

FRAUDES DIGITAIS E SEUS EFEITOS NA SEGURANÇA PÚBLICA BRASILEIRA

Matheus Trajano Franco de Sousa¹

Murilo Francisco Misson Júnior²

Paulo Henrique da Silva³

RESUMO: Este estudo tem como objetivo analisar o crime de estelionato, destacando suas modalidades contemporâneas e repercussões na segurança pública brasileira. A metodologia adotada consiste em uma revisão bibliográfica que explora definições legais e a engenharia social utilizada por criminosos para manipular as vítimas. Os resultados evidenciam um aumento significativo nos casos de estelionato, especialmente em contextos digitais, devido à transformação tecnológica que expõe vulnerabilidades. A pesquisa conclui que a dinâmica entre criminosos e vítimas, agravada pela pandemia, intensifica os riscos de fraudes. Embora a legislação recente tenha tipificado o estelionato digital, há uma necessidade urgente de aprimorar investigações e políticas públicas. O estudo recomenda que futuras pesquisas explorem a eficácia das novas leis e que sejam desenvolvidos programas de educação digital para conscientizar a população sobre os riscos. A colaboração entre órgãos de segurança e plataformas digitais é essencial para uma resposta eficaz. Em suma, a pesquisa destaca a urgência de fortalecer políticas de segurança digital e reestruturar práticas policiais para mitigar os impactos do estelionato no Brasil.

Palavras-Chave: Estelionato digital. Segurança pública. Engenharia social. Políticas públicas. Educação digital

INTRODUÇÃO

O tema deste artigo aborda a transformação do estelionato no contexto digital, enfatizando as modalidades de golpes que emergem nesse ambiente e os impactos que esses crimes geram na segurança pública brasileira. Diante do aumento alarmante das estatísticas de estelionato, especialmente os que ocorrem de forma virtual, torna-se imprescindível investigar como as novas tecnologias têm influenciado o comportamento criminoso e afetado a vida dos cidadãos.

A delimitação do assunto abrange o crescimento dos crimes de estelionato nos últimos anos, com foco particular naqueles realizados por meios digitais, como internet e telefonia.

¹Graduando do 10º período de Direito na Centro Universitário Presidente Tancredo de Almeida Neves (UNIPTAN). Endereço eletrônico: matheustrajanofranco@gmail.com

² Graduando do 10º período de Direito na Centro Universitário Presidente Tancredo de Almeida Neves (UNIPTAN). Endereço eletrônico: murilomissonjunior@hotmail.com

³ Graduando do 10º período de Direito na Centro Universitário Presidente Tancredo de Almeida Neves (UNIPTAN). Endereço eletrônico: paulohds.13@gmail.com

Esses crimes têm se proliferado devido à facilidade de acesso às plataformas online e à falta de educação digital entre os usuários, principalmente entre populações vulneráveis, como idosos e pessoas de baixa renda. A pandemia de COVID-19 intensificou essa situação, forçando muitos a realizarem transações online sem a devida precaução, resultando em um aumento significativo nas ocorrências de estelionato.

A problematização central deste estudo gira em torno da questão: como o crescimento significativo dos crimes de estelionato no Brasil pode ser relacionado à era digital? A pesquisa busca compreender de que maneira o ambiente virtual propicia a ação dos golpistas e como a confiança excessiva das vítimas contribui para o sucesso dessas fraudes.

O objetivo geral desta pesquisa é realizar um levantamento bibliográfico da literatura recente sobre o crime de estelionato, apresentando as modalidades de golpes aplicadas pelos criminosos e analisando suas repercussões na segurança pública brasileira.

Os objetivos específicos incluem a análise da definição do delito segundo a legislação atual, a identificação das modalidades de estelionato mais comuns na contemporaneidade e a coleta de dados estatísticos sobre os impactos desse crime na segurança pública.

As hipóteses a serem testadas sugerem que a engenharia social utilizada pelos criminosos e a vulnerabilidade das vítimas, exacerbada pela confiança excessiva e pela falta de vigilância, são fatores fundamentais para o aumento do estelionato virtual. Ademais, a escolha dos criminosos por esse tipo de crime, que não exige presença física e minimiza riscos, é uma das razões para a escalabilidade desse fenômeno.

O marco teórico deste estudo será fundamentado em uma abordagem interdisciplinar, combinando a análise jurídica, empírica e estatística do crime de estelionato. Serão exploradas obras de referência sobre o tema, como as de Rogério Greco e Fernando Capez, apresentando uma visão de algumas das modalidades de golpes digitais recorrentes. Também serão utilizadas estatísticas do Anuário Brasileiro de Segurança Pública de 2024, que revelam um crescimento alarmante nos casos de estelionato, fornecendo uma base sólida para a discussão sobre as tendências e padrões desse crime.

A justificativa deste trabalho reside na necessidade urgente de entender e alertar sobre os mecanismos que levam as vítimas a serem manipuladas pelos golpistas, especialmente em um contexto onde as fraudes digitais estão em ascensão. Compreender a dinâmica da engenharia social e a exploração das fraquezas emocionais das vítimas é essencial para o desenvolvimento de estratégias eficazes de prevenção e combate a esses crimes. A pesquisa visa contribuir para a criação de políticas públicas mais efetivas e campanhas educativas que abordem os riscos associados ao estelionato digital.

A metodologia a ser utilizada inclui uma revisão literária dos conceitos e definições sobre o crime de estelionato, aliada à análise de dados estatísticos do Anuário Brasileiro de Segurança Pública. A pesquisa será qualitativa e quantitativa, buscando compreender tanto os aspectos teóricos quanto os práticos da criminalidade digital. A partir dessa análise, pretende-se desenvolver recomendações para políticas públicas e intervenções sociais que possam mitigar os riscos enfrentados pelas vítimas de estelionato, promovendo uma maior conscientização sobre as fraudes digitais.

1 ASPECTOS FUNDAMENTAIS DO CRIME DE ESTELIONATO

a) Definição do delito de estelionato

O estelionato, crime tipificado no artigo 171 do Código Penal Brasileiro, é uma das práticas criminosas mais recorrentes no contexto social e econômico do país. Esse delito é caracterizado pela obtenção de vantagem ilícita em detrimento de outra pessoa mediante artifício, fraude ou qualquer outro meio enganoso, cuja finalidade é obter uma vantagem ilícita sobre a vítima, na qual, em consequência da sua ação, cause prejuízo alheio, conforme figurado na redação do Código Penal Brasileiro:

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 (Brasil, 1940).

