RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

CRIME DE ESTELIONATO NA CONTEMPORANEIDADE FRENTE À TECNOLOGIA VIRTUAL

CRIME OF STEALING IN CONTEMPORARY TIME IN FRONT OF VIRTUAL TECHNOLOGY

DELITO DE ROBO EN LA TIEMPO CONTEMPORÁNEO ANTE LA TECNOLOGÍA VIRTUAL

Thalya Aparecida SIlva Marques[1]

e555244
https://doi.org/10.47820/recima21.v5i5.5244

PUBLICADO: 05/2024

RESUMO

A Lei 14.155/2021, recentemente em vigor, introduz emendas ao Código Penal sobre crimes de pirataria informática e estelionato eletrônico. A mudança mais importante é a alteração do Artigo 154-A, que criminaliza a invasão de dispositivos informáticos para obter, manipular ou destruir dados. Sob o título "estelionato eletrônico", a nova lei criminaliza o estelionato qualificado pelo uso de meios eletrônicos, como redes sociais, contatos telefônicos e e-mails fraudulentos (art. 171, §2º-A). Essa mudança reflete a adaptação da lei ao avanço tecnológico contemporâneo, destacando os desafios jurídicos relacionados aos crimes cibernéticos. Este estudo analisa a relação entre o estelionato e a tecnologia digital, explorando como esta última potencializa essas práticas ilícitas. Os objetivos específicos são identificar métodos utilizados por criminosos cibernéticos, examinar medidas preventivas e repressivas e analisar os impactos sociais e econômicos do estelionato. Utilizou-se uma metodologia bibliográfica, com revisão sistemática da literatura. Espera-se contribuir para uma melhor compreensão dos desafios jurídicos no combate ao estelionato em um contexto tecnológico e fornecer subsídios para políticas públicas e estratégias preventivas mais eficazes.

PALAVRAS-CHAVE: Estelionato. Tecnologia Virtual. Crimes Cibernéticos.

ABSTRACT

Law 14,155/2021, recently in force, introduces amendments to the Penal Code on crimes of computer piracy and electronic fraud. The most important change is the amendment to Article 154-A, which criminalizes the invasion of computer devices to obtain, manipulate or destroy data. Under the title "electronic fraud", the new law criminalizes qualified fraud through the use of electronic means, such as social networks, telephone contacts and fraudulent emails (art. 171, §2º-A). This change reflects the adaptation of the law to contemporary technological advances, highlighting the legal challenges related to cybercrimes. This study analyzes the relationship between fraud and digital technology, exploring how the latter enhances these illicit practices. The specific objectives are to identify methods used by cyber criminals, examine preventive and repressive measures and analyze the social and economic impacts of embezzlement. A bibliographic methodology was used, with a systematic review of the literature. It is expected to contribute to a better understanding of the legal challenges in combating embezzlement in a technological context and provide support for more effective public policies and preventive strategies.

KEYWORDS*: Fraud. Virtual Technology. Cyber Crimes.*

RESUMEN

Acaba de entrar en vigor la Ley 14.155/21, que introduce modificaciones al Código Penal en relación con los delitos de piratería informática, hurto por fraude electrónico, estafa por fraude electrónico, entre otras cuestiones relevantes. El cambio más importante es la modificación del artículo 154-A del Código Penal, que tipifica como delito la invasión de un dispositivo informático con el objetivo de obtener, manipular o destruir datos. En el mismo sentido, bajo el título "fraude electrónico", la nueva ley tipifica como delito el fraude calificado mediante el uso de medios electrónicos "si el fraude se comete utilizando información proporcionada por la víctima o por terceros engañados a través de redes sociales, contactos telefónicos o el envío de correos electrónicos fraudulentos, o por cualquier otro medio fraudulento similar" (art. 171, §2-A, del Código Penal). Este cambio en la ley es importante ya que muestra cómo la ley está en línea con el contexto contemporáneo, donde el avance de la

[1] Centro Universitário de Goiatuba (Unicerrado).

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

tecnología virtual ha desencadenado una serie de desafíos y oportunidades, especialmente en el ámbito legal, donde los delitos cibernéticos, como la malversación de fondos, ganan terreno. prominencia. Este estudio tiene como objetivo analizar la relación entre el delito de malversación y la tecnología digital, investigando cómo esta última influye en el aumento de estas prácticas ilícitas. El objetivo general es comprender los mecanismos a través de los cuales la tecnología virtual incrementa la ocurrencia de casos de fraude.

