ESTELIONATO DIGITAL: UMA ANÁLISE CRÍTICA DA DISCIPLINA NORMATIVA, SUAS FORMAS DE CONDUTA E AS POSSÍVEIS CONSEQUÊNCIAS SOCIAIS

Rafael Lemos Garcia de Oliveira[1]
Ricardo Simões Xavier dos Santos[2]

Resumo

O presente artigo discorre sobre a figura do estelionato digital, fazendo uma análise crítica da disciplina normativa, suas formas de conduta e as possíveis consequências sociais. É notório que a atual legislação do país tem avançado, conforme mencionado, na forma que tipifica os crimes que ocorrem em meios virtuais, todavia as sanções ainda são moderadas e as normas devem avançar no sentido de impedir a prática dos crimes virtuais. Para que seja viável a hipótese narrada, o Estado tem o dever de incrementar métodos novos de apuração e averiguação e aprimorar os recursos tecnológicos e digitais que estão à disposição das autoridades responsáveis. Nesse sentido, é necessário compreender o que é o estelionato digital, suas características, maneiras de prevenção e formas em que pode aparecer no dia a dia dos usuários da rede, compactuando com a legislação penal e o cabimento de penalização para os criminosos que praticam esse crime. Por fim, conclui-se que a legislação penal brasileira vem evoluindo, mas para que alcance um nível suficiente de eficácia no combate a esse crime é necessário compreender o que é o estelionato digital, suas características, maneiras de prevenção e formas em que pode aparecer no dia a dia dos usuários da rede, compactuando com a legislação penal e o cabimento de penalização para os criminosos que praticam esse crime.

PALAVRAS-CHAVE: Internet. Crime Cibernético. Estelionato Digital. Código Penal.

[1] Graduando em bacharelado em direito pela UCSAL. E-mail: rafaell.oliveira@ucsal.edu.br

[2] Doutor em Políticas Sociais e Cidadania pela Universidade Católica do Salvador – UCSal. E-mail: ricardo.santos@pro.ucsal.br

ABSTRACT: This article discusses the figure of digital fraud, making a critical analysis of the normative discipline, its forms of conduct and the possible social consequences. It is notable that the country's current legislation has advanced, as mentioned, in the way it typifies crimes that occur in virtual media, however sanctions are still moderate and standards must advance in order to prevent the practice of virtual crimes. In order for the narrated hypothesis to be viable, the State has the duty to increase new methods of investigation and investigation and improve the technological and digital resources that are available to the responsible authorities. In this sense, it is necessary to understand what digital fraud is, its characteristics, methods of prevention and ways in which it can appear in the daily lives of network users, in agreement with criminal legislation and the appropriateness of penalizing criminals who practice this crime. Finally, it is concluded that Brazilian criminal legislation has been evolving, but in order to achieve a sufficient level of effectiveness in combating this crime, it is necessary to understand what digital fraud is, its characteristics, methods of prevention and forms in which it can appear. in the daily lives of network users, complying with criminal legislation and the appropriateness of penalizing criminals who commit this crime.

KEYWORDS: Internet. Cybercrime. Digital Fraud. Penal Code.

1 INTRODUÇÃO

No âmbito penalista são diversos os crimes que têm como objetivo a obtenção de lucros financeiros da vítima, o referido trabalho tem como objetivo abordar o estelionato digital fazendo uma análise crítica da disciplina normativa, apresentando suas formas de conduta e relacionando a suas possíveis consequências sociais.

Há uma previsão legal do Código Penal em garantir que todos os cidadãos lesados por práticas de golpes, em que são utilizados artifícios ou qualquer meio fraudulento, podem ingressar no juízo criminal a fim de prosseguirem com a punição penal e com o ressarcimento dos prejuízos.

Para breve introito, o estelionato é 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.

