Periódicos Brasil. Pesquisa Científica ISSN 2674-9432

CIBERCRIMES NO BRASIL: ANÁLISE DO ESTELIONATO VIRTUAL E SUAS IMPLICAÇÕES JURÍDICAS

Adriana Abreu de Sá, Rebeca Tárcia da Costa, Gabryella Cunha Nascimento Silva, Francisco Vidal Negreiro

REVISÃO

RESUMO

O artigo discutiu o avanço dos crimes cibernéticos no Brasil, com foco no estelionato virtual. Esse crime consiste em fraudes realizadas no ambiente digital, com o objetivo de enganar vítimas para obtenção de vantagens ilícitas. O texto apresenta o conceito de estelionato virtual, diferenciando-o do estelionato tradicional, e descreve os métodos mais comuns, como o uso de redes sociais, e-mails fraudulentos e aplicativos de mensagens. Destaca-se o aumento significativo desses crimes no Brasil, impulsionado pela ampliação do uso de tecnologias digitais e do comércio eletrônico. No âmbito jurídico, o artigo examina a legislação brasileira aplicável, com destaque para a Lei 14.155/2021, que endureceu as penas para fraudes eletrônicas, e aponta os desafios enfrentados pelas autoridades na investigação e punição desses delitos. Além disso, analisa os impactos sociais, econômicos e psicológicos dessas práticas, que afetam tanto indivíduos quanto empresas. Por fim, o artigo propõe soluções como o investimento em cibersegurança, campanhas de conscientização pública e o aprimoramento das ferramentas de investigação digital. Conclui-se que o enfrentamento do estelionato virtual requer uma abordagem colaborativa entre governo, empresas e cidadãos, com o objetivo de reforçar a segurança no ambiente digital brasileiro
.

Palavras-chave: Cibercrimes. Estelionato Virtual. Direito Brasileiro.

CYBERCRIMES IN BRAZIL: ANALYSIS OF VIRTUAL FRAUD AND ITS LEGAL IMPLICATIONS

ABSTRACT

The article discussed the increase in cybercrimes in Brazil, with a focus on virtual fraud. This crime consists of frauds carried out in the digital environment, with the aim of deceiving victims in order to obtain illicit advantages. The text presents the concept of virtual fraud, differentiating it from traditional fraud, and describes the most common methods, such as the use of social networks, fraudulent emails, and messaging applications. It highlights the significant increase in these crimes in Brazil, driven by the increased use of digital technologies and e-commerce. In the legal sphere, the article examines the applicable Brazilian legislation, with emphasis on Law 14.155/2021, which toughened penalties for electronic fraud, and highlights the challenges faced by authorities in investigating and punishing these crimes. In addition, it analyzes the social, economic, and psychological impacts of these practices, which affect both individuals and companies. Finally, the article proposes solutions such as investment in cybersecurity, public awareness campaigns, and the improvement of digital investigation tools. It is concluded that tackling virtual fraud requires a collaborative approach between government, companies and citizens, with the aim of reinforcing security in the Brazilian digital environment.

Keywords: Cybercrimes. Virtual Fraud. Brazilian Law.

Dados da publicação: Artigo publicado em Junho de 2025

DOI: https://doi.org/10.36557/pbpc.v4i1.336

1 INTRODUÇÃO

A pesquisa aborda o tema dos cibercrimes, com foco no estelionato virtual no contexto do Direito brasileiro, analisando os fatores associados à prática desse crime, investigando os crimes cibernéticos no Brasil e compreendendo o estelionato conforme previsto no ordenamento jurídico nacional. O estudo também explora o surgimento do estelionato virtual e as formas de punição aplicáveis, destacando a relevância da Lei nº 14.155/2021, que aumentou as penas para crimes cometidos por meios digitais.

Com o avanço das tecnologias digitais e a crescente dependência da internet nas transações cotidianas, novos desafios surgem para o Direito, especialmente diante da criminalidade cibernética. O estelionato virtual, caracterizado pelo uso de meios digitais para enganar e causar prejuízo financeiro às vítimas, tem ganhado destaque por seu impacto econômico e social. A facilidade de atuação anônima e sem barreiras territoriais torna esse crime de difícil controle, exigindo do sistema jurídico brasileiro constante adequação às novas realidades tecnológicas.

Nesse contexto, a pesquisa levanta como problema central a questão: Quais são as medidas preventivas direcionadas às vítimas de estelionato virtual que podem contribuir para a redução e inibição desse tipo de crime? Assim, busca-se avaliar a evolução legislativa e a eficácia das normas vigentes, analisando os desafios enfrentados pelo sistema judiciário para garantir a prevenção e repressão do estelionato virtual.