PALABRAS CLAVE: *Malversación. Tecnología Virtual. Delitos informáticos.*

INTRODUÇÃO

Com a promulgação da Lei 14.155/2021, que introduz alterações ao Código Penal brasileiro em relação aos crimes cibernéticos, incluindo o estelionato, surge uma necessidade crítica de examinar a conexão entre os avanços contemporâneos na tecnologia digital e a perpetração de atividades fraudulentas. No centro dessas modificações legais está a criminalização do acesso não autorizado a dispositivos de computador e o uso de meios eletrônicos para cometer fraudes, destacando a evolução do cenário comportamental criminoso na era digital.

A pesquisa em questão adentra nas complexidades do estelionato no contexto da tecnologia virtual, com o objetivo de elucidar como a proliferação de ferramentas digitais influencia o aumento de práticas ilícitas. Central para essa investigação é a questão principal: Como a tecnologia digital contribui para a escalada do estelionato na sociedade contemporânea?

O objetivo geral deste estudo é compreender os mecanismos pelos quais a tecnologia virtual exacerbada a prevalência de esquemas fraudulentos, especialmente no âmbito do estelionato. Para alcançar esse objetivo, foram delineados objetivos específicos, incluindo identificar os principais métodos empregados por criminosos cibernéticos para perpetrar o estelionato, avaliar a eficácia de medidas preventivas e punitivas implementadas para combater tais crimes, e analisar as ramificações sociais e econômicas do estelionato nos tempos modernos.

Metodologicamente, esta pesquisa adota uma abordagem bibliográfica, conduzindo uma revisão sistemática da literatura existente sobre o tema. Ao sintetizar e analisar trabalhos acadêmicos pertinentes, este estudo se propõe a fornecer uma compreensão abrangente dos desafios apresentados pelo estelionato em um ambiente digitalizado e oferecer *insights* para a formulação de estratégias legais mais eficazes e medidas preventivas.

A importância desta pesquisa reside em seu potencial para contribuir para o aprimoramento de estruturas legais e políticas destinadas a combater o estelionato na era digital. Ao lançar luz sobre a interação entre tecnologia virtual e atividades fraudulentas, este estudo busca informar partes interessadas, formuladores de políticas e agências de aplicação da lei sobre a natureza em constante evolução dos crimes cibernéticos e a necessidade imperativa de adaptar os mecanismos regulatórios de acordo.

2. MODALIDADES DE ESTELIONATO

Entre os crimes sem violência física ou grave ameaça à pessoa, temos a perseguição,

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

caracterizada pelo Artigo 171 do Código Penal. Este crime é caracterizado quando o agente usa qualquer meio fraudulento, enganando alguém ou mantendo-o nesta situação e obtendo assim uma vantagem indevida para si ou para outra pessoa, em detrimento da propriedade de outra pessoa.

Na segunda seção deste artigo, "os fatos que possivelmente constituiriam o crime de estelionato em sua fórmula básica são definidos, mas que, na opinião do legislador, mereciam uma referência proeminente para evitar qualquer dúvida sobre a qualificação desses eventos" (Mirabete, 2017, p. 295).

2.1 Disposição de coisa alheia como própria

Esta ofensa é cometida por aqueles que, "vendem, trocam, dão em pagamento, alugam ou garantem uma coisa pertencente a outro como própria". (Artigo 171(2)(I) do Código Penal).

O assunto ativo é o vendedor. O sujeito passivo é o comprador de boa-fé, enganado pelo engano do vendedor, ou seja, é o comprador enganado e não o dono da coisa.

A infração surge com o recebimento do preço (venda), da coisa (troca) ou do primeiro aluguel (locação), com o pagamento (pagamento em espécie), com o recebimento do empréstimo (pagamento em espécie) ou do objeto desejado pelo infrator, mesmo que não tenha havido a tradição da coisa móvel e a transcrição da coisa imóvel.

Como esta é uma lista restritiva, ela não inclui a promessa de venda ou a transferência de direitos. O consumo desta cláusula ocorre quando o benefício é concedido, ou seja, quando o preço, a coisa trocada etc., é recebido.

2.2 Alienação ou oneração faudulenta de coisa própria

Este é o caso de uma pessoa que "vende, troca, dá em pagamento ou como garantia sua própria propriedade inalienável, onerada ou disputada, ou aquela que prometeu vender a terceiros, mediante pagamento em prestações, mantendo-se em silêncio sobre qualquer uma destas circunstâncias". (Artigo 171, parágrafo 2, II, Código Penal).