Dentre os crimes mais comuns no Brasil e no mundo pode-se destacar o estelionato, além do meio físico os criminosos procuram pela navegação na rede com o fito de obtenção de dados e informações das pessoas que tem perfil para serem suas possíveis vítimas, pondo em prática das mais diversas maneiras tais como ligações, mensagens, falsificação de identidade, haja vista que todos os dias, a população vive a internet, cadastrando senhas, trocando mensagens, adentrando redes sociais, fazendo negócios pela internet...

Nesse sentido, acompanhando o aumento dos usuários das redes a realização de crimes online cresceu consideravelmente, obviamente relacionado a simplicidade de manejo dos meios virtuais e pela dificuldade de identificação dos criminosos para posterior punição, haja vista ausência de legislações específicas e supressão das identidades.

A realização de golpes e fraudes cometendo ilícitos para obter vantagem sob outras pessoas é prática recorrente e por muitas vezes impune no Brasil, com o estelionato digital não é diferente.

Em sua esfera digital ele se configura quando o criminoso submete o aparelho da vítima e sincroniza-o a demais sistemas de informação ou, em outra hipótese, quando a vítima é posta em uma conjuntura de sensibilidade para obtenção de vantagem ilícita. Na atualidade é mais comum do que se imagina conhecer alguém que tenha passado por essa situação e caído nesse golpe, desde ligações de números sem chamador ou desconhecidos a e-mails/mensagens com ofertas incríveis.

Outro ponto importante que contribuiu para esse aumento, além da facilidade no manejo dos meios virtuais foi o advento da pandemia do Covid-19, as práticas desses crimes se multiplicaram, haja vista que, relevante porcentagem da população tanto brasileira quanto mundial, se viu obrigada a passar mais tempo em casa, o que, em consequência, ampliou o número de pessoas online, acessando a rede. Neste liame, os criminosos têm agido cada vez mais e feito várias vítimas no mundo virtual.

Para que o crime possa ser classificado como estelionato digital é imprescindível que a entrega das informações pela vítima seja de forma voluntária, haja vista que a obtenção dos dados se deu por outros meios, o crime pode ter outra classificação, tal como “furto mediante fraude eletrônica”.

Dentre as principais vítimas desse crime tão comum na atualidade estão as pessoas desatentas e que não tomam total atenção para se esquivar dos estelionatários, seguindo as hipóteses de compra e venda pela internet não verificando a fonte, se é de confiança etc., links enviados de números aleatórios possibilitando o acesso do criminoso a rede da vítima entre outros...

A despeito da clara regulação e evolução da internet e redes sociais, os conselhos e observações para a premeditação dos crimes digitais em geral continua sendo de cuidado e cautela com os dados pessoais e sua divulgação, ainda com o remetente e usuários/links que adentra. É necessário que sempre pense que tudo que identifique quem você é ou que busque saber informações que só você teria acesso são o alerta inicial para entender se não se está diante de uma possível tentativa de estelionato digital.

É notório que a atual legislação do país tem avançado, conforme mencionado, na forma que tipifica os crimes que ocorrem em meios virtuais, todavia as sanções ainda são moderadas e as normas devem avançar no sentido de impedir a prática dos crimes virtuais. Para que seja viável a hipótese narrada, o Estado tem o dever de incrementar métodos novos de apuração e averiguação e aprimorar os recursos tecnológicos e digitais que estão à disposição das autoridades responsáveis.

Nesse sentido, é necessário compreender o que é o estelionato digital, suas características, maneiras de prevenção e formas em que pode aparecer no dia a dia dos usuários da rede, compactuando com a legislação penal e o cabimento de penalização para os criminosos que praticam esse crime.

Assim, as perguntas que ficam são quais as formas de conduta do estelionato digital e seus impactos na sociedade, além do questionamento acerca das normas brasileiras, nosso sistema jurídico atual contempla qual espécie de responsabilização para o crime de estelionato digital, alinhado a isso, como o Estado Democrático Brasileiro pode melhorar para combater o aumento desse crime.