A metodologia adotada é de natureza bibliográfica, com base em estudos científicos, doutrina e legislação. O trabalho também reflete sobre a necessidade de cooperação internacional, revisão constante das leis e implementação de políticas preventivas que promovam maior proteção aos usuários e mais eficiência na aplicação da justiça. Dessa forma, pretende-se contribuir para o debate jurídico sobre cibercrimes e oferecer subsídios para o desenvolvimento de estratégias eficazes contra o estelionato virtual.

2 CRIMES CIBERNÉTICOS

Os crimes cibernéticos, também conhecidos como cibercrimes, referem-se a delitos cometidos no ambiente virtual, utilizando dispositivos conectados à internet. Esse tipo de

criminalidade abrange uma ampla gama de ações ilícitas, desde invasões de sistemas e roubo de dados até fraudes financeiras e disseminação de conteúdos ilegais. Com o crescimento exponencial do uso das tecnologias digitais e a dependência da internet para atividades cotidianas, os cibercrimes tornaram-se um problema global, desafiando legislações e sistemas de segurança em todo o mundo.

No Brasil, os cibercrimes estão tipificados em leis específicas, como o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que criminaliza a invasão de dispositivos informáticos. Além disso, outros crimes do Código Penal Brasileiro, como estelionato (art. 171), foram adaptados para contemplar modalidades digitais, especialmente após a promulgação da Lei nº 14.155/2021, que agravou penas para crimes cometidos pela internet.

A principal característica dos cibercrimes é a utilização de tecnologias avançadas para cometer delitos de maneira anônima e, muitas vezes, transnacional. Isso dificulta a identificação dos autores e a aplicação das penalidades, exigindo cooperação entre diferentes países e um constante aprimoramento dos mecanismos de investigação. Entre os crimes cibernéticos mais comuns estão o estelionato virtual, o roubo de identidade, ataques de ransomware, phishing, hacking de contas bancárias e a exploração sexual online. A prevenção e o combate a esses crimes demandam não apenas leis atualizadas, mas também investimentos em segurança digital, conscientização da população e capacitação das autoridades responsáveis pela investigação e punição dos infratores.

Nesse cenário, os crimes cibernéticos representam um grande desafio para o Direito e a segurança pública, demandando soluções integradas e inovadoras que garantam a proteção dos usuários e a eficácia no enfrentamento dessa modalidade de criminalidade. Com o avanço da tecnologia, a internet se tornou uma importante ferramenta no mundo globalizado, pois tem se mostrado como um importante instrumento na relação entre as pessoas e comércio assim como na transmissão de informações. Contudo, a internet, juntamente com os benefícios, traz em mesma proporção uma quantidade infinita de ilícitos, que vêm aumentando assustadoramente (Santos *et. al.,* 2017, p. 73). Desse modo, apesar da internet ser uma ferramenta de integração global, proporcionando o relacionamento de

pessoas independente da distância, acaba por dar margem ao cometimento de vários delitos.

Nesse contexto, destaca-se que as pessoas perderam parcialmente sua privacidade, ficando sujeita a riscos decorrentes da exposição excessiva, ou até mesmo de danos a sua moral, embora seja inegável os pontos benéficos, como a integração cibernética, o armazenamento e coordenação de dados e a facilitação de atividades e processos. Assim, tem se demonstrado também como um meio para o cometimento de delitos informáticos, visto que serve de instrumento para a prática delitiva (Spinieli, 2018, p. 24).

Faz-se necessário assim, esclarecer a definição de crimes cibernéticos, a qual se configura como ampla, pois, abrange uma variedade de condutas delitivas praticadas por meio da utilização de tecnologias da informação e comunicação. Os crimes cibernéticos são condutas delitivas que ocorrem por meio do uso de tecnologias de informação e comunicação, onde o meio digital é utilizado como instrumento para a prática de infrações penais. Esses delitos são cometidos de maneira virtual, envolvendo a utilização de dispositivos eletrônicos e a internet para a realização de atividades ilegais. Com o avanço tecnológico e a ampla adoção da internet em diversas esferas da sociedade, os crimes cibernéticos se tornaram uma preocupação global. (Almeida, 2018, p. 97).

A investigação dos crimes virtuais é feita através de uma análise técnica, que permite verificar a autoria e materialidade dos crimes praticados por meio de uma rede que interliga os computadores (Wendt, 2017).