O doutrinador, Rogério Greco (2024, p. 641), em sua obra literária, faz uma conclusão sobre o que se trata o estelionato, trazendo da seguinte forma:

Concluindo, a palavra estelionato se origina de *stellio*, ou seja, camaleão, justamente pela qualidade que tem esse animal para mudar de cor, confundindo sua presa, facilitando, assim, o bote fatal, bem como para poder fugir, também, dos seus predadores naturais, que não conseguem, em virtude de suas mutações, perceber a sua presença, tal como ocorre com o estelionatário que, em razão de seus disfarces, sejam físicos ou psíquicos, enganar a vítima com sua fraude, a fim de que tenha êxito na sua empresa criminosas.

Essa comparação ilustra de forma clara a natureza furtiva e estratégica do estelionatário, que, assim como o camaleão, se insere no ambiente social de forma discreta e calculada, ocultando seus verdadeiros interesses. A capacidade de manipulação e a habilidade em criar situações fraudulentas são características centrais no modo de agir desse crime, que visa alcançar seus objetivos ilícitos sem serem descobertos.

Ao utilizar essa analogia, a frase sublinha a engenhosidade e a perversidade inerentes ao estelionato, um crime que se baseia na confiança e na credulidade da vítima para se concretizar. Assim, o estelionatário, tal qual o camaleão em seu habitat natural, se adapta ao contexto em que atua, utilizando-se de truques que lhe permitem enganar e, conseqüentemente, obter vantagem ilícita com sucesso.

Um ponto importante a ser salientado nesta conceituação é a diferenciação entre o estelionato (artigo 171 do Código Penal) e furto mediante fraude (artigo 155, §4º, II, do Código Penal) que, apesar de ambos envolverem a utilização de meios fraudulentos, diferem significativamente em sua execução e na natureza do prejuízo causado à vítima, sendo tratados de forma distinta pelo Código Penal brasileiro.

A distinção entre os dois crimes reside na forma como o bem é transferido. No estelionato, há uma entrega voluntária, ainda que induzida pelo engano, ou seja, a vítima é enganada por uma falsa realidade, ocasionando, na entrega do bem ou dinheiro de maneira consciente do ato realizado. No furto mediante fraude, o bem é subtraído sem que a vítima perceba ou consinta, com a fraude servindo apenas como meio para facilitar essa subtração. Essa diferença é essencial para a aplicação das leis penais, influenciando a qualificação do crime e a pena aplicada.

Em consonância com esse pensamento, Rogério Greco (2024, p. 478) no diz que:

O fundamento da diferença reside no fato de que no furto com fraude o comportamento ardiloso, insidioso, como regra, é utilizado para que seja facilitada a subtração pelo próprio agente dos bens pertencentes à vítima. Ao contrário, no crime de estelionato, o artifício é utilizado pelo agente para que, induzindo ou mantendo a vítima em erro, ela própria possa entregar-lhe a vantagem ilícita.

Portanto, é fato que o estelionato é um crime marcado pela astúcia e capacidade de dissimulação do crime. Essa analogia ressalta a habilidade do estelionatário em se camuflar no contexto social, utilizando fraudes e truques para explorar a confiança e a vulnerabilidade de suas vítimas. A análise de Rogério Greco reforça essa perspectiva, ao destacar como o estelionatário emprega disfarces físicos ou psicológicos para induzir ao erro e obter vantagens ilícitas e, conseqüentemente, fazer com que a vítima tenha uma participação direta no delito, sendo um agente fundamental para a sua consumação.

b) Sujeito ativo e passivo

Qualquer indivíduo pode ser autor de crime de estelionato, uma vez que o tipo penal não exige uma qualidade ou condição especial para quem comete o ato. Da mesma forma, qualquer pessoa pode ser vítima desse crime. Vale ressaltar que, além do proprietário, qualquer um que, mesmo sem ser o proprietário, sofra prejuízo devido à conduta do agente pode ser considerado vítima da ação criminosa.

Porém, Rogério Greco(2024, p. 642). elucida que:

Há necessidade, entretanto, que o sujeito passivo seja pessoa determinada, pois, caso contrário, se for praticado contra um número indefinido de pessoas, o delito poderá ser desclassificado para uma das hipóteses previstas na Lei nº 1.521, de 26 de dezembro de 1951, que dispõe sobre os crimes contra a economia popular, ou mesmo uma das infrações penais contra a relação de consumo, previstas pelo Código de Defesa do Consumidor (Lei nº 8.078, de 11 de setembro de 1990).

O sujeito passivo do crime de estelionato deverá possuir capacidade de discernimento para que possa, de acordo com os elementos do tipo penal em estudo, ser induzido ou mantido em erro. Se lhe falta essa capacidade, tal como ocorre com alguns incapazes, o fato poderá ser desclassificado, por exemplo, para o delito tipificado no art. 173 do Código Penal.

Neste trecho, Rogério Greco aborda aspectos importantes da tipificação do crime de estelionato, enfatizando a necessidade de que o sujeito passivo seja uma pessoa identificável e tenha a capacidade de compreender a situação para que possa ser enganada ou mantida em erro. Caso contrário, se o crime for praticado contra um grupo indefinido de pessoas, ele pode ser reclassificado para um delito previsto em legislações específicas, como a Lei n° 1.521/51 (Lei de Crimes contra a Economia Popular) ou na Lei n° 8.078/90 (Código de Defesa do Consumidor), que trata de fraudes e abusos de forma mais abrangente.

Além disso, a menção à capacidade de discernimento do sujeito passivo é crucial, pois a falta dessa capacidade, como nos casos envolvendo pessoas deficientes, pode levar à desclassificação do crime de estelionato para outro delito, como o previsto no art. 173 do Código Penal, que trata do abuso de incapazes. Isso demonstra a importância de se considerar a condição da vítima para a correta tipificação do crime, o que reflete a necessidade de uma análise detalhada dos elementos envolvidos em cada caso.

c) **Bem jurídico tutelado**

Quando se trata do crime de estelionato, o bem jurídico protegido nesta relação é o patrimônio, conforme expresso no título II da Lei n° 2.848/40 (Código Penal). Tal afirmação é condizente com o entendimento do Doutrinador Fernando Capez (2024, p. 446), haja vista que, em sua obra literária, afirma que “{...}O dispositivo penal visa, em especial, reprimir a fraude causadora de dano ao patrimônio do indivíduo {...}”.

Bem como, seguindo a mesma linha de raciocínio de Fernando Capez, Rogério Greco (2024, p. 642), em sua obra acrescenta que:

Não se pode esquecer de que, por meio da incriminação contida no tipo penal do art. 171 do diploma repressivo, procura-se proteger as relações sociais com a punição do comportamento fraudulento, preservando-se, assim, a indispensável confiança que deve existir entre os membros da sociedade.