No presente artigo, seguindo após a introdução para o capítulo “2” onde serão apresentadas as condutas do estelionato digital, seus conceitos prévios e formas apresentadas, a diferença entre o estelionato e outros crimes contra o patrimônio e

sua forma de proliferação pela rede mediante sites falsos, mensagens e e-mails. O capítulo “2” contém ainda um subtópico “2.1” onde serão analisadas as consequências sociais advindas da conduta do estelionato digital, desde a inovação dos criminosos partindo para o meio digital até os “traumas” das vítimas e sua repercussão na sociedade.

Já no capítulo “3” será amplamente explicada a quem deve ser dirigida a responsabilidade pelo crime do estelionato digital, no âmbito jurídico, já que o crime na grande maioria das vezes tem por conclusão a “fuga” do criminoso pelo meio cibernético. Ainda no capítulo “3” serão exploradas, mediante subtópico “3.1”, as normas jurídicas atualizadas e formas de punição do crime tendo relação direta com a ampla possibilidade de escape do criminoso.

Por fim, em capítulo “4”, será demonstrado o histórico da prática do estelionato digital, sua evolução paralela ao avanço da tecnologia na sociedade e os reflexos da Lei 14.155, instituída em 2021 especialmente para tornar mais grave a pena de estelionato cometido de forma eletrônica pela internet, frente ainda a vulnerabilidade da vítima. Seguidos da conclusão e as referências bibliográficas.

De certo, cumpre-se destacar que a pesquisa em questão, valeu-se do método da revisão bibliográfica de trabalhos científicos atualizados das áreas penal e constitucional, frente às questões sociais, publicadas em periódicos nacionais e internacionais, qualificados como publicações de A1, assim como B1. Além de importantes nomes do cenário retrato, ao passo que se cita Rogério Greco e Fabio Barbosa Chavez, bem como análise jurisprudencial e legislativa da lei 14.155. Compreende-se então, que a escolha metodológica se justifica de base teórica, fundada em estudos atualizados sobre o estelionato digital, suas formas de conduta e as consequências sociais.

O foco da pesquisa bibliográfica foi de apresentar informações e dados específicos sobre a evolução dos crimes digitais, exibindo o progresso do direito penal frente os crimes digitais, através da análise filosófica e de referenciais teóricos de artigos, códigos e outros trabalhos sobre a mesma questão jurídica. Assim, o método empregado é de leitura e análise de material doutrinário especializado já existente sobre o tema de Direito Penal, tal como de jurisprudência, dados, legislação e artigos científicos.

2 CONDUTA DO ESTELIONATO DIGITAL: CONCEITOS PRÉVIOS, DISCUSSÕES INICIAIS E FORMAS APRESENTADAS.

O termo estelionato está disposta no Art. 171 do Código Penal como:

> Art. 171. Obter, para si ou para outrem, vantagem ilícita em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: pena – Reclusão, de 1 (um) a 5 (cinco) anos, de multa.

Trata-se de crime contra o patrimônio onde a legislação penal visa proteger a inviolabilidade patrimonial orientada pela prática de atos que visam enganar a vítima e beneficiar o agente (CUNHA, 2019, p. 345).

Assim, pode-se inferir que a diferença entre o estelionato e os diversos crimes contra o patrimônio, ou seja, crimes que tenham por objetivo atentar contra o patrimônio de uma pessoa ou organização, é que no estelionato não é utilizada a força para obtenção de “vantagem”. É sabido, portanto, que essa atitude é conhecida há muitos anos, de modo que Greco cita que:

> Desde que surgiram as relações sociais, o homem se vale da fraude para dissimular seus verdadeiros sentimentos e intenções para, de alguma forma, ocultar ou falsear a verdade, a fim de obter vantagens que, em tese, lhe seriam indevidas (GRECO, 2019, p. 228).

Ressalta-se que o crime existe apenas na modalidade dolosa, sem previsão na forma culposa.