Com o avanço da tecnologia e assim a utilização da internet pela população, o cometimento de crimes virtuais tem crescido nos últimos anos, ocasionando assim, a criação de delegacias especializadas a investigar determinados crimes, porém, se no local em que ocorreu o crime virtual não tiver uma Delegacia Especializada, poderá ser registrado um boletim na delegacia mais próxima da residência da vítima.

Isso porque as provas devem ser colhidas por profissionais especializados, assim como um perito capacitado, pois demanda tempo, pela complexidade dos procedimentos.

De acordo com Regis (2011, p. 13):

> Além da coleta de provas é necessário também se chegar até ao autor do delito, e para se chegar até ele existe um caminho onde há

> uma burocracia enorme que dificulta muito o andamento da investigação, essa dificuldade decorre, devido ao endereço IP da máquina do autor, ser uma informação protegida pelo sigilo de dados (Art.5 da CF), assim, para poder se comprovar os dados referentes ao cadastro do IP, faz-se necessária autorização judicial para as autoridades acessarem as informações da pessoa que proferiu a injúria, calúnia ou difamação.

Portanto, ao se conectar à internet, o servidor de acesso à rede, atribui um endereço ao computador, que funcionará como sua identidade. Nesse processo, o IP desenvolve um papel relevante, no prazo em torno de 30 dias, pois, identificará quem são os indivíduos que se conectaram na internet naquele momento e lugar, ajudando na identificação dos autores.

Durante esse processo, há duas posições no ordenamento jurídico brasileiro, pois, há os que defendem que a quebra desse sigilo do IP fere o que o artigo 5º, inciso XII, da Constituição o qual declara que: "É inviolável o sigilo das correspondências e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal". Por outro lado, há os que defendem o posicionamento de que o artigo 5º, inciso IV, da CF/88, determina que: "É livre a manifestação do pensamento, sendo vedado o anonimato" (Brasil, 1988).

2.1 A lei dos crimes cibernéticos (lei nº 12.737/2012) - O caso Carolina Dieckman

A Lei nº 12.737/2012, conhecida como "Lei Carolina Dieckmann", representa um marco na legislação brasileira sobre crimes cibernéticos. Sancionada em 30 de novembro de 2012 e em vigor desde abril de 2013, a lei foi criada em resposta a um caso amplamente divulgado envolvendo a atriz Carolina Dieckmann. Na ocasião, o computador da atriz foi invadido, e fotos íntimas foram roubadas e divulgadas sem sua autorização. O incidente evidenciou a necessidade de regulamentação específica para lidar com crimes no ambiente digital, especialmente a invasão de dispositivos informáticos e a violação de privacidade.

A lei trouxe alterações importantes ao Código Penal Brasileiro, tipificando crimes cibernéticos como a invasão de dispositivo informático, descrita no artigo 154-A, que penaliza o acesso não autorizado a dispositivos alheios mediante violação de mecanismos de segurança com a finalidade de obter, adulterar ou destruir dados ou informações sem o consentimento do titular. Além disso, a lei prevê aumento de pena caso o crime cause prejuízo econômico ou seja cometido contra dispositivos destinados a serviços públicos ou de utilidade pública. O caso Carolina Dieckmann destacou a fragilidade do sistema jurídico brasileiro diante da crescente criminalidade cibernética e impulsionou debates sobre a privacidade e a segurança no ambiente digital. Antes da promulgação da lei, não havia previsão legal clara para punir a invasão de dispositivos, o que dificultava a responsabilização de infratores.

Apesar de ser um avanço significativo, a Lei nº 12.737/2012 enfrenta desafios contínuos, como a evolução constante das tecnologias e a sofisticação das técnicas utilizadas por cibercriminosos. O caso da atriz foi um divisor de águas ao trazer visibilidade à questão dos crimes cibernéticos e acelerar mudanças legislativas necessárias para proteger os direitos dos usuários no ambiente digital. Mesmo sendo um pilar no combate à criminalidade cibernética no Brasil, a lei demanda atualizações constantes para acompanhar as novas ameaças impostas pela era digital.

Em conclusão, a Lei nº 12.737/2012 representa um avanço significativo na proteção dos direitos dos cidadãos no espaço virtual, especialmente em um contexto onde crimes cibernéticos se tornaram uma preocupação crescente. O caso de Carolina Dieckmann catalisou a discussão sobre a necessidade de legislação específica e a importância da proteção da privacidade. No entanto, é necessário que a lei seja efetivamente aplicada e que haja um esforço contínuo para educar a população sobre os riscos da internet e a importância de proteger seus dados pessoais.