Assim sendo, Fernando Capez enfatiza que o objetivo principal do dispositivo penal é garantir a inviolabilidade do patrimônio, reprimindo fraudes que causem prejuízo patrimonial aos indivíduos. Ele ressalta que a função do artigo 171 do Código Penal é proteger o patrimônio das pessoas contra ações fraudulentas.

Por outro lado, Rogério Greco expande essa visão, observando que a proteção do estelionato também visa proteger as relações sociais, preservando a confiança necessária para o bom funcionamento da sociedade. Ele argumenta que o crime de estelionato não afeta

apenas o patrimônio individual, mas também a confiança mútua que é fundamental para o convívio social.

d) Consumação

Quando se fala do estelionato sabemos que se trata de um crime material onde ocorre a consumação quando o agente obtém um benefício econômico causando danos patrimoniais à vítima. Geralmente, esses resultados ocorrem de forma simultânea, de modo que o estelionatário, através de um golpe, obtém o lucro enquanto a vítima, sendo ludibriada, sofre o prejuízo.

Seguindo a linha de raciocínio, Rogério Greco (2024, p. 643) nos diz que:

Crime material, tem-se por consumado o estelionato, em sua modalidade básica, quando o agente consegue obter a vantagem ilícita, em prejuízo da vítima. Há necessidade, para efeitos de reconhecimento de consumação do estelionato, da afirmação do binômio vantagem ilícita/prejuízo alheio. Assim, quando o agente consegue auferir a vantagem ilícita em prejuízo da vítima, o delito chega à sua consumação.

Bem como, em consonância com o autor mencionado anteriormente, Fernando Capez (2024, p. 449) entende que:

Trata-se de crime material. Consuma-se com a obtenção da vantagem ilícita indevida, em prejuízo alheio, ou seja, quando o agente auferir o proveito econômico, causando danos à vítima. Via de regra, esses resultados ocorrem simultaneamente. Há, assim, ao mesmo tempo, a obtenção de proveito pelo estelionatário e o prejuízo da vítima.

Fica evidente que ambos enfatizam a necessidade da existência do binômio vantagem ilícita e prejuízo alheio para que o delito seja considerado consumado. Portanto, a consumação do estelionato ocorre no momento em que o estelionatário, através de um ato fraudulento, obtém o benefício econômico às custas do dano patrimonial sofrido pela vítima.

e) Tentativa

É admissível a tentativa quando o agente não consegue obter a vantagem indevida por motivos alheios à sua vontade. Um exemplo seria um indivíduo que, fingindo ser técnico de informática, adentra na casa da vítima, sob o pretexto de consertar o notebook e utiliza da sua condição para levar o aparelho consigo. No entanto, durante a execução do fato criminoso, é surpreendido pelo verdadeiro profissional que teria sido contratado para efetuar o conserto. Nesse caso, o agente não obteve a vantagem ilícita em prejuízo da vítima por motivo alheio, caracterizando-se a tentativa.

Fernando Capez (2024, p. 450) acrescenta que:

É também necessário verificar se o meio empregado era realmente apto a ludibriar a vítima, caso em que haverá tentativa. É a hipótese em que alguém tenta iludir a balconista de uma loja, com um cheque adulterado, mas esta, por cautela, vem a certificar-se da fraude, mediante consulta ao terminal de computador. Haverá tentativa, pois o meio era eficaz, tendo sido frustrado por circunstâncias alheias à

vontade do autor. Tal não ocorre se o meio empregado for totalmente ineficaz, como, por exemplo, na adulteração grosseira de documento, que pode de pronto ser constatada. Nesse caso, haverá crime impossível pela ineficácia absoluta do meio empregado.

Sendo assim, após breve análise, fica evidente que a admissibilidade da tentativa em situações onde o agente não consegue obter a vantagem ilícita se caracteriza devido a fatores fora de seu controle, contra a vontade do sujeito ativo. O exemplo apresentado ilustra como a tentativa é configurada quando o criminoso é impedido de concluir o crime por uma intervenção externa, como no caso do falso técnico de informática que é surpreendido antes de completar o delito.

Bem como, Fernando Capez acrescenta uma análise importante, destacando a necessidade de avaliar a eficácia do meio empregado para enganar a vítima. Se o meio utilizado for eficaz, mas o crime for frustrado por circunstâncias alheias à vontade do autor, como no caso de um cheque adulterado que é detectado pela balconista, caracteriza-se a tentativa. No entanto, se o meio empregado for totalmente ineficaz, como uma falsificação grosseira de documento, o crime é considerado impossível devido à ineficácia absoluta do método, conforme o artigo 17 da Lei nº 2.848/40 (Código Penal).

f) Qualificadora da fraude eletrônica

Os § 2º-A e 2º-B, introduzidos ao art. 171 do Código Penal pela Lei 14.155/21, tipifica crimes relacionados a fraudes em transações eletrônicas, como fraudes em pagamentos online e invasão de dispositivos, fornecendo uma abordagem mais coesa e específica, onde as penas foram aumentadas, refletindo a gravidade das consequências dessas ações, e há uma ênfase na proteção de dados pessoais, tendo como objetivo aprimorar a segurança digital, buscando proteger cidadãos e empresas e promovendo um ambiente online mais seguro.

Vejamos o texto da lei:

§ 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.

§ 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional. (BRASIL, 1940).

Nesse contexto, Guilherme de Souza Nucci (2023, p. 724)., em sua obra literária, elucida o tema da seguinte forma:

Tratando-se de estelionato, a utilização da fraude (ardil, cilada, engano) envolve a vítima de tal forma que ela acredita estar dispondo de algum valor porque realiza um negócio promissor ou qualquer atividade de seu interesse. Por isso, a norma estabelece que a pessoa ofendida, por erro, entrega o montante sugerido pelo agente do crime. O meio utilizado é a informação fornecida pela própria vítima ou terceiro enganado, valendo-se de redes sociais, contatos feitos por telefone ou envio de e-

mails fraudulentos. Amplia-se ao final, prevendo qualquer outro mecanismo fraudulento análogo.

Bem como, de maneira diferente, porém, seguindo a mesma linha de pensamento de Guilherme de Souza Nucci, Fernando Capez (2024, p. 464) traz o tema do seguinte aspecto:

Segundo o § 2º-A, em caso de fraude cometida com 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 meio análogo, a pena é de reclusão de 4 a 8 anos e multa. É o caso, por exemplo, das mensagens via SMS encaminhadas para celulares oferecendo prêmios, cliques em links falsos ou até ligações em que atendem pessoas vulneráveis ou idosas que acabam por passar informações que darão “munição” para o fraudador atuar. Se o crime for praticado mediante a utilização de servidor mantido fora do território nacional, considerada a relevância do resultado gravoso, a pena será aumentada de 1/3 (um terço) a 2/3 (dois terços) (§ 2º-B).