A respeito da expressão “vantagem ilícita”, Fernando Capez (2020) ensina que, esta, trata-se do objeto material do crime e, caso o agente esteja agindo em razão de uma vantagem devida, a conduta é tipificada como exercício arbitrário das próprias razões, delito previsto no art. 345, do Código Penal.

De acordo com o que se retira do artigo 171, do supramencionado dispositivo legal, o estelionato pode ser cometido mediante artificio, ardil ou qualquer outro meio fraudulento. Em relação ao termo “artificio”, o doutrinador Júlio Fabbrini Mirabete ensina o seguinte:

> “o artifício existe quando o agente se utilizar de um aparato que modifica, ao menos aparentemente, o aspecto material da coisa, figurando entre esses meios o documento falso ou outra falsificação qualquer, o disfarce, a modificação por aparelhos mecânicos ou elétricos, filmes, efeitos de luz etc.” (MIRABETE, 2021, pag. 325).

Em sua modalidade digital o estelionato ocorre através de sites falsos, mensagens e até e-mail, sendo prioritariamente focado no âmbito virtual. É bastante

normal que o consumidor busque virtualmente os mesmos bens desejados fisicamente, mas com a comodidade de não se deslocar e em grande maioria dos casos a acessibilidade com preços menores, levando a promessa da oferta muitas vezes a encantar o consumidor que não percebe a fraude.

Dentre as formas de conduta do referido crime podem ser listadas as mais comuns sendo: vendas falsas em sua maioria quando os estelionatários oferecem serviços ou produtos inexistentes em redes sociais e/ou sites e links de comércio eletrônico; “phishing”, uma artimanha utilizada pelos criminosos para enganar os usuários e conseguir informações privadas, tais como senhas, detalhes de cartões de crédito, comumente realizado por meio do envio de mensagens eletrônicas se passando por instituições de confiança, pode ser realizado por sites e por redes sociais também, mas sempre com o intuito de prejudicar e obter vantagem, “vishing” popularmente conhecido por “phishing por voz” quando o ato é realizado por ligações ou envio de áudios com o mesmo intuito de ludibriar a vítima, mas para divulgar dados pessoais, “smishing” realizada também por mensagem, mas nessa modalidade a vítima é provocada a acessar link que corrompe seu aparelho, e por último os golpes de investimentos fraudulentos que podem acontecer de diversas maneiras, tais como promessas de retornos financeiros utopicamente elevados e esquema de pirâmides, esses golpistas beneficiam-se da leiguice de suas vítimas no âmbito de investimento financeiro com falsas promessas de enriquecimento acelerado para enganá-las.

No Art. 171 do Código Penal, o estelionato possui a pena de reclusão de 1 a 5 anos e multa. Diante disso, o crime admite suspensão condicional no processo de acordo com o art. 89, § 1ª, da Lei dos Juizados Especiais - Lei n. 9099/95:

> Art. 89. Nos crimes em que a pena mínima cominada for igual ou inferior a um ano, abrangidas ou não por esta Lei, o Ministério Público, ao oferecer a denúncia, poderá propor a suspensão do processo, por dois a quatro anos, desde que o acusado não esteja sendo processado ou não tenha sido condenado por outro crime, presentes os demais requisitos que autorizariam a suspensão condicional da pena (art. 77 do Código Penal).

Conforme dito, o crime de estelionato digital, no sistema jurídico atual do Brasil, é apreciado no âmbito do Direito Penal o qual pressupõe responsabilização penal para esse tipo de ato, o qual era equiparado ao crime de estelionato, previsto no artigo 171 do Código Penal, ocorre que ainda no caminhar para a especificação do crime de estelionato na modalidade digital foi introduzida a Lei 12.737/2012, ou como é popularmente conhecida a “Lei Carolina Dieckmann”, que surgiu após um incidente

em que a atriz teve seu aparelho pessoal invadido e com isso o vazamento de fotos íntimas na rede, mediante ainda tentativa de extorsão.