2.2 O Marco Civil da Internet (lei nº 12.965/2014) e a proteção de dados dos usuários

Em 2014, foi sancionada a Lei nº 12.965, também conhecida como a Lei do Marco Civil da Internet, que trouxe princípios, direitos, garantias e deveres dos usuários da internet. O crime de estelionato tipificado no artigo 171 do Código Penal brasileiro, obter para si ou para outra vantagem ilícita mediante ardil, artificio, meio fraudulento em prejuízo de

outrem. A principal característica do estelionato é manter a vítima em erro e deixá-la no prejuízo. No que tange o estelionato virtual, a única diferença havida entre o estelionato virtual e o real, é o modus operandi, pois o virtual necessita do uso de um equipamento de informática. Para este não há qualquer tipificação no ordenamento jurídico, a qual não pode haver qualquer condenação.

Maia (2017, p. 76), afirma que o Marco Civil se assenta em três pilares: "a garantia da neutralidade da rede; proteção à privacidade do usuário da Internet; e a garantia da liberdade de expressão".

O Marco Civil da Internet, estabelecido pela Lei nº 12.965/2014, representa um avanço significativo na regulamentação do uso da internet no Brasil. Essa legislação foi criada com o intuito de garantir os direitos dos usuários na rede, promovendo a liberdade de expressão, a privacidade, e a proteção de dados pessoais. A lei surgiu em um contexto em que a expansão da internet e a crescente digitalização das relações sociais e comerciais levantaram preocupações sobre a segurança e a privacidade dos dados dos usuários (Mendes, 2020).

Um dos principais objetivos do Marco Civil da Internet é assegurar a proteção da privacidade e dos dados pessoais dos internautas. De acordo com o artigo 7º, a lei estabelece que é assegurado ao usuário o direito à proteção de seus dados pessoais, sendo obrigatória a obtenção de consentimento para a coleta, uso e tratamento dessas informações. Essa abordagem reforça a ideia de que os dados dos usuários são uma extensão de sua identidade e, portanto, devem ser tratados com respeito e cuidado. Segundo Silva (2021), essa proteção é crucial em um cenário onde dados pessoais são frequentemente utilizados para fins comerciais sem o consentimento adequado dos titulares.

Além disso, a lei também define a responsabilidade dos provedores de serviço em relação à segurança dos dados que armazenam. O artigo 14 estabelece que esses provedores são responsáveis por danos causados por conteúdo gerado por terceiros, salvo se comprovada a ausência de culpa. Essa disposição busca garantir que os provedores adotem medidas eficazes de segurança e que os usuários sejam informados sobre as políticas de privacidade e de proteção de dados aplicáveis a suas informações pessoais (Costa, 2022).

O Marco Civil da Internet também criou um ambiente propício para a discussão e a formulação de políticas públicas relacionadas à proteção de dados. A Lei Geral de Proteção de Dados (LGPD), que entrou em vigor em 2020, é um desdobramento do Marco Civil, complementando as disposições sobre a proteção de dados pessoais. A LGPD estabelece princípios e diretrizes mais abrangentes, garantindo um maior controle dos usuários sobre suas informações e impondo obrigações rigorosas às empresas que lidam com dados pessoais. A relação entre o Marco Civil e a LGPD reforça a necessidade de um marco regulatório robusto e coeso para a proteção da privacidade e dos dados na era digital (Almeida, 2021).

A efetividade do Marco Civil da Internet na proteção de dados dos usuários também depende da conscientização e da educação digital. Muitos usuários ainda não estão plenamente cientes de seus direitos ou das implicações do compartilhamento de seus dados pessoais na internet. Portanto, campanhas de conscientização são fundamentais para empoderar os cidadãos e permitir que façam escolhas informadas sobre a privacidade e a segurança de suas informações. Como observado por Oliveira (2022), a educação digital deve ser parte integrante da discussão sobre proteção de dados, capacitando os usuários a compreenderem melhor os riscos envolvidos na navegação online.

Em síntese, o Marco Civil da Internet (Lei nº 12.965/2014) representa um marco significativo na proteção dos direitos dos usuários na internet, com ênfase na proteção de dados pessoais e na privacidade. A inter-relação com a LGPD e a necessidade de conscientização digital reforçam a importância de uma abordagem integrada para garantir a segurança e a privacidade dos internautas. Embora a legislação tenha avançado, a implementação efetiva das normas e a educação dos usuários são essenciais para assegurar que os direitos digitais sejam respeitados e protegidos.

