da linha discada.

Desde então a tecnologia da internet evoluiu e vem evoluindo de formas grandiosas, inimagináveis e com uma velocidade incrível, conforme previu a Lei de Moore o universo digital vem se expandindo e dobra sua capacidade a cada dois anos. Moore (1998, p. 02) afirma:

> A complexidade para componentes com custos mínimos tem aumentado em um fator de dois por ano. Certamente, em um curto prazo, pode-se esperar que esta taxa se mantenha, se não aumentar. A longo prazo, a taxa de aumento é mais incerta, embora não haja razões para acreditar que não se manterá constante por pelo menos dez anos. Isso significa que, em torno de 1975, o número de componentes do circuito integrado para um custo mínimo será de 65.000 (nanômetros). Eu acredito que circuitos grandes como estes poderão ser construídos em um único componente.

A sociedade está cada vez mais imersa na tecnologia e com essa evolução vários aspectos sociais se integraram ao mundo digital, juntamente com esses aspectos os crimes também migraram para o mundo digital dando origem aos crimes cibernéticos, que são estelionato virtual, phishing, clonagem de cartões e dados bancários, falsos empréstimos entre outros, e a partir de tais crimes deu-se início a criação da legislação brasileira sobre crimes cibernéticos através da Lei Carolina Dieckmann, sancionada em 2012, do Marco Civil da Internet, estabelecido em 2014 e Lei nº 14.815/2024, promulgada em 15 de janeiro de 2024 que reconheceu os direitos digitais, trouxe garantias de privacidade e segurança, regulamentou o uso de dados e trouxe algumas medidas de combate aos crimes cibernéticos.

O crime de phishing é uma modalidade de fraude cibernética que busca enganar vítimas por meio da falsificação de identidades digitais, geralmente utilizando e-mails, mensagens ou sites fraudulentos para induzir o usuário a fornecer informações sensíveis, como senhas, dados bancários e números de cartões de crédito. O termo "phishing" deriva da palavra inglesa "fishing" (pescar), em referência à tentativa dos criminosos de "pescar" informações pessoais por meio do engano. No Brasil, esse crime se enquadra no estelionato

virtual, previsto no artigo 171, §2º-A, do Código Penal, que trata especificamente de fraudes eletrônicas.

As fraudes bancárias representam uma das formas mais comuns e prejudiciais do phishing. Os criminosos costumam enviar mensagens falsas em nome de bancos, alegando problemas na conta do usuário ou a necessidade de atualização cadastral. Quando a vítima clica no link fornecido, ela é redirecionada para uma página falsa que simula o site oficial da instituição financeira. Ao inserir suas credenciais, os dados são capturados pelos golpistas, que podem realizar transações indevidas. Um exemplo notório ocorreu em 2022, quando o Banco Central do Brasil alertou sobre golpes de phishing envolvendo o sistema de pagamentos instantâneos "pix", nos quais os criminosos criavam sites falsos prometendo bônus e recompensas para induzir os usuários a compartilhar suas informações bancárias.

A sofisticação dos golpes de phishing tem crescido com o avanço da tecnologia. Além de e-mails fraudulentos, os criminosos utilizam mensagens em aplicativos como WhatsApp e SMS, fingindo serem instituições bancárias. Muitos desses ataques exploram a engenharia social, manipulando o medo ou a urgência da vítima para que ela tome decisões precipitadas. Conforme apontado pelo especialista em segurança digital Kevin Mitnick (2002), os hackers mais bem-sucedidos não necessitam invadir sistemas complexos quando podem ludibriar uma pessoa para que lhes entregue as chaves.

Assim, a conscientização e a adoção de boas práticas de segurança digital, como a verificação de remetentes e o uso de autenticação em dois fatores, são medidas essenciais para evitar esse tipo de crime.

Nesse contexto, com o avanço acelerado da era digital, os crimes também migraram para o ambiente virtual, aproveitando-se das facilidades proporcionadas pela internet. Entre inúmeros delitos praticados nos ambientes virtuais, está o estelionato, um crime conhecido por envolver a indução da vítima em erro para obtenção de vantagem ilícita.

Conforme estabelece o artigo 171 do Código Penal, é crime "obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante planejamento, ardil, ou qualquer outro meio fraudulento" (Brasil, 1940). Assim, a legislação prevê pena de reclusão de 1 (um) a 5 (cinco) anos, além de multa, para quem cometer este tipo de fraude.