Os referidos autores mencionados acima, em suas respectivas obras, elucidam a aplicabilidade desses novos dispositivos, destacando como o engano e a manipulação das vítimas por meio de diferentes tecnologias se tornaram um modo comum de agir dos estelionatários. Nucci foca na característica do crime de estelionato, onde a vítima, induzida a erro, acredita estar agindo de forma legítima, enquanto Capez enfatiza exemplos práticos, como mensagens de SMS fraudulentas ou ligações a pessoas vulneráveis, demonstrando a abrangência e a pertinência das novas regras.

Ambos os autores convergem na ideia de que a legislação visa não apenas punir, mas também dissuadir essas práticas ao impor penas mais rigorosas, e promovendo, assim, um ambiente digital mais seguro e protegido contra fraudes, tendo a vista a evidenciação do aumento de delitos cometidos através do modo virtual.

2 ALGUMAS MODALIDADES DE ESTELIONATO

A doutrina majoritária, conforme expõem autores como Nucci, Capez e Greco, examina em detalhe algumas modalidades de golpes, com especial atenção para o crime de estelionato. Esses estudiosos ressaltam como a forma de obtenção do bem – geralmente caracterizada pela entrega voluntária da vítima, induzida em erro – influencia diretamente na tipificação penal e na definição da pena aplicável. Além disso, observam que, embora a vítima devesse ter um dever de cuidado, o estelionatário aprimora constantemente suas estratégias de engenharia social, tornando o golpe ainda mais eficaz.

Acrescenta-se que normalmente os estelionatários, quando obtém uma vantagem ilícita financeira, esta é costumeiramente recebida através de transferências bancárias rápidas, como por exemplo as transações pix, entretanto, conforme Ribeiro (2023, p. 123):

Em tais casos, salienta-se a questão da impunidade na medida em que as transações bancárias, ainda que registradas e rastreáveis, nem sempre indicam a autoria do delito, tendo em vista que atualmente é possível criar contas em carteiras digitais

com poucos cliques e quase nenhuma documentação, o que possibilita que os golpistas utilizem de “contas-laranja”, adquiridas por meio de informações vazadas em bancos de dados, por exemplo, a fim de afastar sua autoria.

Ao fim de sua pesquisa, reforçando a ideia da dificuldade em se encontrar o real autor do golpe, Ribeiro (2023, p. 124), G. S., constatou que:

Logrou-se êxito em confirmar a hipótese da dificuldade em identificar o sujeito ativo dos crimes virtuais, em especial, do estelionato, na medida em que a autoridade policial, por muitas vezes, não consegue encontrar os autores com os meios que tem em mãos, devido ao constante uso de perfis e contas falsas, ou ainda de titulações bancárias ou números de telefone em nome de laranjas, o que protela ainda mais qualquer tentativa de persecução penal.

Desta forma, nota-se que as contas bancárias receptoras da transação e até mesmo os dados cadastrais do telefone envolvido na fraude, após uma investigação policial, acabam sendo rastreáveis, todavia identificados como “laranjas” ou pessoas que já foram vítimas em situações pretéritas e que acabaram passando informações e documentações para os estelionatários que realizaram a abertura e cadastro destas contas.

Vejam os seguintes exemplos de modalidades:

Golpe dos falsos banners de publicidade: Ocorre o anúncio falso em sites e redes sociais de vendas de produtos ou pacotes de viagens com preços muito mais acessíveis do que as lojas convencionais, redirecionando as vítimas para sites fraudulentos, que por fim realizam o pagamento acreditando que receberão aquilo pelo que pagaram, todavia sem sucesso.

Golpe do site falso do DETRAN para pagamento de IPVA: A vítima realiza pesquisas de pagamento de IPVA ao DETRAN de seu estado através da plataforma Google, a qual disponibiliza logo no início da página de busca o site falso do DETRAN. Após a vítima digitar dados como renavam e placa, acaba realizando o pagamento, impelido mais ainda pelo fato do golpista disponibilizar o pagamento via pix com desconto, o que não é ofertado pelos sites oficiais do DETRAN dos estados e do Distrito Federal. Este golpe também pode ser aplicado por e-mail, pelo qual a vítima acessa o boleto enviado pelo estelionatário e realiza o pagamento, também de forma fraudulenta.

Golpe do falso leilão de veículos: A vítima realiza pesquisas de veículos que estejam a venda em sites de leilões, que normalmente, quando legítimos, já são vendidos por um valor mais baixo que o convencional. Após entrar no site, aquele que não é legítimo, e contactar o autor por um telefone, um possível leiloeiro, através do aplicativo whatsapp, é que a vítima fornece dados, documentos e realiza o pagamento. O estelionatário anuncia os veículos por um preço ainda mais acessível que o leilão autêntico, e a vítima, ao realizar o pagamento e receber uma carta de arrematação falsa, quando se desloca ao pátio credenciado não encontra o bem adquirido e nem a pessoa que lhe realizou a venda.

Golpe da falsa venda de produtos anunciados no Market Place do Facebook: Através de perfis fakes, os estelionatários anunciam a venda de eletrodomésticos, como televisão, geladeiras, etc., ou até mesmo veículos, todos eles usados, por um preço muito abaixo do ofertado no mercado, todavia solicitam um adiantamento de pagamento via pix, pois, caso não o façam, não poderão segurar a venda, visto que existem outros compradores interessados, dizendo que, assim que realizarem o pagamento, poderão pegar o produto no endereço em que se encontram, que é falso, repassado pelo autor do golpe.

Golpe da intermediação de venda de veículos automotores: O golpe consiste na situação em que o estelionatário contacta um vendedor de carro através do WhatsApp, solicitando fotos e documentação do veículo anunciado online. O golpista então publica o carro em outra plataforma a um preço muito abaixo do valor real, atraindo um comprador. Ele simula a venda com o comprador, alegando que o carro está com um parente, e também faz promessas ao vendedor para garantir a negociação. O estelionatário organiza um encontro entre vendedor e comprador, pedindo que não comentem sobre valores. No final, ele solicita um pagamento via Pix, alegando que o parente entregará o carro após o pagamento. Após receber o dinheiro, o golpista bloqueia ambos no WhatsApp e desaparece.

Golpe da falsa compra realizada no cartão de crédito: O estelionatário envia uma mensagem SMS ou liga para a vítima informando que realizaram uma compra em seu cartão de crédito. Acreditando que o estelionatário é realmente algum atendente do banco que estaria auxiliando a cancelar aquela falsa compra, bem como a não ter o restante de seu patrimônio dilapidado por uma possível falsa invasão de dispositivo ou clonagem de cartão, a vítima acaba fornecendo alguns dados pessoais para o autor da ação. Com a promessa de que está realizando algumas ações para colocar segurança no aplicativo bancário da vítima, o estelionatário a orienta a realizar diversos pix para contas bancárias fraudulentas, informando que estas contas são do banco e que está transferindo estes valores para que fiquem em um local seguro, comunicando que serão devolvidos posteriormente, todavia não se passam de falsas promessas.