A propriedade inalienável é aquela que não pode ser vendida, seja por determinação legal ou contratual. O sujeito ativo da ofensa é o proprietário, o possuidor, que não pode vender a coisa porque está em uma das condições descritas acima, "(...) se o comprador, entretanto, souber da inalienabilidade ou que a coisa já foi cometida para pagamento em prestações, ele também será responsável pela ofensa, se for provada a conivência com o vendedor" (2015, p. 16). A parte ofendida é aquela que sofre o dano pecuniário, aquela que dá em pagamento uma coisa resultante de um contrato viciado, portanto nulo ou anulável. Ele recebe a coisa sem saber que ela é inalienável, sobrecarregada, disputada ou prometida a terceiros.

A lista também é exaustiva, não incluindo aluguel, promessa de venda e cessão de direitos. O objeto material é a coisa em si, que não pode ser vendida ou sobrecarregada. O tipo subjetivo desta ofensa é caracterizado pela vontade de se envolver em um dos comportamentos previstos pela lei, conhecendo as circunstâncias que a impedem. Consumado quando o lucro ilícito é obtido, o

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

agente enganar a vítima sobre o estado da coisa vendida ou onerada, mantendo-se em silêncio sobre qualquer uma das circunstâncias acima mencionadas.

2.3 Defraudação do penhor

É cometido por alguém que "de estelionato, por uma disposição não consentida pelo credor ou por outros meios, o bem penhorado, enquanto ele estiver de posse do mesmo". (Artigo 171(2), Seção III, Código Penal).

Esta é a alienação não consentida pelo credor, desviando a penhora da garantia penhorada enquanto em posse do objeto. O contrato de penhor pressupõe uma transação legal envolvendo duas pessoas, o credor e o devedor. Excepcionalmente, o devedor pode manter o objeto em sua posse e, se ele o descarta ou o torna irrealizável, comete estelionato.

O agente desta ofensa é o devedor que, embora permanecendo na posse do objeto depositado, dispõe dele em detrimento do credor. O simples depositário não comete esta ofensa, mas pode ser caracterizado no primeiro ponto deste mesmo parágrafo do artigo 171.

Os bens penhorados devem ser móveis e constituem o objeto material desta ofensa. A ausência de consentimento por parte do credor garantido é o elemento normativo da infração. O consumo ocorre quando a coisa é vendida, destruída etc.

3. O ESTELIONATO NA LEI 14.155

3.1 Estelionato Virtual

O crime virtual está aumentando constantemente. A Internet é uma forma fácil e hábil de acessar informações; neste sentido, a velocidade do progresso tecnológico permite, de certa forma, um acesso fácil aos computadores, e a população sente a necessidade de estar conectada a este meio de computador, para desfrutar e compartilhar qualquer tipo de informação.

Embora a tecnologia da informatização tenha vindo para facilitar e racionalizar a vida social e profissional dos seres humanos, há pessoas que se aproveitam da vulnerabilidade da informação e, através de meios astutos e fraudulentos, obtêm para si mesmas uma vantagem ilícita às custas dos outros.

O direito, como ciência social aplicada, não pode permanecer inerte diante do comportamento ilícito virtual que está ocorrendo. A lei deve se adaptar e fornecer novas tipologias de comportamento virtual (Lima, 2011)

No capítulo anterior, tratamos do crime de estelionato, conforme definido no artigo 171 do Código Penal, quando o sujeito obtém uma vantagem ilícita para si mesmo às custas do sujeito passivo por artifício, trapaça ou qualquer outro meio fraudulento.

Mas agora gostaríamos de falar sobre estelionato virtual, um crime que ocorre em um ambiente virtual, e que está em constante aumento. No entanto, não há uma criminalização expressa da estelionato virtual; de fato, a própria lei penal é inerte a esta questão.

O artigo 5º da Constituição Federal de 1988, parágrafo XXXIX, garante que não há crime sem

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

uma disposição legal e nenhuma punição sem uma condenação prévia. Entretanto, a natureza jurídica desta disposição limita a pretensão punitiva do Estado, e como a estelionato virtual não é caracterizada no sistema jurídico, o sujeito ativo é absolvido da conduta praticada.