3 CRIME DE ESTELIONATO

O estelionato é um crime tipificado no artigo 171, do Código Penal. No âmbito virtual, o estelionato é praticado pela conduta do agente de “induzir ou manter a vítima em erro, e com isso, obter vantagem ilícita, para si ou para outrem”. Portanto, o objetivo do agente é iludir a vítima, induzi-la ao erro, para que voluntariamente, ela entregue o bem,

valores ou informe seus dados pessoais, os quais possibilitará ao agente encontrar formas de obter vantagens nome da vítima.

3.1 Crime de Estelionato virtual no ordenamento jurídico brasileiro

Esse crime se configura majoritariamente através da possibilidade em que o autor delituoso encontra para obter proveito de modo ilícito, para si, ou para outrem, se utilizando de meios fraudulentos para realizar tal ato. Diante do ordenamento jurídico brasileiro, o sujeito passivo do estelionato será a vítima que sofreu o prejuízo, devendo ser pessoa certa e determinada, embora muitas vezes exista mais de um indivíduo envolvido na relação e o ativo é o indivíduo que o comete de forma dolosa, com livre e consciente vontade, podendo de modo diverso para alcançar seus fins.

Vale ressaltar que o estelionato virtual ainda é recente dentro dos tribunais brasileiros, apesar de seu cometimento ter sido bastante visto nos últimos anos, em que se deve a evolução da tecnologia que são identificados por meios mais eficazes para a realização.

O estelionato virtual pode ser realizado como meio de: venda de produtos falsificados ou inexistentes em plataformas de comércio eletrônico, o oferecimento de oportunidades de investimento falsas em criptomoedas ou outros esquemas de pirâmide, e a aplicação de golpes em redes sociais, onde os criminosos se passam por pessoas conhecidas das vítimas para solicitar dinheiro ou informações pessoais.

Destaca-se o modo de realizar tal crime por meio da utilização de sites falsos com a mesma aparência e registro semelhante dos originais, para a captação de dados do usuário. Essa prática é conhecida como *Typosquatting*, em que os agentes estruturam uma página web na internet e registram o domínio idêntico ao de alguma grande empresa conhecida, resultando, por exemplo em: site original – www.walmart.com; site falso – www.wallmart.com (Barreto, 2021, p. 83).

Segundo Ataide (2017, p. 172) ocorre crime de estelionato virtual quando os infratores criam links, e-mails, etc., falsos, com o objetivo de não ser identificado e consequentemente prometem fazer algo que sabem não ser possível fazer, mas fazem a promessa em troca de alguma vantagem que em grande parte das vezes é pecuniária. Em síntese, o estelionato virtual se consuma com o induzimento da vítima, utilizando-se de

meios digitais, aproveitando-se das brechas que esses lhe permitem para conseguir obter vantagens.

A invasão do correio eletrônico da vítima também é uma forma de cometer esse crime, especialmente aquelas que tem o costume de consultar saldos e extratos bancários pelo computador. Nesse caso em específico, o estelionatário encontra uma maneira de clonar a página da internet banking e fazer com que a vítima tente fazer o acesso a conta, sem saber que os danos inseridos na dita página serão interceptados por um terceiro de má-fé. Outro tipo bem comum é praticado por pessoas de menor saber informático, os quais se utilizam de crenças populares ou correntes de sorte, para que ao final a vítima deposite determinada importância em dinheiro para que obtenha aquilo que foi veiculado, sendo garantido a esta que ao adquirir o almejado a importância lhe será devolvida, fato que não ocorre (Feitoza, 2012, p. 92).

Contudo, o cometimento do referido crime é perfeitamente realizado através da rede mundial de computadores. Aliás, tem sido bem comum que pessoas sejam vítimas de golpes de estelionatários na internet (Freitas, 2009, p. 23). Percebe-se, pois, que cada vez é mais frequente a prática de estelionato virtual, o que se deve principalmente como já analisado, ao avanço da tecnologia e popularização da internet.

De acordo com Cruz e Rodrigues (2018, p. 26) quando falam que o estelionato na internet tem se tornado cada vez mais frequente, um exemplo são os indivíduos que maliciosamente produzem sites de vendas com informações falsas de modo a induzir as vítimas a pagarem por produtos que sequer existem. Como informam os autores tem sido comum, a prática de estelionato no meio digital, e os autores, se utilizam de informações falsas para manipular a vítima e fazê-la acreditar em uma suposta vantagem.

Destaca-se que o estelionato virtual tende a ser praticado por pessoas com mais conhecimentos em informática. A única diferença entre o estelionato virtual e o estelionato comum, é o modo pelo qual o agente irá operar, pois o estelionato virtual é realizado em ambiente virtual e o estelionato comum em ambiente físico.