Uma importante mudança ocorreu com a Lei nº 14.155/2021, que alterou o artigo 171 do Código Penal para agravar as penas de crimes de estelionato cometidos pela internet,

especialmente quando envolvem fraudes bancárias. Essa alteração representou um avanço na tentativa de coibir os golpes virtuais, mas ainda há desafios na aplicação da lei, principalmente devido à dificuldade em rastrear os criminosos, que frequentemente operam a partir de locais remotos e utilizam métodos sofisticados para ocultar sua identidade.

O crime de estelionato pode ser identificado desde o Direito Romano, no qual já se penalizava condutas fraudulentas voltadas à obtenção indevida de bens ou vantagens. Antes das inovações da tecnologia, os golpes eram aplicados de forma presencial, por meio de falsificações, promessas enganosas e manipulações, com o decurso do tempo, essa infração foi se adaptando às transformações sociais e tecnológicas, a era digital trouxe novas oportunidades para os criminosos, tornando as fraudes mais sofisticadas e de difícil identificação. Nesse contexto, Bitencourt (2019, p.103) esclarece:

> No estelionato, há dupla relação causal: primeiro, a vítima é enganada mediante fraude, sendo está a causa e o engano o efeito; segundo nova relação causal entre o erro, como causa, e a obtenção de vantagem ilícita e o respectivo prejuízo, como efeito. Na verdade, é indispensável que a vantagem obtida, além de ilícita, decorra do erro produzido pelo agente, isto é, que aquela seja consequência desta. Não basta a existência do erro decorrente da fraude, sendo necessário que da ação resulte vantagem ilícita e prejuízo patrimonial. Ademais, à vantagem ilícita deve corresponder um prejuízo alheio.

Dessa forma, não há necessariamente um perfil específico para vítimas ou fraudadores. Qualquer pessoa pode ser alvo, assim como qualquer pessoa pode praticar a fraude, desde que haja a intenção de induzir alguém ao erro para obter vantagem indevida, com o consequente prejuízo para a vítima.

Com a digitalização das interações sociais e do setor financeiro, as instituições bancárias foram significativamente impactadas pelo avanço tecnológico, proporcionando maior comodidade aos clientes. Entretanto, essa modernização também gerou novas vulnerabilidades exploradas por criminosos. Bitencourt (2019, p. 519) destaca que, “dependendo da finalidade da denunciação, a conduta pode configurar outra infração penal, como, por exemplo, alegar falsamente ter sido vítima de furto para justificar o recebimento do seguro, caracterizando uma modalidade de estelionato (art. 171, § 2º, V, do Código Penal)”.

Dentre diversas formas de fraudes existentes, uma das mais comuns no ambiente digital é o Phishing, que é uma técnica usada para enganar usuários e obter dados bancários por meio de diferentes meios, como mensagens, sites falsos que simulam diretamente às instituições financeiras. Sobre a segurança das transações eletrônicas, Nakamura (2007, p. 22)

observa:

> A transação eletrônica segura, utilizada no comércio eletrônico, faz com que as lojas virtuais não tenham acesso ao número do cartão de crédito, o que poderia ser aproveitado para uma base de dados de seus clientes. Essa, na realidade, é uma característica importante para a segurança, pois o maior perigo dos incidentes envolvendo cartões de crédito está relacionado ao seu armazenamento.

Os bancos passaram a oferecer serviços de forma online, permitindo que seus clientes realizem transações bancárias sem a necessidade de deslocamento até uma agência física. Com a ascensão dos bancos digitais, que operam exclusivamente via aplicativos, essa realidade se consolidou ainda mais. No entanto, a facilidade no acesso a esses serviços também elevou a vulnerabilidade dos usuários a golpes financeiros, tornando-os alvos fáceis para criminosos que exploram falhas na segurança e a falta de conhecimento digital das vítimas. Muitas vezes, o crime só é percebido quando a vítima recebe notificações ou e-mails sobre compras que não realizou.