Veja como Cezar Roberto Bitencourt ensina esta interpretação do princípio de legalidade:

> O princípio da legalidade ou da reserva legal constitui efetiva limitação ao poder punitivo estatal. Feuerbach, no início do século XIX, consagrou o princípio da reserva legal por meio da fórmula latina *nullum crimen, nulla poena sine lege.* O princípio da reserva legal é um imperativo que não admite desvios nem exceções e representa uma conquista da consciência jurídica que obedece a exigências de justiça; somente os regimes totalitários o têm negado (Bitencourt, 2015, p. 109).

Neste norte, três condições essenciais são necessárias para a composição do fato típico, ou seja, o crime deve ser típico, ilegal e culpado. Neste sentido, o elo causal é a relação entre o comportamento do sujeito ativo e os danos sofridos pelo sujeito passivo. É necessário enfatizar que os crimes de computador não são praticados por qualquer pessoa, mas por aqueles que têm um conhecimento profundo de programas de computador, que têm a capacidade técnica para este tipo de conduta.

Se compararmos brevemente estelionato virtual e estelionato real, a diferença entre as duas reside apenas no modus operandi, já que a estelionato virtual utiliza um suporte informático. Somente. Guilherme Feitoza mostra como ocorre a estelionato virtual:

> Uma das formas mais recorrentes do estelionato no ciberespaço é a invasão do correio eletrônico da vítima, em particular o daquelas pessoas que possuem o costume de consultar seus saldos e extratos bancários pelo computador. Nesta situação, o estelionatário (*crackler*) encontra alguma maneira de clonar a página legítima do internet banking do usuário e fazer com que ele tente fazer o acesso, sem saber que os dados que estão sendo inseridos serão interceptados por um terceiro de má-fé que irá usá-losindevidamente (Feitoza, 2012, p. 48).

A primeira maneira é quando o fraudador invade o e-mail da vítima e encontra uma maneira de clonar a página onde o sujeito passivo consulta seus saldos bancários, e deixa esta página para a vítima, induzindo-a ao erro, permitindo-lhe assim fornecer os dados de acesso acreditando que a página consultada é real. A segunda modalidade apresentada, é semelhante à história do "bilhete", a maioria das pessoas idosas cai nas histórias contadas pelo sujeito ativo.

3.2 As mudanças trazidas pela Lei 14.155

Ao longo dos anos, a tecnologia tem imposto novas formas de interação na sociedade e transformado as relações interpessoais. O desenvolvimento da inteligência artificial trouxe seres humanos para um mundo cada vez mais interconectado, no qual os países estão se aproximando uns dos outros. As ferramentas tecnológicas transcenderam as barreiras do espaço e do tempo, e é impossível dissociar o homem do século 21 do acesso à informação.

Apesar das profundas mudanças trazidas pela tecnologia da informação, o lado negativo deste progresso é o uso desta vantagem para a prática de crimes. A necessidade de formas de proteção e segurança das informações transmitidas através da web é, portanto, urgente, pois os

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

crimes cometidos com dispositivos virtuais estão se tornando cada vez mais frequentes em todo o mundo.

O legislador criminal tem tentado lentamente acompanhar o desenvolvimento do crime cibernético e, através da prevenção geral negativa, não conseguiu agravar os crimes mencionados no menu legislativo da Lei 14.155, como fez no pacote anticrime. De acordo com Cláudio do Prado Amaral (2020, p. 08), o legislador:

> equivoca-se ao abraçar, práticas de criminologia e segurança pública comprovadamente falidas, como nos casos de aumento de penas in abstrato e de elevação das frações para obtenção de progressão de regime prisional na execução. São políticas criminais que revelam claramente a acolhida da prevenção geral negativa ou da intimidação psicológica.

A Lei nº 14.155, de 27 de maio de 2021, modificou o Código Penal Brasileiro a fim de aumentar a punibilidade dos crimes de violação de dispositivos de informática, roubo e estelionato cometidos por meios eletrônicos ou pela Internet, e definir a jurisdição nas modalidades de estelionato através do Código de Processo Penal.

A estelionato eletrônica apresentada no Artigo 171, §2º-A, em sua redação, é punível com uma pena de prisão de 4 a 8 anos, se o comportamento fraudulento do agente for cometido através de redes sociais, contatos telefônicos fraudulentos ou envio de e-mails fraudulentos, ou qualquer outro meio fraudulento semelhante.