Golpe do falso combatente e produto retido na alfândega: O golpista faz contato através de uma rede social fazendo amizade com a vítima, informando ser um militar ou um trabalhador em missão humanitária em outro país. Por fim, após conquistar a confiança da vítima, após um longo período de conversas e envio de falsas fotos no local, que não são suas, o golpista alega ter encontrado uma grande quantia em dinheiro ou um pacote valioso que precisa ser enviado ao Brasil, solicitando à vítima que receba este produto em solo brasileiro para que possam dividir posteriormente quando retornar ao Brasil. Entretanto o objeto, falsamente, é retido na alfândega, momento em que o golpista solicita que a vítima faça

pagamento de taxas alfandegárias ou outros custos para liberar o produto enviado, todavia não se passa de um golpe.

Golpe da falsa carta de crédito de consórcio: Neste golpe o autor anuncia uma falsa carta de crédito de consórcio já contemplada, através de redes sociais, sendo que o golpista a oferece por um valor atrativo, muitas vezes abaixo do mercado, para atrair a vítima. O estelionatário alega urgência na venda, usando desculpas como necessidade de dinheiro rápido ou mudança de planos. Convencida da vantagem, a vítima realiza o pagamento integral ou faz o pagamento de uma parte como forma de dar um sinal. Após o pagamento, o golpista ainda pode solicitar mais dinheiro como forma de pagar outras taxas que ainda estão pendentes, fazendo com que a vítima se veja na necessidade de pagá-las, visto que já realizou o pagamento da entrada da referida carta e não quer perder o investimento já feito, todavia fraudulento. Ressalta-se que para fazer com que o golpe se torne mais real, o estelionatário utiliza nomes verdadeiros, todavia de pessoas que não sabem que tem seu nome envolvido na fraude, enviando para vítima até mesmo contratos de compra e venda e a carta de crédito em negociação.

Golpe da falsa venda de eletrodomésticos e móveis pelo perfil do Instagram ou Whatzapp: Inicialmente o golpista se apropria de um perfil real, geralmente de alguém que tenha uma boa reputação ou muitos seguidores. Em seguida, usando o perfil comprometido, o golpista começa a publicar ofertas de venda de eletrodomésticos, móveis, ou outros produtos populares alegando que estaria de mudança e que por este motivo estaria vendendo por um preço mais baixo. Rapidamente, com os preços tentadores, as vítimas entram em contato, momento em que o golpista as pressiona alegando que os produtos estão disponíveis em quantidade limitada ou que a oferta é válida por tempo determinado. Sendo assim, o estelionatário solicita que o pagamento seja feito antecipadamente, normalmente via transferência bancária, pix, ou outros métodos de pagamento que não oferecem proteção ao comprador. Após receber o pagamento o golpista bloqueia a vítima e não lhe responde mais as mensagens, momento em que a vítima percebe que caíra em um golpe.

Golpe do falso investimento financeiro pelo perfil do Instagram: Iniciado identicamente ao golpe exemplificado acima, o golpista, após se apropriar do perfil real de uma pessoa, utilizando da popularidade daquele perfil que normalmente possui diversos seguidores, o golpista anuncia investimentos financeiros atraentes, os quais terão um retorno rápido e significativo. Os golpistas atraem vítimas com promessas de dobrar ou até triplicar o investimento em pouco tempo. Eles usam técnicas de persuasão, convencendo a vítima a investir valores que em meses já teriam um retorno multiplicado, pedindo à vítima que faça

transferências, normalmente, por pix. Após o investimento da vítima, o golpista bloqueia a vítima ou desaparece completamente, levando todo o dinheiro angariado com a ação.

Golpe do falso parente solicitando dinheiro pelo *WhatsApp*: O golpe se inicia quando o estelionatário obtém números de telefone de parentes da primeira vítima, geralmente através de vazamento de dados e redes sociais abertas. Usando um número de telefone com o mesmo DDD das vítimas e uma foto roubada da rede social, o golpista entra em contato com um parente, como a mãe da vítima, fingindo ser o familiar que trocou de número. Ele alegadamente informa que sua conta bancária está bloqueada e pede ao parente que faça um pagamento urgente para outra pessoa. A vítima, acreditando que está ajudando um parente em necessidade, realiza a transação e acaba prejudicada. O estelionatário continua pedindo mais transações até que a vítima perceba o golpe.

Golpe da falsa renegociação de dívida: Neste golpe o autor oferece à vítima uma oportunidade falsa de renegociar suas dívidas com condições aparentemente vantajosas. Através do vazamento de dados, os golpistas têm conhecimento que a vítima já possui empréstimo realizado em seu nome. Em seguida, entra em contato com a vítima se passando por um representante de uma financeira ou funcionário de outro banco, oferecendo a renegociação, prometendo descontos significativos, com condições de pagamento facilitadas. Após o golpista conseguir com que a vítima contraia o empréstimo em outra instituição bancária, se passando por um representante de financeira, através da confiança adquirida pela vítima, solicita que ela faça o pix do valor total do empréstimo que foi para sua nova conta bancária para a conta da falsa financeira, informando que, no momento que cair em conta, realizará o pagamento àquele banco que havia feito o empréstimo inicialmente, todavia, é o momento em que percebe que ficará com os dois empréstimos em seu nome e que aquela financeira não era real.

Golpe da falsa herança: através das redes sociais, por mensagem privada, o golpista entra em contato com a vítima, fingindo ser um advogado, tabelião, ou representante de uma instituição financeira, alegando que a vítima foi identificada como beneficiária de uma grande herança deixada por um parente distante, ou até mesmo uma pessoa rica que faleceu sem herdeiros diretos. Por fim, acreditando que realmente possuía o referido parente, bem como de que não tinha nada a perder, somente ganhar, a vítima começa a atender às solicitações demandadas pelo falso advogado, o qual solicita o pagamento de tributos. Inicialmente solicita o pagamento de somente um, entretanto, posteriormente, solicita o pagamento de outros, momento em que a vítima entra em um túnel e se vê na necessidade de continuar pagando aquelas despesas para obter aquela falsa herança. Após realizar o falso pagamento de diversos tributos, acaba caindo em si e percebendo que fora envolvida em uma fraude.