Dessa maneira, torna-se evidente que, embora a evolução da internet tenha trazido benefícios inegáveis, também impôs desafios relacionados à segurança das informações e proteção dos dados financeiros. O estelionato virtual, especialmente no setor bancário, representa um dos maiores desafios do direito penal contemporâneo, exigindo ações integradas entre o estado, as empresas e os usuários para minimizar os riscos e responsabilizar os infratores. “Justamente com a ampliação dos perigos surgem na sociedade de risco desafios inteiramente novos à democracia”. **(**Beck, 2010, p. 97)**.**

Atualmente, grande parte das transações financeiras ocorre no ambiente digital, e essa modernização ampliou os ataques para fraudes financeiras, com o aumento significativo de casos de estelionato virtual no Brasil. O Banco Central do Brasil, por exemplo, tem incentivado a inovação no setor financeiro por meio da criação do Sistema de Pagamentos Instantâneos (PIX) e a regulamentação do Open Banking, que é o compartilhamento de dados entre instituições financeiras.

A ausência da necessidade de locomoção para realização de transações, bem como a redução do contato físico com agências bancárias, aumentou a exposição dos usuários a golpes. Os criminosos exploram tanto falhas nos sistemas de segurança quanto a desinformação dos usuários sobre práticas seguras no ambiente digital.

O cenário atual demonstra que, embora a digitalização tenha facilitado a vida dos

usuários, ela também trouxe novos desafios que exigem uma adaptação constante das instituições financeiras e do sistema jurídico. O combate ao estelionato virtual depende não apenas do fortalecimento das medidas de segurança, mas também da atuação do Poder Público na regulamentação e punição eficaz dos crimes cibernéticos.

Segundo o Anuário Brasileiro de Segurança Pública de 2024, os crimes de fraudes digitais cresceram significativamente, com destaque para os golpes financeiros praticados por aplicativos. O estudo revelou que os casos de estelionato, em geral, e os realizados por meios virtuais aumentaram consideravelmente. Entre 2022 e 2023, os estelionatos virtuais registraram um crescimento de aproximadamente 13,6%, enquanto o total de estelionatos subiu 8,2%.

A migração dos bancos para o ambiente digital representa um marco na modernização do setor financeiro, mas também reforça a necessidade de um aprimoramento contínuo das estratégias de prevenção a fraudes. A evolução do crime cibernético segue o ritmo do avanço tecnológico, tornando essencial que bancos, consumidores e autoridades trabalhem juntos para minimizar os impactos do estelionato virtual e garantir a segurança das transações digitais.

Diante desse cenário, observa-se que o combate ao estelionato virtual requer medidas preventivas mais eficazes, regulamentações adequadas e a conscientização dos usuários sobre segurança digital. A atuação conjunta entre órgãos reguladores, instituições financeiras e a população é essencial para minimizar os impactos desse tipo de crime e garantir maior proteção no ambiente digital.

3. APLACANDO A EXPANSÃO DO ESTELIONATO VIRTUAL: SOLUÇÕES TECNOLÓGICAS, POLÍTICAS PÚBLICAS E LEGISLAÇÃO.

Indubitavelmente a crescente digitalização dos serviços financeiros e a evolução dos crimes cibernéticos expuseram um novo cenário de insegurança para a sociedade. O estelionato virtual, principalmente na modalidade de phishing, conforme discutido nas seções anteriores, se consolidou como um dos crimes mais recorrentes no meio digital, colocando em risco a integridade financeira de indivíduos e empresas. Além dos prejuízos econômicos, esse tipo de delito impacta diretamente a confiança da população no uso de plataformas digitais, aumentando o sentimento de vulnerabilidade e exigindo respostas mais efetivas tanto do setor privado quanto do Estado.

A digitalização trouxe inúmeras facilidades para o cotidiano das pessoas, mas também gerou novas preocupações quanto à segurança dos dados e expôs a sociedade ao risco de fraudes financeiras. O aumento dos casos de estelionato virtual fez com que muitos usuários adotassem uma postura mais receosa ao utilizar serviços digitais, o que, paradoxalmente, pode retardar o avanço tecnológico e prejudicar a inclusão digital.

De acordo com o Relatório de Segurança Digital da FEBRABAN (2023), aproximadamente 40% dos brasileiros já foram vítimas de golpes digitais ou conheceram alguém que passou por essa experiência. Esse dado reflete o risco crescente que a internet representa para transações financeiras, levando muitas pessoas a evitar serviços bancários online, compras digitais e o uso de sistemas de pagamento instantâneos, como o PIX.