Este não é um novo tipo de estelionato, infere-se que o legislador apenas delimitou os meios/espaços para cometer estelionato, proporcionando um grau mais elevado de reprovação, aumentando assim a sanção da conduta:

> 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:
>
> Estelionato eletrônica
>
> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a estelionato 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).

A redação do estelionato eletrônico é semelhante às disposições do caput do artigo 171 do Código Penal, na medida em que retoma o uso da expressão "qualquer outro meio fraudulento", que anteriormente cobria todas as formas de comissão da infração. O estelionato é, portanto, o ato que potencialmente leva a vítima ao engano, independentemente do espaço (físico ou virtual) em que é realizada, sendo suficiente a configuração dos elementos essenciais do tipo criminoso: erro, vantagem ilícita e danos a terceiros, e intenção de dano.

Em 2013, o ex-deputado Eduardo Azeredo ofereceu uma proposta legislativa para tentar permitir a criminalização do crime de estelionato informática, com base na técnica fraudulenta

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

conhecida mundialmente como *Phishing,* e chamou a atenção para a falta de campanhas esclarecedoras na mídia sobre esses ataques que estão se espalhando pelo país.

Phishing seria incorporado ao Artigo 171(2) como ponto VII, e teria a seguinte redação: as mesmas penalidades seriam incorridas por aqueles que "enviassem mensagens digitais de qualquer tipo, fazendo-se passar por empresas, instituições ou pessoas com o objetivo de induzir outros a revelar informações pessoais, identidade ou senhas de acesso".

Antes da entrada em vigor desta lei, os delitos nesta área eram atípicos e os tribunais não concordavam sobre como aplicá-los ou como adaptá-los à lei existente. Portanto, era necessário criar um delito criminal capaz de incorporar este delito moderno, que não poderia ser baseado em estelionato comum, roubo ou desvio de fundos.

Entretanto, o uso do termo por meio de redes sociais (delimitando o espaço onde o comportamento criminoso será sancionado pela pena agravada), contatos telefônicos ou envio de *e-mails* fraudulentos é uma das formas de engenharia social utilizada para cometer o delito, uma espécie do gênero, ou seja, *phishing.* E por qualquer outro meio fraudulento ou similar, a mesma formulação utilizada na seção principal do artigo 171 retorna, sem promover a inovação prevista com a aplicação do estelionato eletrônico, que seria incorporar a manipulação do computador ou da rede como o núcleo da ofensa, o que ampliaria a lista de condutas utilizadas pelos fraudadores digitais.

Portanto, é evidente que o legislador não está pronto para se adaptar às novas tendências criminosas presentes no ciberespaço. A analogia continuará sendo a base dos juízes diante da nova forma de crime no mundo moderno.

Mais uma vez, a retórica do direito penal simbólico parece ser a resposta do Estado às demandas cada vez mais estruturais - contribuindo para o sistema prisional inchado e para a hiperinflação legislativa - já que se baseia em criminologia retrógrada e repressão excessiva.

O direito penal está assim saturado de exigências que nunca foi capaz de satisfazer. Existem incentivos ao crime que vão muito além da capacidade da lei penal de contornar, seja através de seus objetivos preventivos ou através da mera imposição de punição como retribuição.

A evolução manifestada pela Lei 14.155 é apenas uma atualização das penas, que praticamente dobram em comparação com a estelionato comum (prisão de 1 a 5 anos), para a estelionato eletrônica (prisão de 4 a 8 anos). Quanto ao direito penal espanhol, no entanto, houve uma grande melhoria legislativa na adaptação da lei ao delito cibernético, a ponto de levar tanto os delitos, a estelionato comum como a estelionato informática, ao mesmo quantum de punição, exceto por certas circunstâncias agravantes.

3.2.1 Da aplicação da lei frente ao princípio da retroatividade da lei penal mais benéfica

Em conformidade com o princípio de não retroatividade da lei, cobrir fatos anteriores somente se for benéfico. Assim, ela é aceita na doutrina e na jurisprudência, incluindo o mandato constitucional (art. 5º, XL, CFRB/1988), a retroatividade da lei mais benéfica, ou, como alguns a

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

conhecem, "o princípio da retroatividade da lei mais benéfica". Isto significa que a nova lei se aplica retroativamente apenas em benefício do acusado.

Assim, a lei penal será retroativa, mesmo que o réu já tenha sido condenado. De fato, se não for mais um crime, ou se a sentença for reduzida, por exemplo, isso é benéfico para o réu e deve ser aplicado a ele. Neste sentido, Art. 2 do Código Penal: "Ninguém pode ser punido por um ato que uma lei posterior deixa de considerar como crime, e a execução e os efeitos penais da condenação cessam em virtude dessa lei".