Na época em questão os criminosos seriam apenas denunciados pelo crime de tentativa de extorsão, haja vista ausência de legislação específica quanto aos crimes digitais, assim vários projetos de lei foram analisados para tentar tipificar condutas para crimes semelhantes ao sofrido pela atriz e findada essa fase foi sancionada a Lei 12.737/2012 que entrou em vigor em 02 de abril de 2013.

A lei visava combater o vazamento de informações pessoais dos usuários das redes, zelando pela proteção da privacidade dos mesmos, ainda acrescentou ao Código Penal, mais especificamente no Decreto-Lei 2848, os artigos 154-A e 154-B.

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

A lei se demonstrou efetiva a época da sanção sendo citada como um marco legislativo por muitos autores, desde que entrou em vigor a invasão de computadores, celulares, tablets...no geral dispositivos informáticos alheios passou a ser crime.

Cabe destacar que execução da lei e a responsabilização dos golpistas submete-se a conduta das autoridades capazes, para investigar, processar e julgar os casos de estelionato digital, como a polícia e o Poder Judiciário.

2.1 ANÁLISE ACERCA DAS EVENTUAIS CONSEQUÊNCIAS SOCIAIS ADVINDAS DA CONDUTA DO ESTELIONATO DIGITAL.

A sociedade está cada vez mais conectada e as redes sociais têm uma função muito importante nessa interação, vez que o ser humano sempre precisou de convívio social. Assim, tais ferramentas estão presentes na vida de muitos brasileiros e esse ambiente digital, como já evidenciado, tornou-se, também, um meio para a prática de crimes, seja pela facilidade de acesso e/ou pelo grande número de usuários.

Na atualidade existe uma grande facilidade na obtenção de produtos, sendo de maneira virtual, de modo que não existe mais a necessidade do consumidor se deslocar até o fornecedor para adquirir o produto, nesta feita, é notório que a compra virtual vem amadurecendo cada vez mais, o que consequentemente ocasiona um aumento dos crimes cibernéticos. Nesse contexto, Chaves e Teixeira destacam que:

> Com a investigação correta é possível localizar e punir os criminosos que causaram prejuízo a essa nova espécie de consumidores. Todavia, no mesmo ritmo que a internet evolui, os fraudadores também se renovam com novas modalidades de golpes, alguns tão específicos que são até difíceis de definir qual a punição correta a ser aplicada (CHAVES e TEIXEIRA, 2019, p. 119).

Conforme já citado a inovação dos criminosos acompanha em paralelo o avanço da tecnologia pela sociedade, de modo que muitos usuários têm a sensação de que a internet é “terra sem lei” fomentando sua “liberdade tecnológica” em pequenos delitos, tais como injúria, difamação... Ao passo em que não imaginam ter a sua responsabilidade realmente comprovada, agindo por trás da tela do celular ou computador.

Perpassando por isso os criminosos buscam a obtenção de vantagem ilícita e veem na internet uma oportunidade recheada de opções, possuídos pela sensação de impunidade e munidos das mais diversas artimanhas para concluir seu objetivo. Cumpre ressaltar que sociedade caminha para um futuro mais tecnológico e os criminosos “surfam nessa onda”.

A cada dia que passa resta mais rudimentar os métodos de pagamento por cédulas ou moedas, a trajetória da população tem destino eletrônico, de modo que é fato notório o quão comum se tornaram os sistemas de pagamento eletrônico, estando já alguns mais rudimentares como a transferência “TED”.

A popularização dos sistemas de pagamento eletrônico, a exemplo do “pix”, propicia diariamente um combate necessário entre as autoridades e os golpistas. Já é rotina na sociedade a divulgação de novos meios de golpes cibernéticos com o fito de alertar os usuários a se precaverem mais, infelizmente nem sempre todo cuidado é tomado e as consequências podem ser desastrosas para os consumidores da rede.