Além das perdas econômicas individuais, o estelionato virtual contribui para o enfraquecimento da confiança no sistema financeiro digital e pode gerar um retrocesso na adesão às inovações tecnológicas, impactando a economia e o avanço da digitalização no país. A confiança no sistema financeiro digital tem apresentado sinais de enfraquecimento nos últimos anos. Tales (2025) revela que:

> O Índice de Confiança Digital do grupo Thales de 2025 revelou um declínio universal na confiança dos serviços digitais em comparação com o ano anterior. O setor bancário, embora ainda seja o mais confiável, viu a confiança cair para apenas 32% entre os clientes da Geração Z. Além disso, 82% dos consumidores abandonaram uma marca nos últimos 12 meses devido a preocupações sobre o uso de seus dados pessoais

A incidência crescente do crime de estelionato virtual e a sofisticação das fraudes digitais impõem desafios complexos à segurança cibernética, exigindo respostas rápidas e eficazes por parte do Estado, das instituições financeiras e da sociedade como um todo. Para conter essa ameaça crescente, faz-se necessária uma abordagem multifacetada, que contemple inovações tecnológicas, políticas públicas eficientes e aprimoramento legislativo. A presente seção aborda as principais estratégias para mitigar a ocorrência desses crimes, promovendo um ambiente digital mais seguro e confiável.

A tecnologia age como uma faca de dois gumes sendo ao mesmo tempo o veneno e o antídoto pois tem desempenhado um papel central no combate às fraudes bancárias e demais modalidades de estelionato virtual. As instituições financeiras e empresas de tecnologia vêm investindo em soluções cada vez mais sofisticadas para minimizar vulnerabilidades e aprimorar a segurança dos usuários. Febraban (2024, p. 19) destaca que: “no último ano,

houve aumento de 89% na quantidade média de profissionais terceirizados em segurança cibernética e, para 2024, a expectativa de 25% dos bancos é de aumentar a quantidade de profissionais desta área".

No entanto, à medida que novas barreiras são criadas, criminosos se reinventam, desenvolvendo métodos mais avançados para burlar sistemas de proteção. O método tradicional de autenticação, baseado apenas em login e senha, já não é suficiente para garantir a segurança das transações digitais. O uso de autenticação multifatorial, que combina diferentes camadas de verificação, tem se mostrado uma solução eficaz contra invasões de contas bancárias e fraudes em plataformas financeiras. A implementação de autenticação biométrica, reconhecimento facial, envio de códigos temporários e dispositivos de segurança físicos pode dificultar significativamente a ação de criminosos, protegendo os dados dos usuários.

Ademais, a criptografia de ponta a ponta tornou-se um dos pilares da segurança digital, garantindo que informações bancárias e transações financeiras permaneçam protegidas contra interceptação por terceiros. Além disso, protocolos como HTTPS e TLS (Transport Layer Security) são essenciais para proteger a comunicação entre usuários e instituições financeiras, impedindo ataques de interceptação e manipulação de dados.

A tecnologia Blockchain tem sido explorada como uma alternativa promissora para aumentar a transparência e a segurança em transações financeiras. A descentralização desse sistema reduz as chances de adulteração de dados e fraudes bancárias, proporcionando maior confiabilidade aos usuários. Já a tokenização tem sido aplicada na substituição de dados sensíveis por identificadores criptografados, minimizando o risco de exposição indevida de informações bancárias.

Atualmente o Banco Central está desenvolvendo uma nova moeda Digital o DREX (Digital Real X), sendo a representação do real em uma plataforma digital a nova moeda promete transformar por completo o mercado financeiro, e já está sendo utilizado por algumas instituições para fins de teste sua capacidade de transformação é equiparável a do Pix, conforme aponta a pesquisa FEBRABAN de Tecnologia Bancária 2024 - Vol. 1 que ao falar da transparência e segurança das instituições trouxe dados sobre a convergência entre Blockchain e DREX. Febraban (2024, p. 27) menciona que:

> Ao utilizar a tecnologia Blockchain para registrar e verificar transações, as instituições financeiras podem garantir a integridade dos dados e a proteção dos processos. Aproximadamente 42% dos bancos entrevistados destacaram o impacto

do DREX na transparência e segurança das operações.

Outra estratégia eficaz adotada por bancos e instituições financeiras é a criação de mecanismos que limitam transações suspeitas, com base em históricos de movimentação do usuário. Dessa forma, pagamentos fora do padrão usual podem ser automaticamente bloqueados ou submetidos a novas etapas de verificação antes da conclusão.