Estelionato amoroso: O golpista inicia o contato com a vítima por meio de aplicativos de namoro ou redes sociais, criando um perfil falso com fotos e informações atraentes. Ele investe tempo em construir um relacionamento intenso e envolvente, trocando mensagens carinhosas e demonstrando interesse sincero. Após ganhar a confiança da vítima, o golpista cria uma emergência financeira, como um problema de saúde ou uma crise no trabalho, e começa a pedir ajudas financeiras, alegando que a reembolsará em breve. A vítima, indulgente, no intuito de ajudar, envia o dinheiro para aquele “namorado virtual”. O golpista continua pedindo diversas ajudas financeiras até que a vítima percebe que está diante de um golpe, pois aquele “namorado virtual” só acumula dívidas com a vítima, deixando-a com um prejuízo financeiro e emocional.

Após apresentados alguns dos golpes, nota-se, portanto, que, além da engenharia social ser bem aplicada pelo criminoso, a vítima não tem o dever de cuidado em analisar com paciência o contexto em que está inserida, não adotando medidas de cautela e verificação necessária antes de realizar as transações financeiras ou compartilhar informações sensíveis, sujeitando-se ao prejuízo que lhe é causado.

É o que corrobora Silva (2023, p. 69):

De plano, deve-se reiterar que grande parte dos delitos informáticos somente concretizam-se em virtude da contribuição da vítima. Em verdade, há uma maior incidência de tais crimes em vítimas que tenham dispensado as cautelas mínimas exigíveis no ambiente virtual, do que se deflui, ao revés, que a adoção destas últimas evitaria o êxito delitivo. Contudo, porquanto à vítima compete a autorresponsabilidade em relação aos seus próprios bens jurídicos, bem como o dever de informar-se relativamente aos riscos inerentes à sociedade atual, o seu papel não pode ser reputado irrelevante para o Direito Penal. Por isso, vislumbra-se a possibilidade de se suscitar a autocolocação da vítima em risco nos delitos cibernéticos, dentre os quais se insere o estelionato virtual.

Contudo, não se pode olvidar que, apesar da vítima tomar ações que contribuem para o sucesso do golpe, a responsabilidade principal pelo crime recai sobre o estelionatário, que utiliza meios ardilosos e fraudulentos para induzir a vítima ao erro. Desta forma, a contribuição da vítima é, em grande parte, uma consequência da manipulação habilidosa por parte do golpista, que explora as vulnerabilidades e as circunstâncias da vítima para alcançar seu objetivo ilícito.

3 IMPACTOS DO CRIME DE ESTELIONATO NA SEGURANÇA PÚBLICA BRASILEIRA

O Anuário Brasileiro de Segurança Pública de 2024 destacou um crescimento significativo nos casos de estelionato ocorridos no Brasil. Em comparação ao ano anterior, houve um aumento de 8,2% no total de registros, totalizando quase 2 milhões de casos em

2023. Nos últimos sete anos, o número de estelionatos aumentou em impressionantes 360%. Esse crescimento pode ser atribuído, em grande parte, à transformação digital e ao aumento das transações online, que facilitaram a proliferação de golpes virtuais, todavia reforça-se a ideia de que o criminoso e a vítima têm uma participação ativa e efetiva para a consumação do delito, visto que o primeiro está cada vez mais aprimorando sua persuasão manipulativa, e a vítima, pelo contrário, não toma o dever de cuidado necessário para evitar a fraude.

A pandemia de COVID-19 forçou a adaptação rápida ao ambiente digital, com reuniões e trabalhos sendo realizados, quase que sempre, de forma online. Essa mudança trouxe facilidades, mas também expôs vulnerabilidades, resultando no aumento dos crimes de estelionato virtual. Criminosos aproveitaram o aumento da presença online das pessoas para aplicar golpes, explorando a falta de familiaridade de muitos com as ferramentas digitais. Além disso, a redução de crimes de rua, como roubos e furtos físicos, em razão, talvez, do aumento da vigilância e da segurança pública, pode ter contribuído para a migração dos criminosos para atividades ilícitas online, que oferecem menos riscos, maior retorno financeiro, muitas vezes com a ocorrência da impunidade,

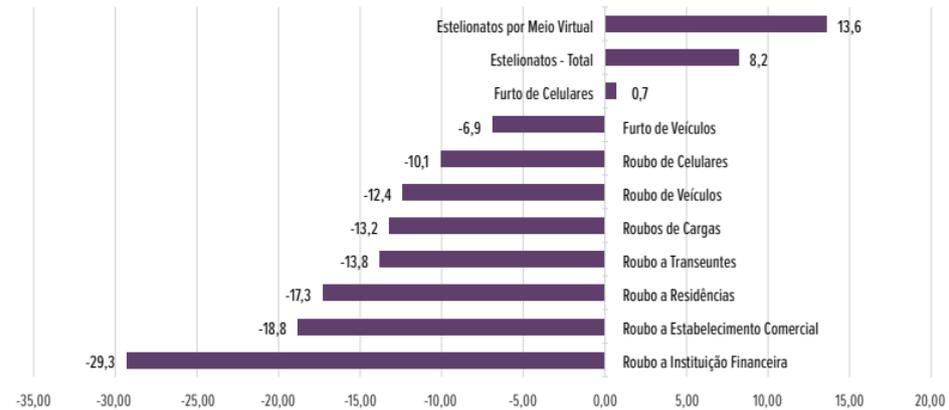
Neste sentido o Anuário de Segurança Pública aponta que:

No caso dos estelionatos cometidos por meios eletrônicos, a situação muda completamente de figura. O criminoso não precisa estar presencialmente diante da vítima e usar armas ou organizar uma estrutura física para um eventual confronto com as forças de segurança. Por trás da tela de um computador ou de um smartphone, o criminoso está protegido de todos os riscos associados à interação humana direta. Ou seja, as tecnologias digitais servem de escudo para o criminoso que pode atuar deixando menos vestígios e com chances ínfimas de confronto com a polícia. Além disso, as novas tecnologias permitem que os criminosos virtuais realizem os golpes em um volume muito maior, pois a partir de uma base de dados de telefones, por exemplo, podem criar robôs para enviar mensagens que busquem ludibriar literalmente milhões de vítimas em potencial. (Fórum Brasileiro de Segurança Pública, 2024, p. 101).

Vejamos o gráfico exposto no Anuário de Segurança Pública de 2024:

Gráfico 01 – Crimes contra o Patrimônio no Brasil

Brasil, variação das taxas entre 2022 e 2023



Fonte: Secretarias Estaduais de Segurança Pública e/ou Defesa Social; Instituto de Segurança Pública/RJ (ISP); Polícia Civil do Estado do Acre; Polícia Civil do Estado de Alagoas; Polícia Civil do Distrito Federal; Polícia Civil do Estado de Roraima; Ministério dos Transportes/Secretaria Nacional de Trânsito – SENATRAN; Instituto Brasileiro de Geografia e Estatística (IBGE) – Censo Demográfico 2022; Banco Central do Brasil; Fórum Brasileiro de Segurança Pública.