Portanto, se for prejudicial ao acusado, não deve ser retroativo Art. 5, XL, CFRB/1988. Entretanto, o direito penal substantivo da época do crime deve ser aplicado em benefício do acusado.

Assim, por exemplo, se John comete um ato que não é considerado crime hoje, e amanhã entra em vigor uma lei que criminaliza essa conduta, ele não pode ser punido pelo ato que antecede a lei criminal.

Neste sentido, a única coisa que é legalmente inaceitável é que partes de ambas as leis sejam aplicadas, eliminando apenas as partes benéficas de ambas as leis. Um excelente exemplo utilizado pelos autores é o caso da Lei de Narcóticos e da antiga Lei de Narcóticos, onde a jurisprudência demonstra isso. Neste exemplo, portanto, se a nova lei é vantajosa para o réu, que é o caso da posse para consumo, a lei antiga é substituída, no momento dos fatos, pela nova lei, mais vantajosa, mesmo que os fatos sejam anteriores.

Para ilustrar, por exemplo, o Art. 4 do Art. 171 CP, anteriormente a pena era dobrada, com a nova redação, de 1/3 (um terço) para o dobro. Aconteceu que 1/3 era mais benéfico do que o dobro (aplica-se).

Por outro lado, os artigos 2, A e 2, B, do estelionato eletrônico, são novos tipos que estão inseridos, portanto, as condutas anteriores, não devem ser consideradas nesta lei. É necessário encontrar outro tipo de crime que existia no momento do ato, para verificar se corresponde, caso contrário, o ato deve ser atípico, em conformidade com o mandamento constitucional do art. 5, XL, CF.

Ele se aplica ao artigo 154-A, que na época previa uma pena de prisão de três meses a um ano e uma multa, e que agora prevê uma pena de prisão de um a quatro anos e uma multa. Esta última, por sua vez, só é aplicável a condutas cometidas após a entrada em vigor da lei, uma vez que, mais importante, não será retroativa. Portanto, para os tipos de 154-A, se cometidos antes da entrada em vigor da Lei 14. 155, deve ser enquadrado com o que a regra já previa anteriormente, ou seja, detenção de três meses a um ano, e uma multa (ofensa de menor potencial ofensivo).

4. CRIME DE ESTELIONATO NA CONTEMPORANEIDADE FRENTE À TECNOLOGIA VIRTUAL

Com as transformações trazidas pelas inovações tecnológicas, as trocas de informações e os meios de comunicação alcançaram um patamar antes inimaginável. Notícias são disseminadas instantaneamente, transações comerciais são realizadas a todo momento, bastando alguns cliques

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

na tela de dispositivos móveis, que outrora eram apenas vislumbrados como ficção científica, mas que hoje se tornaram centros de mídia, conhecimento, interação social e comércio. Paralelamente a essas mudanças, a internet, concebida e implementada antes do virar do século, serviu como catalisador para o fenômeno da globalização. No entanto, tais avanços também trouxeram consigo desafios ainda maiores, uma vez que, ao proporcionar um espaço vasto, acessível e aparentemente anônimo, a prática de crimes, inerente à natureza humana, encontrou terreno fértil na web, onde novos esquemas e fraudes foram concebidos, revestidos pela volatilidade do meio digital (Silva; Carvalho, 2022).

A partir da utilização do ambiente virtual, os criminosos passaram a operar com mais respaldo em suas ações delituosas, uma vez que estas podem ser realizadas à distância, de forma ágil e repetida, ampliando o número de vítimas devido à abrangência das redes. Além disso, a facilidade na obtenção de informações permite aos golpistas manipular suas vítimas com mais eficácia, enquanto, contemporaneamente, existem diversas formas de transferência de valores que facilitam a obtenção rápida de vantagens ilícitas, reduzindo as oportunidades para que as vítimas percebam que estão sendo enganadas (Silva; Carvalho, 2022).

O crime de estelionato, uma das formas mais comuns de fraude, assumiu novas dimensões na contemporaneidade, em meio ao avanço da tecnologia virtual. Nesse contexto, os golpistas se adaptaram às ferramentas digitais, ampliando suas táticas para ludibriar as vítimas. A facilidade de acesso à internet e o uso generalizado de dispositivos eletrônicos proporcionaram aos criminosos um campo fértil para suas atividades ilícitas. Por meio de e-mails fraudulentos, sites falsos e até mesmo aplicativos de mensagens, os estelionatários conseguem alcançar um grande número de pessoas de forma rápida e eficaz (Dias, 2023).