O prejuízo causado a essa nova espécie de consumidores afeta tanto de forma direta as vítimas quanto a sociedade, de maneira geral. Dentre as consequências sociais advindas dessa conduta resta mister destacar o impacto financeiro nas vítimas, de forma direta, que podem encarar perdas financeiras o que acarreta

problemas emocionais e instabilidade, perda de confiança no meio digital para compras que também gera impacto na maneira como as pessoas conduzem negócios online.

Além do consumidor direto, as instituições financeiras também sofrem em muitos casos ressarcindo o valor perdido por seus clientes lesados, arcando com o custo de fraude e também no investimento em segurança virtual, mesmo ainda tendo um receio a implantação dos pagamentos digitais buscando ao máximo reforçar sua segurança desde confirmação por “face id” quanto senhas regularmente trocadas e “tokens digitais”, sempre tentando confirmar que é realmente o usuário da conta quem realmente está fazendo a operação e não um terceiro. Frisa-se que essas consequências sociais acarretam, num todo, impacto na economia.

Felizmente, não são somente os consumidores que passam pelo processo de consequências negativas, mas também os fraudadores. Mesmo diante da crescente a qual ocorre o “fenômeno” do estelionato digital, os criminosos não restam imunes a responsabilização pelo seu crime. Conforme será demonstrado no presente artigo, a legislação do país delimita o crime e suas consequências, assim como as penalidades que podem levar os fraudadores a condenação pelas atividades ilícitas.

Nesse sentido, o avanço da tecnologia com o passar dos tempos corroborou indiretamente para que os criminosos inovassem seus meios ilícitos para obtenção de vantagens, causando diversos impactos na sociedade que não teriam como ser positivos, sendo alguns dos principais o prejuízo financeiro as vítimas; perda de confiança na segurança online e transações digitais, além do choque nos sistemas judiciais, de segurança e nas bases digitais o que consequentemente requer mecanismos e investimentos relevantes de atribuição das empresas e do judiciário.

Sendo assim, infere-se que ainda existe certa dificuldade para identificação dos golpistas o que, alternativamente, tem relação com a legislação brasileira que tem avançado na tipificação dos crimes cibernéticos, todavia as sanções ainda são moderadas e as normas devem acompanhar no sentido de bridar a prática desses crimes na modalidade virtual.

3 A RESPONSABILIZAÇÃO DO CRIME DE ESTELIONATO DIGITAL NO ÂMBITO JURÍDICO.

É claro que a internet e toda a esfera digital não foi inserida na sociedade com o intuito ou sequer resguarda em relação a possibilidade do advento de crimes em paralelo a isso, mas como toda imprevisão, a criminalidade evoluiu em conjunto deixando cada vez mais vulnerável a segurança dos usuários na rede, como amplamente demonstrado no presente trabalho, os golpes digitais se aperfeiçoam com o passar dos anos, com ênfase para o estelionato que conta hoje com diversos tipos de obtenção de vantagem ilícita na sua modalidade digital.

A internet tornou-se essencial na rotina da população, interligando usuários e pessoas conectadas a rede, assim, como bem destacou Uchoa de Brito:

> (...) O problema da internet passou a ser identificado quando a tecnologia incrementou e complicou as relações sociais consideradas, até então, pacíficas e controladas, possibilitando algumas experiências socialmente desagradáveis e indesejadas, como a sua utilização para a prática de crimes, e a criação de novos contatos que colocam em risco bens que ainda não tiveram sua relevância reconhecida pelo Direito. (BRITO, 2013, p. 9).

Assim, a prática do estelionato na modalidade virtual cresceu ao longo dos anos, sempre com a tentativa em paralelo do Direito Penal de acompanhar para poder punir em cerceamento legislativo, com projetos de lei, inovações e acréscimos a legislações já vigentes.

Quanto a responsabilização do crime em questão torna-se direta em relação ao Autor, sendo aferida pelo Estado, mesmo em sua modalidade digital, haja vista que tem o encargo de combater, controlar e reprimir tais práticas tanto no mundo “real” quanto no ambiente digital, além de ser responsável por tutelar a convivência e atuação neste âmbito cibernético.