A implementação dessas soluções tecnológicas, aliada à conscientização dos usuários, pode reduzir consideravelmente o impacto do estelionato virtual, dificultando a ação dos criminosos e fortalecendo a confiança no ambiente digital.

Apesar dos avanços tecnológicos, a segurança digital não depende apenas de inovações em sistemas de proteção, mas também da conscientização da população e da criação de políticas públicas eficazes. O desconhecimento sobre práticas básicas de segurança na internet ainda é um fator determinante para o sucesso de golpes digitais, tornando indispensável o investimento em educação digital. Nascimento (2024, p. 10) afirma que:

> A educação digital desempenha um papel fundamental na conscientização sobre os direitos e deveres no contexto digital. Os estudantes devem ser orientados sobre os riscos e desafios presentes na internet e capacitados para tomar decisões controladas. Isso envolve a formação de habilidades críticas para avaliar a segurança das fontes de informação, a capacidade de proteger sua privacidade e a compreensão dos limites éticos no uso das tecnologias digitais.

Governos e instituições financeiras devem investir na promoção de campanhas educativas permanentes, alertando sobre as principais táticas utilizadas por criminosos digitais e ensinando boas práticas de segurança. Essas campanhas podem ser veiculadas em meios de comunicação de massa, redes sociais e canais oficiais de bancos, ampliando seu alcance e impacto.

Além disso, programas de inclusão digital são essenciais para capacitar populações mais vulneráveis a reconhecerem golpes e se protegerem de fraudes. Idosos e pessoas com menor acesso à informação frequentemente são vítimas de estelionatários, o que reforça a necessidade de iniciativas voltadas para esse público. Nesse sentido, Volpini (2022) afirma que "o ciberespaço é traiçoeiro. Por isso, é importante que o cliente esteja atento, como se estivesse na rua. A melhor maneira de combater esses engenheiros sociais é que o usuário reconheça as atitudes e os contatos suspeitos, e isso só é possível por meio da educação digital."

A segurança digital deveria ser um tema abordado desde os primeiros anos da educação formal. A inclusão de conteúdos sobre proteção de dados, privacidade e riscos cibernéticos nos currículos escolares e universitários ajudaria a criar uma cultura preventiva contra fraudes, preparando as futuras gerações para um uso mais seguro da internet.

A ampliação do número de delegacias especializadas em crimes cibernéticos e o investimento em capacitação para agentes de segurança pública são medidas fundamentais para aumentar a eficácia da investigação e repressão ao estelionato virtual. Além disso, a criação de parcerias entre órgãos governamentais e empresas de tecnologia pode facilitar a troca de informações sobre fraudes e aprimorar os mecanismos de rastreamento de criminosos.

A Lei nº 14.155/2021, que alterou o artigo 171 do Código Penal, endurece as penas para o estelionato virtual, mas sua aplicação ainda enfrenta obstáculos práticos. Uma das dificuldades reside na identificação dos autores do crime, que frequentemente operam sob anonimato e utilizam redes internacionais para dificultar sua localização.

Para superar esse problema, especialistas defendem a criação de mecanismos mais ágeis para rastreamento de transações fraudulentas, além de acordos de cooperação entre bancos e autoridades policiais para facilitar a recuperação de valores desviados.

O caráter global dos crimes cibernéticos exige uma abordagem que transcende fronteiras. Muitos golpes virtuais são operados a partir de outros países, dificultando sua repressão pelas autoridades locais. Nesse sentido, a adesão do Brasil à Convenção de Budapeste sobre crime cibernético através do decreto 11.491, de 12/04/23h, pode fortalecer a cooperação internacional na investigação e punição de criminosos que atuam no meio digital.

Além do fortalecimento de parcerias internacionais, outro passo importante na mitigação das fraudes bancárias seria a imposição de sanções administrativas e multas com a finalidade de incentivar essas instituições a investirem em tecnologias mais eficazes contra fraudes. Empresas que oferecem serviços financeiros digitais devem ser responsabilizadas caso falhem em adotar medidas adequadas de segurança.

O combate ao estelionato virtual exige um esforço conjunto entre sociedade, instituições financeiras, órgãos governamentais, legisladores e educadores. A combinação de medidas tecnológicas avançadas, políticas públicas voltadas à educação digital e aprimoramento legislativo pode garantir maior segurança ao ambiente digital, protegendo usuários e reduzindo a impunidade dos criminosos.