A respeito de sua previsão, o Código Penal não faz menção ao crime de estelionato virtual em seu texto, a conduta descrita no art. 171 do diploma diz respeito tão somente ao delito praticado diretamente pelo infrator, isto é, obter vantagem ilícita em prejuízo alheio,

não importando aqui se isto foi realizado por intermédio do computador ou da internet (Feitoza, 2012, p. 21).

Desse modo, o impasse que surge quando da tipificação do crime de estelionato virtual, é a ausência de norma penal específica. A própria Constituição Federal no art. 5º, inc. XXXIX, firma o princípio da legalidade, pelo qual não a crime sem lei anterior que venha para defini-lo, nem pena sem prévia previsão legal. A natureza jurídica desse dispositivo acaba por limitar a pretensão punitiva do estado, por inexistir tipificação expressa para o crime de estelionato virtual, em alguns casos seus adeptos são absolvidos devido a esta brecha deixada pelo Código Penal que datado de 1940 é antiquado para os dias atuais (Feitoza, 2012, p. 32).

Contudo, torna-se necessário o aprimoramento da legislação para enfrentar o estelionato virtual, considerando a dinamicidade e a evolução constante dos crimes cibernéticos. A criação de leis específicas que tipifiquem e punam de forma adequada as práticas criminosas no ambiente virtual é um passo importante para a efetividade do combate a esse tipo de crime.

4 PROJETOS DE LEI SOBRE O TEMA

O avanço tecnológico e a crescente digitalização das interações sociais e comerciais trouxeram consigo um aumento significativo no número de crimes cometidos no ambiente virtual. Entre os crimes cibernéticos, o estelionato virtual tem ganhado destaque, especialmente pela sua natureza fraudulenta e pelo impacto financeiro e emocional que causa às vítimas. O estelionato, tipificado no artigo 171 do Código Penal Brasileiro, consiste em obter vantagem ilícita, induzindo alguém em erro, por meio de artifícios ou meios fraudulentos. Com a digitalização, esse tipo de crime migrou para o ambiente virtual, exigindo que o legislador adaptasse as normas para coibir essa nova modalidade de fraude.

No Brasil, a Lei nº 14.155, sancionada em 2021, introduziu importantes alterações no Código Penal, estabelecendo agravantes para o crime de estelionato praticado por meio eletrônico ou digital, aumentando a pena em caso de utilização de informações fornecidas por dispositivos eletrônicos. A mudança legislativa visa adequar o ordenamento jurídico à realidade dos crimes digitais, uma vez que os crimes cometidos no ambiente cibernético

muitas vezes envolvem esquemas de difícil rastreamento, atingindo muitas vítimas em pouco tempo (Brasil, 2021).

Além dessa lei, diversos projetos de lei tramitam no Congresso Nacional com o objetivo de tornar ainda mais rigorosa a punição para os cibercrimes, em especial o estelionato virtual. Um dos exemplos é o Projeto de Lei nº 4554/2020, que propõe medidas mais efetivas para a responsabilização criminal e civil de infratores no ambiente digital, além de prever a criação de mecanismos de proteção e conscientização da população quanto aos riscos de golpes eletrônicos (Câmara dos Deputados, 2020). O projeto busca, entre outras coisas, equiparar as punições aplicadas a crimes cibernéticos àquelas já estabelecidas para crimes cometidos no ambiente físico, ampliando a abrangência das investigações e das penalidades.

Essas iniciativas legislativas refletem a preocupação do legislador brasileiro com o aumento dos crimes digitais e a necessidade de proteger os cidadãos no ambiente virtual. O estelionato virtual, que envolve práticas como fraudes bancárias, vendas falsas em plataformas digitais e golpes de *phishing*, tem prejudicado uma parcela significativa da população, sobretudo os mais vulneráveis, como idosos e pessoas com menor acesso à educação digital. Assim, a adaptação das leis e a criação de novos projetos são passos essenciais para garantir a segurança jurídica e combater de forma eficaz esses crimes (Santos, 2020).

Outro ponto relevante abordado nos projetos de lei sobre cibercrimes é a necessidade de cooperação internacional para combater o estelionato virtual. Devido à natureza transnacional da internet, muitos crimes são cometidos por indivíduos ou grupos localizados fora do território brasileiro, o que dificulta a investigação e a responsabilização. Nesse sentido, iniciativas como o Marco Civil da Internet (Lei nº 12.965/2014) e acordos de cooperação internacional são fundamentais para enfrentar esses desafios, estabelecendo diretrizes para o compartilhamento de informações entre nações e a agilização de processos investigativos (Vasconcellos, 2020).