A rapidez e a facilidade com que as transações podem ser realizadas online também contribuíram para a proliferação do estelionato. Muitas vezes, as vítimas são levadas a agir impulsivamente, sem a devida verificação da autenticidade das informações ou da legitimidade do negócio proposto. Além disso, a sensação de anonimato proporcionada pela internet pode levar as pessoas a baixarem a guarda, compartilhando informações pessoais e financeiras com indivíduos desconhecidos (De Azevedo Nunes; Madrid, 2019).

Os golpes virtuais podem assumir diversas formas, desde a clonagem de cartões de crédito até a criação de sites falsos de compras online. Os criminosos utilizam técnicas sofisticadas de engenharia social para manipular as emoções e a confiança das vítimas, induzindo-as a fornecer dados sensíveis ou a realizar transferências bancárias fraudulentas. As consequências desses golpes podem ser devastadoras, resultando em prejuízos financeiros significativos e danos emocionais para as vítimas (De Azevedo Nunes; Madrid, 2019).

A complexidade e a transnacionalidade dos crimes cibernéticos também representam desafios adicionais para as autoridades policiais e os sistemas jurídicos. Muitas vezes, os criminosos operam em redes globais, dificultando sua identificação e captura. Além disso, as leis e regulamentações relacionadas à segurança cibernética ainda estão em processo de

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

desenvolvimento, o que pode dificultar a aplicação efetiva da justiça em casos de estelionato virtual (Silva, 2023).

Diante desse cenário, torna-se imperativo adotar abordagens multidisciplinares e cooperativas para combater o estelionato na era digital. A educação pública sobre segurança cibernética e práticas seguras de navegação na internet é essencial para capacitar os usuários a reconhecerem e evitarem golpes online. Além disso, é fundamental que as empresas e instituições financeiras implementem medidas robustas de segurança digital para proteger seus clientes contra fraudes virtuais. Somente por meio de uma abordagem abrangente e colaborativa, podemos enfrentar eficazmente os desafios apresentados pelo crime de estelionato na contemporaneidade frente à tecnologia virtual (Dias, 2023).

CONSIDERAÇÕES

Seguindo os esforços de muitos profissionais que trabalham em vários ramos do direito e que defendem um ambiente digital legalmente sólido, a Lei 14.155/21, destinada a combater a estelionato eletrônica, foi finalmente publicada em 27 de maio, após aprovação pelo Presidente Jair Bolsonaro.

Com base no PL 4554/20, de autoria do Senador Izalci Lucas (PSDB/DF), a nova lei, que tem como um de seus objetivos qualificar os crimes cometidos através de estelionato eletrônica, aumentando as penas aplicáveis, introduz modificações no Código Penal (Decreto-Lei 2.848/40) e no Código de Processo Penal (Decreto-Lei 3.689/41), mecanismos antigos e desatualizados que exigem ajustes constantes na realidade factual de nosso sistema jurídico.

As emendas da nova lei são parcialmente baseadas no art. 154-A do Código Penal, que classifica a invasão de dispositivos informáticos como um ato ilegal, que foi inserido por ocasião da Lei 12.737/12, na época apelidada de "Lei Carolina Dieckmann", devido à atriz brasileira, vítima de um ato equivalente, que fortaleceu o debate sobre o assunto e levou à aprovação da lei.

A nova lei trata do agravamento dos delitos de violação de dispositivos informáticos, roubo e estelionato cometidos eletronicamente ou através da Internet, e oferece uma nova perspectiva na luta contra um tipo de crime que experimentou forte crescimento, especialmente porque encontra novas maneiras de ser cometido.

É importante salientar que a mudança de gravidade é fundamental para este tipo de crime, pois o poder de incômodo do crime digital é muito maior, além da necessidade, em muitos casos, de realizar uma investigação para identificar os infratores, o que pode depender da realização de um determinado tipo de escuta telefônica, que, de acordo com a legislação sobre intercepções, Lei 9.296/96, artigo 2, só pode ser obtida para crimes puníveis com prisão, não sendo aplicável a crimes de menor potência ofensiva, que seriam aqueles puníveis com detenção.