Assim, somente por meio da integração dessas estratégias será possível não só conter a expansão dos golpes cibernéticos, mas até mesmo de superar as fraudes bancárias e fortalecer a confiança da população no uso das plataformas digitais, pavimentando o caminho a uma sociedade digital saudável e livre de riscos financeiros.

CONCLUSÃO

Por tudo quanto foi exposto, ressalta-se a relevância da teoria da sociedade de risco de Ulrich Beck no entendimento dos crimes cibernéticos, com especial enfoque no estelionato virtual. A pesquisa evidenciou como a digitalização, embora tenha trazido inovações e benefícios significativos para a sociedade, também criou novas vulnerabilidades que são exploradas por criminosos. A internet, enquanto um meio poderoso de comunicação e acesso à informação, também se apresenta como um ambiente propício para a realização de crimes, cujos impactos são tanto financeiros quanto emocionais para as vítimas.

A evolução do estelionato, desde suas formas tradicionais até as sofisticadas modalidades virtuais, foi amplamente discutida ao longo deste estudo. As fraudes bancárias online, o phishing e outras formas de estelionato virtual se tornaram mais complexas, tornando-se difíceis de detectar e, consequentemente, mais perigosas para os indivíduos e para a economia como um todo. A transição do estelionato tradicional para o virtual está intimamente ligada ao avanço da tecnologia, que ampliou as formas de fraudar e explorar vulnerabilidades, além da falta de conscientização dos usuários sobre os riscos do ambiente digital. Este panorama coloca a sociedade diante de novos desafios, não apenas no âmbito criminal, mas também na adaptação do sistema jurídico a essas novas formas de delito.

A legislação brasileira tem buscado acompanhar essa evolução, com destaque para a Lei nº 14.155/2021, que ampliou e agravou as penas para os crimes de estelionato cometidos por meios eletrônicos. No entanto, apesar dos avanços legais, o sistema penal ainda enfrenta obstáculos significativos na identificação e punição de criminosos que operam frequentemente de maneira transnacional. Muitos desses infratores utilizam recursos para ocultar suas identidades, dificultando a atuação das autoridades competentes. Além disso, as medidas preventivas ainda são insuficientes em termos de conscientização pública, o que aumenta a vulnerabilidade da população frente aos golpes virtuais.

A pesquisa também abordou as estratégias de combate ao estelionato virtual, tanto do

ponto de vista das soluções tecnológicas quanto das políticas públicas e aprimoramento legislativo. As instituições financeiras e empresas de tecnologia têm investido em sistemas de segurança mais robustos, como autenticação multifatorial e criptografia, visando proteger os dados e as transações dos usuários. No entanto, a eficácia dessas medidas depende diretamente da educação digital e da conscientização da população, que precisa entender como se proteger no ambiente virtual. Sem a colaboração ativa dos cidadãos e a adoção de boas práticas de segurança, qualquer sistema de segurança digital, por mais avançado que seja, torna-se vulnerável.

Nesse contexto, o papel do Estado também é fundamental. A criação de políticas públicas que incentivem a segurança digital e a atualização constante da legislação são passos essenciais para enfrentar as novas modalidades de crimes cibernéticos. Além disso, a cooperação entre os diversos atores sociais, como órgãos reguladores, instituições financeiras, empresas de tecnologia, sociedade civil e poder público, é crucial para criar uma rede de proteção mais eficaz contra o estelionato virtual.

Em última análise, a conclusão deste trabalho reforça a importância de uma abordagem conjunta e coordenada no combate ao estelionato virtual. A conscientização e a educação digital da população, o desenvolvimento de soluções tecnológicas eficazes, e a evolução da legislação são componentes essenciais para criar um ambiente digital mais seguro e confiável. O estudo destaca que a prevenção e repressão ao estelionato virtual exigem não apenas mudanças no campo jurídico, mas também uma transformação cultural, onde todos os atores da sociedade desempenham um papel ativo na construção de um ambiente digital mais seguro para todos. O esforço coletivo e coordenado é a chave para enfrentar esse desafio crescente de forma eficaz.

REFERÊNCIAS

Advogados Criminais. **Crimes cibernéticos no Brasil: guia completo sobre tipos, penas e agravantes.** JusBrasil, 2023. Disponível em: https://jus.com.br/artigos/105875/crimes-ciberneticos-no-brasil-guia-completo-sobre-tipos-penas-e-agravantes>. Acesso em: 11 dez. 2024.