Fonte de pesquisa: Anuário de segurança pública de 2024

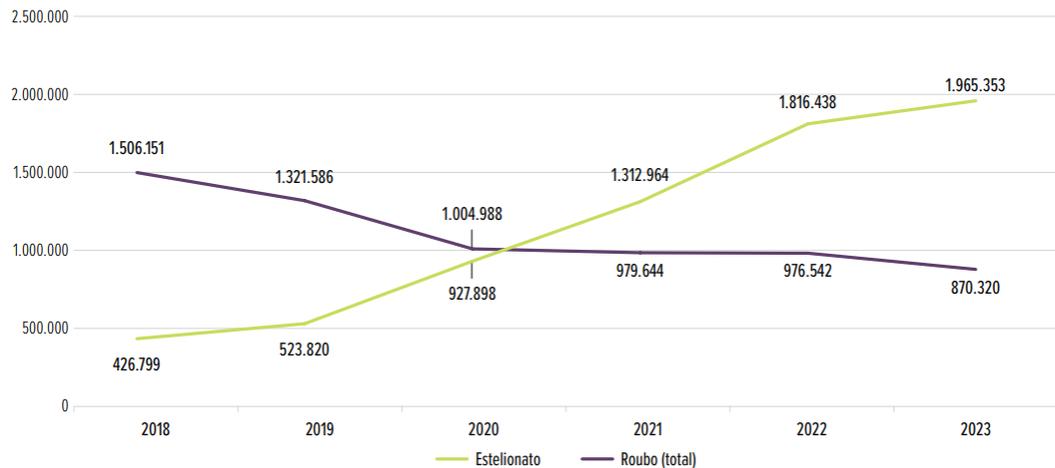
Infere-se, desta forma, que o criminoso está cada vez mais optando por um crime que normalmente não necessita de sua presença física para se obter êxito na ação, bem como abre mão de utilizar da violência ou grave ameaça, fator que normalmente gera um aumento ou agravante em sua pena. Ainda mais pelo fato de o criminoso em um estelionato virtual ter a chance de sair impune de sua conduta, muito em razão das dificuldades e burocracias que os órgãos de segurança pública têm de obterem informações sigilosas e importantes para se chegar a autoria, conforme menciona Moraes (2021, p. 14):

O anonimato parece ser o grande fator que demonstra a possibilidade de se evadir das punições, isso pois, o Estado ou o ofendido não pode buscar a punição quando não se sabe a autoria do fato criminoso. Essa impunidade é recorrente em redes sociais que não cooperem com os órgãos de justiça ou até mesmo prezem por um direito ao anonimato e extrema proteção a informações pessoais.

Fazendo um comparativo com o crime de roubo no Brasil, percebe-se que o estelionato, desde o ano de 2021, supera-o em seu número significativamente, tendo uma crescente inversamente proporcional em relação ao roubo, provando que o criminoso tem optado cada vez mais por este delito, no qual a segurança pública tem encontrado obstáculos burocráticos para elucidação criminosa, é o que nos mostra o gráfico 31 do Anuário de Segurança Pública.

Gráfico 02 – Evolução dos roubos e estelionatos

Brasil, 2018-2023



Fonte: Secretarias Estaduais de Segurança Pública e/ou Defesa Social; Instituto de Segurança Pública/RJ (ISP); Polícia Civil do Estado do Acre; Polícia Civil do Distrito Federal; Polícia Civil do Estado de Roraima; Fórum Brasileiro de Segurança Pública.

Fonte de pesquisa: Anuário de segurança pública de 2024

Este aumento exponencial vem chamando a atenção das autoridades públicas, tanto é que o legislador se preocupou com esta crescente dos estelionatos cometidos no ambiente virtual e acabou tipificando um crime específico através da Lei nº 14.155, de 2021, pela qual foi criada a figura do Estelionato Digital no Código Penal, através do artigo 171, § 2º-A, § 2º-B e § 3º, uma forma qualificada do caput no crime de estelionato, recebendo, assim, uma pena mais severa, quando cometida neste contexto.

Aliado a isto, a escassez de um contingente policial mais robusto nos estados e uma ausência de modernização na atividade de investigação criminal agrava ainda mais esse cenário, fazendo com que esta estatística cresça consideravelmente. Ainda mais que este crescimento apontado no Anuário de Segurança Pública, proporcionalmente, não acompanha o aumento do efetivo de policiais, especialmente aqueles que tenham uma capacidade mais aprimorada para lidar com crimes cibernéticos, que requer especialização e tempo fornecido pelo estado. Conforme aponta o Anuário de Segurança Pública:

É necessário reconhecer que, não obstante meritórios esforços localizados, as polícias estaduais no Brasil não possuem uma capacidade de resposta minimamente razoável para o enfrentamento ao novo cenário dos crimes patrimoniais, no qual predominam os estelionatos e os crimes cibernéticos. Faz-se urgente a modernização do arcabouço jurídico e institucional responsável por enfrentar o problema e repensar, com urgência, as prioridades de alocação dos recursos disponíveis. O fortalecimento da atividade de investigação criminal, com uma reestruturação de cargos e carreiras das Polícias Cíveis, além de uma reforma organizacional que privilegie a atividade de investigação é imperativa. A redução das burocracias da atividade investigativa e a total reformulação da formação dos policiais civis é urgente. Muitas academias de polícia hoje no Brasil estão completamente desatualizadas tanto na forma de ensinar quanto no conteúdo do que é ensinado. (Fórum Brasileiro de Segurança Pública, 2024, p. 101).

Sendo assim, no intuito de reduzir as burocracias encontradas pela segurança pública para combater o crime organizado, para que trabalhem de forma coordenada e eficiente, recentemente, em 2023, foram aprovadas as Leis Orgânicas Nacionais das Polícias Cíveis e Militares, trazendo a esperança de que estas normas gerais em âmbito nacional estabeleçam diretrizes uniformes e enérgicas no combate à criminalidade nacional, buscando a modernização e padronização das práticas policiais no intuito de mostrar ao criminoso que há uma estrutura organizacional séria no país, não deixando que a sensação de impunidade prevaleça e que realmente o crime compensa, trazendo ainda mais criminosos para o espaço virtual, o Anuário de Segurança Pública corrobora com essa afirmativa citando que:

Nessa seara, é válido ressaltar as inovações previstas nas recém aprovadas Leis Orgânicas Nacionais das Polícias Cível e Militar, que definem que as chefias e comandos das 27 Polícias Cíveis e 27 Polícias Militares precisam produzir planejamentos estratégicos e planos de gestão detalhados, com a definição de metas e indicadores de produtividade e resultado. As novas normas abrem uma enorme janela de oportunidades para inovação e mudança da cultura organizacional, na perspectiva da adoção de ferramentas modernas de gestão e planejamento, menos ancoradas em percepções morais e representações sociais acerca de como crime e criminosos precisam ser tratados. Dados e Informações validados, padronizados e transparentes são poderosas ferramentas de transformação. (Fórum Brasileiro de Segurança Pública, 2024, p. 101).