Além da responsabilização direta quanto ao autor do delito, muitas vezes a responsabilidade também recai de forma subjetiva ou objetiva para um terceiro da relação que deveria zelar pela segurança dos dados pessoais do usuário, grandes exemplos são os de vazamento de dados bancários online após invasão por hackers, recaindo responsabilidade também para os bancos que deveriam proteger o consumidor.

> APELAÇÃO CÍVEL. NEGÓCIOS JURÍDICOS BANCÁRIOS. AÇÃO DE INDENIZAÇÃO POR DANOS MATERIAIS. RESSARCIMENTO DE VALORES. TRANSAÇÃO BANCÁRIA REALIZADA DE FORMA FRAUDULENTA POR TERCEIROS. INTERNET BANKING. RESPONSABILIDADE DO BANCO. SUMULA 479 DO STJ. SENTENÇA MANTIDA. As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias. Súmula 479 do STJ. Art. 14 do CDC. Para

> responsabilização do prestador de serviços a existência de culpa ou dolo, exige-se apenas a conduta ilícita e a existência de dano, bem como nexo de causalidade entre eles. Caso. Autora que foi vítima de estelionato praticado por terceiro. Empréstimo autorizado pela instituição financeira. Nesse ponto, desimporta que a fraude tenha se perpetrado através dos canais de atendimento via internet (internet banking), porquanto a parte autora negou ter sido a autora dos saques, e o banco não se desincumbiu do ônus de demonstrar a regularidade das transações impugnadas pelo cliente. NEGARAM PROVIMENTO AO APELO. UNÂNIME.

Entre outros exemplos de golpes como os já citados “phishing”, “vishing” e “smishing” que buscam a obtenção de vantagem ilícita frente as vítimas, muitas vezes fazendo uso de um terceiro como ponte para alçar seu objetivo fraudulento, ocorre que, como mencionado, mesmo esse terceiro não tendo o dolo na prática do crime deve garantir a segurança e impermeabilidade do seu sistema para que isso não ocorra, contando com a obrigação de assegurar os direitos do consumidor e usuário. Este é o entendimento das jurisprudências pátrias:

> RECURSO INOMINADO. AÇÃO DECLARATÓRIA DE INEXISTÊNCIA DE DÉBITO C/C INDENIZAÇÃO POR DANOS MORAIS. PRELIMINAR DE VIOLAÇÃO AO PRINCÍPIO DA DIALETICDADE. INOCORRÊNCIA. BANCÁRIO. TRANSFERÊNCIA DE VALORES REALIZADA POR TERCEIRO. FRAUDE EVIDENCIADA. CULPA DA VÍTIMA NÃO CONFIGURADA. INSTITUIÇÃO FINANCEIRA QUE NÃO APRESENTOU PROVAS ACERCA DA SEGURANÇA, AUTENTICAÇÃO OU IDENTIFICAÇÃO DA OPERAÇÃO. FALHA NA PRESTAÇÃO DO SERVIÇO CONFIGURADA. RESPONSABILIDADE OBJETIVA DO BANCO. APLICAÇÃO DA SÚMULA 479 DO STJ. RESTITUIÇÃO DEVIDA. AUSÊNCIA DE SOLUÇÃO ADMINISTRATIVA. DANO MORAL CONFIGURADO NO CASO CONCRETO. QUANTUM ARBITRADO EM R$ 2.000,00 (DOIS MIL REAIS) QUE COMPORTA MAJORAÇÃO PARA R$ 3.000,00 (TRÊS MIL REAIS). OBSERVÂNCIA AOS PRINCÍPIOS DA PROPORCIONALIDADE E RAZOABILIDADE. SENTENÇA PARCIALMENTE REFORMADA. Recurso da autora conhecido e provido.Recurso do réu conhecido e desprovido. (TJPR - 1ª Turma Recursal - 0003317-67.2020.8.16.0136 - Pitanga - Rel.: JUIZ DE DIREITO DA TURMA RECURSAL DOS JUIZADOS ESPECIAIS NESTARIO DA SILVA QUEIROZ - J. 23.05.2022)
> (TJ-PR - RI: 00033176720208160136 Pitanga 0003317-67.2020.8.16.0136 (Acórdão), Relator: Nestario da Silva Queiroz, Data de Julgamento: 23/05/2022, 1ª Turma Recursal, Data de Publicação: 23/05/2022)