É importante ressaltar que desde a Lei 12.737/12, quase dez anos se passaram e o problema do estelionato eletrônico assumiu maiores proporções devido aos desenvolvimentos tecnológicos e cibernéticos: novas redes sociais, reconhecimento facial, bancos digitais, moedas

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

virtuais, entre outros. Hoje, especialmente com o cenário da pandemia global da covid-19, a atenção a estas questões devem ser ainda maior, pois o momento levou a um aumento substancial da quantidade de transações realizadas em um ambiente virtual.

Uma parte considerável da população que não estava familiarizada com ferramentas digitais e, portanto, não utilizava os equipamentos e plataformas para realizar transações de rotina, tais como compra, venda, recebimento e pagamento, foi forçada a um novo contexto. Entretanto, a resposta deste contingente foi positiva, indicando uma situação de permanência pós-pandêmica.

O surgimento de novos modelos de pagamento e transações instantâneas, como a PIX, e mais recentemente a WhatsApp, também endossou os aspectos de facilitar transações em um ambiente virtual, servindo também como um cenário para a prática de novas estelionatos.

Nesta fase, as instituições financeiras, especialmente os bancos, como guardiões práticos do ambiente financeiro, têm na nova Lei 14.155/21 um reforço da luta contra a estelionato, pois a regulamentação do setor, sem a força do direito penal, é muito menos eficaz.

Agora é imperativo entender a nova lei e usá-la como um aliado para melhorar a segurança cibernética e os procedimentos de segurança da informação para mitigar a ocorrência de estelionato eletrônica e seu impacto sobre as organizações.

REFERÊNCIAS

BAHIA, Flavia. **Direito constitucional.** 3ª ed. Pernambuco: Armador, 2017.
BAYER, D. A. O desuso da ética na busca pela audiência. **Jusbrasil**, maio 2013. Disponível em: https://diegobayer.jusbrasil.com.br/artigos/121943201/o-desuso-da-etica-na-busca-pela-audiencia. Acesso em: 21 abr. 2024.

BOBBIO, Norberto. **A Era dos Direitos**. Tradução: Carlos Nelson Coutinho. Rio de Janeiro: Campus, 1992,

BRANCO, Paulo Gustavo Gonet. Aspectos de teoria geral dos direitos fundamentais. *In:* MENDES, Gilmar Ferreira et al. **Hermenêutica e direitos fundamentais**. Brasília: Brasília Jurídica, 2002.

BRASIL. **Constituição federal da republica de 1988**. Brasilia: Constituição, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 21 abr. 2024.

COMPARATO, Fábio Konder. **A Afirmação Histórica dos Direitos Humanos**. 11. ed. São Paulo: Saraiva. 2018

DE AZEVEDO NUNES, Mário Vinicius; MADRID, Fernanda de Matos Lima. Crimes Virtuais: O Desafio Do Código Penal Na Atualidade E A Impunidade Dos Agentes. **ETIC-ENCONTRO DE INICIAÇÃO CIENTÍFICA**, v. 15, n. 15, 2019. ISSN 21-76-8498.

DIAS, Paulo Eduardo Leite. **A evolução cibernética e a falta de punibilidade célere dos crimes digitais:** crimes digitais na plataforma Whatsapp. 2023. TCC (Graduação) – PUC-GOIÁS, Goiania, 2023. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/5966. Acesso em: 21 abr. 2024.

FERREIRA, Olavo Augusto Viana Alves. **Controle de constitucionalidade e seus efeitos.** 3. ed. Salvador: Editora Juspodivm, 2016.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

GIL, Antônio Carlos**. Métodos e Técnicas de Pesquisa**. 6. ed. São Paulo: Atlas, 2006.

GOMES, J. P.; MELO, S. D. O poder midiático na esfera do Direito Penal: Repercussões de uma sociedade punitiva. **Revista Transgressões**, v. 1, n. 2, p. 66-84, 27 jan. 2015.

LIMA, Alvino**. Culpa e risco**. 2. ed. São Paulo: Revista dos Tribunais, 1999.

RAMOS, André de Carvalho. **Curso de direitos humanos**. 7 ed. São Paulo: Saraiva, 2020.

SILVA, Lucas. Fraude eletrônica: furto ou estelionato? (Direito). **REAL Repositório Institucional**, v. 1, n. 1, 2023.

SILVA, Moacir Antunes; CARVALHO, Urssulla Rodrigues. 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: 21 abr. 2024.