Portanto, os projetos de lei sobre cibercrimes, com especial atenção ao estelionato virtual, mostram-se imprescindíveis para o enfrentamento das novas modalidades de criminalidade. A legislação brasileira tem avançado no sentido de fortalecer o arcabouço jurídico, mas ainda há muito a ser feito para que a sociedade digital seja devidamente

protegida. A educação digital e a conscientização pública são fundamentais para prevenir crimes virtuais, enquanto o aprimoramento das normas jurídicas e a cooperação internacional são essenciais para garantir a punição dos infratores e a segurança do ambiente virtual.

5 CONSIDERAÇÕES FINAIS

O avanço das tecnologias digitais e a crescente dependência da internet têm trazido inúmeros benefícios para a sociedade, mas também têm impulsionado o surgimento de novos desafios, especialmente no campo da criminalidade. Entre os diversos tipos de cibercrimes, o estelionato virtual destaca-se pelo impacto econômico e social significativo, afetando milhares de vítimas que frequentemente têm suas informações pessoais e financeiras exploradas por meio de fraudes eletrônicas.

No Brasil, a legislação tem se adaptado para enfrentar os desafios impostos por esse tipo de delito. A Lei nº 14.155/2021, ao modificar o Código Penal Brasileiro, trouxe importantes avanços ao agravar as penas para crimes cometidos por meios digitais. No entanto, embora as alterações legislativas sejam um passo fundamental, a eficácia do combate ao estelionato virtual depende de outros fatores, como o fortalecimento da investigação policial, a capacitação de profissionais especializados em crimes cibernéticos e a implementação de políticas públicas voltadas para a educação digital da população.

A complexidade do estelionato virtual está ligada ao caráter transnacional e anônimo do ambiente digital, que facilita a atuação dos criminosos e dificulta a identificação e punição dos infratores. Nesse contexto, a cooperação internacional e a modernização contínua das ferramentas de investigação tornam-se imprescindíveis para a eficácia do enfrentamento desses crimes. Além disso, a conscientização dos usuários sobre práticas seguras na internet é essencial para reduzir a vulnerabilidade às fraudes eletrônicas.

O estelionato virtual também levanta questões éticas e jurídicas relevantes, como o equilíbrio entre a proteção da privacidade dos cidadãos e a necessidade de monitoramento digital para identificar atividades ilícitas. O avanço tecnológico exige um constante diálogo entre os atores do sistema de justiça, especialistas em tecnologia e a sociedade, para que o Direito se mantenha atualizado e eficaz diante das transformações digitais. Assim, a análise do estelionato virtual no Brasil reforça a importância de uma abordagem integrada, que

combine legislação adequada, mecanismos preventivos, fortalecimento das instituições e conscientização pública. Somente dessa forma será possível minimizar os impactos desse crime e garantir maior segurança no ambiente digital, contribuindo para a proteção dos direitos e da confiança dos usuários na era tecnológica.

REFERÊNCIAS

ALMEIDA, Gabriela Pinheiro. **Crimes Cibernéticos: uma análise da legislação brasileira e perspectivas de prevenção.** Dissertação (Mestrado em Direito) - Universidade de Brasília, 2018.

ALMEIDA, J. F. **Crimes Cibernéticos e a Lei Carolina Dieckmann**. São Paulo: Editora Atlas, 2021.

ALMEIDA, J. F. **Proteção de Dados e Marco Civil da Internet: Uma Análise Crítica**. São Paulo: Editora Atlas, 2021.

ATAÍDE, Amanda Albuquerque de. **Crimes Virtuais: uma análise da impunidade e dos danos causados às vítimas.** Maceió, 2017. Disponível em: http://www.faaiesa.edu.br/aluno/arquivos/tcc/tcc_amanda_ataide.pdf. Acesso em: 27 Maio 2024.

BRASIL. **Constituição da República Federativa do Brasil**. Vade Mecum. 11. ed. São Paulo: Saraiva, 2017.

BRASIL**. Lei nº 14.155, de 27 de maio de 2021.** Altera o Código Penal e o Código de Processo Penal, para agravar a pena de crimes cometidos por meio eletrônico, digital ou simulado. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 27 maio 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm. Acesso em: 22 out. 2024.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 4554/2020**. Modifica dispositivos do Código Penal, criando novas penas e medidas para crimes cometidos em ambiente digital. Câmara dos Deputados, Brasília, DF, 2020. Disponível em: https://www.camara.leg.br. Acesso em: 22 out. 2024.

COSTA, R. M. **A Eficácia da Lei dos Crimes Cibernéticos no Brasil**. Rio de Janeiro: Editora FGV, 2020.