Em suma, observa-se um crescimento expressivo dos casos de estelionato no Brasil, evidenciando a adaptação do crime à era digital e as limitações das estruturas de segurança para lidar eficazmente com esse cenário. A transformação digital e o aumento das transações online criaram um ambiente propício para golpes cibernéticos, que exigem ações inovadoras e especializadas das forças policiais. É essencial que os três poderes se comprometam em modernizar e padronizar as práticas de combate ao crime, priorizando estratégias coordenadas e eficientes. Contudo, para enfrentar essa nova modalidade criminal de forma concreta, torna-se indispensável o fortalecimento do aparato investigativo e a promoção de uma formação policial atualizada e especializada nos crimes em estudo.

CONSIDERAÇÕES FINAIS

As considerações finais deste estudo expõem os resultados da pesquisa sobre a crescente incidência de estelionato no Brasil, especialmente em sua modalidade digital. Os dados do Anuário Brasileiro de Segurança Pública de 2024 evidenciam um aumento alarmante de 8,2% em relação ao ano anterior, totalizando quase 2 milhões de casos em 2023 e um impressionante crescimento de 360% nos últimos sete anos. Essa elevação está intimamente ligada à transformação digital, que, se por um lado facilitou as transações online,

por outro, também expôs as vulnerabilidades dos usuários e a atuação de criminosos mais sofisticados.

Em resposta à questão central da pesquisa, fica claro que tanto a dinâmica entre criminosos e vítimas quanto as condições propícias criadas pela era digital são fatores críticos para a consumação do estelionato. Os golpistas têm aprimorado suas estratégias de manipulação, enquanto muitos cidadãos permanecem desinformados ou despreparados para lidar com os riscos associados às transações online. A pandemia de COVID-19 acelerou essa transição, resultando em um aumento das interações digitais, o que, por sua vez, ampliou o campo de atuação dos estelionatários.

Diante desse panorama, é evidente que a segurança pública enfrenta um desafio crescente. A migração de criminosos para o ambiente digital é facilitada pela impunidade associada a esse tipo de delito, uma vez que a falta de presença física do criminoso dificulta sua identificação e captura. A legislação recente, como a Lei nº 14.155 de 2021, que tipificou o estelionato digital, é um passo importante, mas a implementação efetiva e a capacidade investigativa das polícias precisam ser urgentemente aprimoradas.

Assim, recomenda-se que futuras pesquisas explorem a eficácia das novas leis e as melhores práticas para a capacitação das forças de segurança no combate a crimes cibernéticos. É fundamental que se desenvolvam programas de educação digital para a população, visando aumentar a conscientização sobre os riscos e a prevenção de fraudes. Além disso, deve-se incentivar a colaboração entre órgãos de segurança pública e plataformas digitais, promovendo uma resposta mais ágil e integrada ao fenômeno do estelionato virtual.

Em suma, este estudo destaca a urgência de um fortalecimento das políticas públicas voltadas para a segurança digital, assim como a necessidade de uma reestruturação nas práticas policiais. Somente com uma abordagem coordenada e inovadora será possível mitigar os impactos do estelionato e garantir uma maior proteção para os cidadãos brasileiros.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Decreto – **Lei nº 1.521 de 26 de dezembro de 1951**. Altera dispositivos da legislação vigente sobre crimes contra a economia popular. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/11521.htm. Acesso em: 04 de set. 2024.

BRASIL. Decreto – **Lei nº 2.848 de 07 de dezembro de 1940**. Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 04 de set. 2024.

BRASIL. Decreto – **Lei nº 8.078, de 11 de setembro de 1990**. Proteção do consumidor e dá outras providências. Disponível em:

https://www.planalto.gov.br/ccivil_03/leis/18078compilado.htm. Acesso em: 04 de set. 2024.

BRASIL. Decreto – **Lei nº 14.155, de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Disponível

em:https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/114155.htm. Acesso em 04 de set. 2024.

CAPEZ, Fernando. **Curso de direito penal: parte especial: arts. 121 a 212.v.2**. Rio de Janeiro: Grupo GEN, 2024. E-book. ISBN 9788553622672. Disponível em:

<https://integrada.minhabiblioteca.com.br/#/books/9788553622672/>. Acesso em: 06 de set. 2024.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **18º Anuário Brasileiro de Segurança Pública**. São Paulo: Fórum Brasileiro de Segurança Pública, 2024. Disponível em: <https://publicacoes.forumseguranca.org.br/handle/123456789/253>. Acesso em: 10 de ago. 2024.

GRECO, Rogério. **Curso de Direito Penal - Vol. 2**. Rio de Janeiro: Grupo GEN, 2024. E-book. ISBN 9786559775811. Disponível

em:<https://integrada.minhabiblioteca.com.br/#/books/9786559775811/>. Acesso em: 06 de set. 2024.

MORAIS, J. A. .R no estudo em **A Criminalidade e Impunidade Frente aos Delitos Praticados no Ambiente Virtual**: disponível

em:<https://anais.unievangelica.edu.br/index.php/praxisjuridica/article/view/8143>. Acesso em 04 de set. 2024.

NUCCI, Guilherme de S. **Manual de Direito Penal**. Volume Único. Rio de Janeiro: Grupo GEN, 2023. E-book. ISBN 9786559646630. Disponível

em:<https://integrada.minhabiblioteca.com.br/#/books/9786559646630/>. Acesso em: 06 de set. 2024.

SILVA, Cristian Renner Virginio da. **A Conduta da Vítima no Delito de Estelionato Virtual: uma Análise à Luz da Teoria da Imputação Objetiva de Claus Roxin** / Cristian Renner Virginio da Silva. - Santa Rita, 2023. 75 f.

Simpósio Internacional de Análise Crítica do Direito / Jairo Néia Lima; Luiz Fernando Kazmierczak; Fernando de Brito Alves, organizadores. – 1. ed. – Jacarezinho, PR: UENP, 2023. (Anais do XII Simpósio Internacional de Análise Crítica do Direito) Vários autores
Bibliografia ISBN 978-65-00-74362-3 1. Simpósio Internacional de Análise Crítica do Direito / Jairo Néia Lima; Luiz Fernando Kazmierczak; Fernando de Brito Alves.