Agência Estado. **IBGE revela que o Brasil tem 163,8 milhões de pessoas com aparelho de telefone celular**. O Povo, 2024. Disponível em: <https://www.opovo.com.br/noticias/economia/2024/08/16/ibge-revela-que-brasil-tem-1638-milhoes-de-pessoas-com-aparelho-de-telefone-celular.html>. Acesso em: 12 nov. 2024.

Beck, Ulrich. **Sociedade de risco: rumo a uma outra modernidade.** São Paulo: Editora Unesp, 2010.

Berticelli, Caroline. **Como Surgiu a Internet No Brasil, No Mundo E Quem Inventou.** Ninho Digital, 9 May 2022, ninho.digital/como-surgiu-a-internet/. Accessed 18 Mar. 2025.

Bitencourt, Cezar Roberto. **Tratado de direito penal: parte especial 19**. ed. São Paulo: Saraiva, 2019.

Brasil. Código Penal. **Decreto-lei nº 2.848, de 7 de dezembro de 1940**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848.htm>. Acesso em: 11 dez. 2024.

Brasil. Lei nº 12.965, de 23 de abril de 2014. **Marco Civil da Internet**. Brasília, DF: Diário Oficial da União, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 11 jul. 2024.

Brasil. Lei nº 14.155, de 27 de maio de 2021. **Altera o Decreto-Lei nº 2.848**. Brasília, DF: Diário Oficial da União, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/Ato2019-2022/2021/Lei/L14155.htm. Acesso em 18 mar. 2025.

Escola, Brasil. **Internet no Brasil; Brasil Escola.** Disponível em: https://brasilescola.uol.com.br/informatica/internet-no-brasil.htm. Acesso em 18 de março de 2025.

Febraban. **Pesquisa de Tecnologia Bancária 2024**. Vol. 1. São Paulo: FEBRABAN, 2024.

Febraban. **Relatório de Segurança Digital**. 2023. Disponível em: <https://www.febraban.org.br>. Acesso em: 11 dez. 2024.

Febraban. **Tech 2024**, [S. l.], p. 1, 25 jul. 2024. Disponível em: <https://febrabantech.com/noticias/bancos-reforcam-estrategias-para-reduzir-riscos-ciberneticos>. Acesso em: 25 mar. 2025.

Lima, Monica Silva de. **A tecnologia é apenas o resultado da manipulação dos recursos materiais da natureza para atender a necessidades sociais**. Revista Brasileira de Tecnologia e Sociedade, p. 18, 2022.

Mitnick, Kevin. **A arte de enganar: como os hackers, trapaceiros e espiões roubam sua informação e identidade**. Rio de Janeiro: 2002.

Moore, Gordon E. **Cramming more components into integrated circuits**. Proceedings of the IEEE. v. 86, n. 1, p. 2, jan. 1998.

Nakamura, E. T.; Geus, P. L. **Segurança de Redes em Ambientes Cooperativos. 1ª**

Nalin, Carolina N. **Nove em cada dez brasileiros têm acesso à internet em casa, com avanço entre os mais pobres**. O Globo, Rio de Janeiro, 4 dez. 2024. Disponível em: <https://oglobo.globo.com/economia/noticia/2024/12/04/nove-em-cada-dez-brasileiros-tem-acesso-a-internet-em-casa-com-avanco-entre-os-mais-pobres.ghtml>. Acesso em: 11 dez. 2024.

Nascimento, Edinardo. **Educação digital: riscos e desafios nas instituições escolares**. Revista Tópicos, v. 10, 2024. ISSN: 2965-6672.

Nic.br. **Na Mídia - A História Da Internet E Suas Tecnologias – Da Guerra Fria a 2024.** NIC.br - Núcleo de Informação E Coordenação Do Ponto BR, 2024, <nic.br/noticia/na-midia/a-historia-da-internet-e-suas-tecnologias-da-guerra-fria-a-2024> acesso em 17 mar 2025.

Tales. **Índice de confiança digital do consumidor de 2025**. Disponível em: <https://www.thalesgroup.com>. Acesso em: 25 mar. 2025.

Volpini, Adriano. **Bancos reforçam estratégias para reduzir riscos cibernéticos**. Disponível em:<https://www.veeam.com>. Acesso em: 22 mar. 2025.