COSTA, R. M. **Marco Civil da Internet: Direitos e Deveres dos Usuários.** Rio de Janeiro: Editora FGV, 2022.

CRUZ, Diego; RODRIGUES, Juliana. **Crimes Cibernéticos e a Falsa Sensação de Impunidade**. 2018. Disponível em: http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf. Acesso em: 27 Maio 2024.

FEITOZA, luis Guilherme de Matos. **Crimes Cibernéticos: o Estelionato Virtual.** Brasília, 2012. Disponível em: https://egov.ufsc.br/portal/sites/default/files/crimes_ciberneticos_o_estelionato_virtual.pdf. Acesso em: 27 Maio 2024.

FREITAS, Riany Alves de. **Segurança Estelionato Digital**. 2009. Disponível em: https://aplicacao.mpmg.mp.br/xmlui/bitstream/handle/123456789/502/Estelionato%20digital.pdf?sequence=3. Acesso em: 27 Maio 2024.

KSHETRI, N. ***International Perspectives on Cybercrime***. Routledge, 2017.

LAKATOS, E. M.; MARCONI, M. DE A. **Metodologia do trabalho científico.** São Paulo: Atlas, 2014.

MAIA, T. S. F. **Análise dos mecanismos de combate aos crimes cibernéticos no sistema penal brasileiro.** Universidade Federal do Ceará. Faculdade de Direito, Curso de Direito, Fortaleza, 2017.

MARCO CIVIL DA INTERNET. Disponível em: www.planalto.gov.br/ccivil_ 03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 27 Maio 2024.

MAUES, Gustavo Brandão Koury et. al. **Crimes Virtuais: uma análise sobre a adequação da legislação penal brasileira.** 2018. Disponível em: https://www.unirios.edu.br/revistarios/media/revistas/2018/18/crimes_virtuais.pdf. Acesso em: 27 Maio 2024.

MENDES, A. L. **O Marco Civil da Internet e Seus Impactos na Proteção de Dados.** Brasília: Editora da Câmara dos Deputados, 2020.

OLIVEIRA, P. R. **Educação Digital e Proteção de Dados na Era da Informação**. Porto Alegre: Editora PUC, 2022.

REGIS, André Tavares. **Crimes Contra a Honra na Internet: Dificuldade na Apuração dos Fatos**. João Pessoa, 2011.

RIBEIRO, L. A. **Privacidade e Segurança na Era Digital: O Caso Carolina Dieckmann**. Brasília: Editora da Câmara dos Deputados, 2019.

SANTOS, C. L. **Cibercrimes e a proteção penal no Brasil: desafios da era digital**. São Paulo: Revista dos Tribunais, 2020.

SANTOS, Liara Ruff dos et. al. **Os crimes cibernéticos e o direito a segurança jurídica: uma análise da legislação vigente no cenário brasileiro contemporâneo**. Santa Maria, 2017. Disponível em: http://coral.ufsm.br/congressodireito/anais/2017 /7-7.pdf. Acesso em: 27 Maio 2024.

SILVA, T. R. **Privacidade e Segurança na Era Digital: Desafios do Marco Civil**. Belo Horizonte: Editora UFMG, 2021.

SOUZA, Júlio Cesar**. Investigação Criminal Pela Polícia Militar e Sua Inconstitucionalidade**. 2012.

SOUZA, P. R. **Educação Digital e Conscientização em Segurança da Informação**. Porto Alegre: Editora PUC, 2022.

SPINIELI, André Luiz Pereira. **Crimes informáticos: comentários ao projeto de Lei n° 5.555/2013**. Brasilia, 2018. Disponível em: http://www.mpf.mp.br/atuacaotematica/ccr2/publicacoes/coletaneas-de-artigos/ coletanea_de_artigos_crimes_ ciberneticos. Acesso em: 27 Maio 2024.

SPINIELI, André Luiz Pereira. **Crimes informáticos: comentários ao projeto de Lei n° 5.555/2013**. Brasilia, 2018. Disponível em: http://www.mpf.mp.br/atuacaotematica/ccr2/publicacoes/coletaneas-de-artigos/ coletanea_de_artigos_crimes_ ciberneticos. Acesso em: 27 Maio 2024.

VASCONCELLOS, M. R. **O marco civil da internet e a cooperação internacional no combate aos crimes cibernéticos**. Belo Horizonte: Fórum, 2020.

WENDT, Emerson e NOGUEIRA JORGE, Higor Vinicius Nogueira. Editora Braspot. **Crimes Cibernéticos: Ameaças e Procedimentos de Investigação** – 2º Edição. 2017.