Ressalta-se que o estelionato na sua modalidade digital é considerado crime de ação penal pública incondicionada, ou seja, a responsabilidade para conduzir o procedimento é do Ministério Público, independente de manifestação de vontade da vítima, a natureza dessa ação ressalva a relevância de tratar esse delito de forma mais eficaz, independente da vontade da vítima de ver o autor do crime responsabilizado, com o fito de preservar a ordem social e diminuir o índice de novos casos.

Nesse sentido, cumpre destacar que mesmo a responsabilidade do crime ser direta em relação ao Autor, também pode abranger mais partes do processo dependendo da especificada do caso. A jurisprudência entende que a responsabilidade não é apenas do Estado, mas também da empresa, entidade ou qualquer terceiro que tenha a obrigação de tornar o ambiente digital seguro para o usuário.

3.1 CONCEPÇÃO DAS NORMAS JURÍDICAS ATUALIZADAS E FORMAS DE PUNIÇÃO DO CRIME DO ESTELIONATO DIGITAL.

Como já explicitado, um grande fator que desencadeou o aumento da efetivação do crime em questão foi a pandemia, de modo que, com o advento do Covid-19, foi necessário que a população se protegesse em suas casas para corroborar com o distanciamento social e assim evitar a proliferação do vírus, ocorre que em contrapartida a isso foi destaque a aproximação online dos usuários que culminou em oportunidade para os criminosos inovarem suas artimanhas, contando com a suposta sensação de anonimato.

O crime de estelionato digital, no sistema jurídico atual do Brasil, é apreciado no âmbito do Direito Penal, o qual pressupõe responsabilização para esse tipo de ato, que era equiparado ao crime de estelionato, previsto no artigo 171 do Código Penal.

A Lei 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann, entrou em vigor como uma tentativa inicial de tipificar a conduta dos crimes na modalidade virtual para proteção dos dados pessoais da população em face aos criminosos virtuais, ocorre que com o passar dos anos se mostrou necessária a inclusão de novas medidas frente a progressão da criminalidade no país, em específico os crimes virtuais.

Para combater essa crescente negativa no âmbito jurídico nacional entrou em vigor a lei 14.155/21, de 27 de maio de 2021, que incluiu e modificou alguns parágrafos no supramencionado dispositivo legal, alterando algumas regras para julgar o crime.

> Art. 1º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar com as seguintes alterações:
> “Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:

> § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.
> § 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso:
> I – 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;
> II – Aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável. Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
> § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.

Dentre as alterações, foram incluídos os § § 2º-A e 2º-B, que tratam de fraude eletrônica, sendo o § 2º-A qualificadora para o crime de estelionato que não é praticado na modalidade presencial, ou seja, quando a frade é cometida com uso de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de reses sociais ou qualquer outro meio fraudulento análogo.

> Fraude eletrônica
> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.
> § 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.
> Estelionato contra idoso ou vulnerável
> § 4º A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso.
> Art. 2º O art. 70 do Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), passa a vigorar acrescido do seguinte § 4º:
> § 4º Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção.” (NR).

Nesse sentido, observa-se que foram elencados os crimes específicos mediante fraude eletrônica objetivando tornar mais rigorosa a lei, ainda tentando acompanhar o avanço da criminalidade. Frisa-se que a Lei 14.155/21 deu ênfase também ao aumento da pena para esse crime na modalidade virtual, com pena de reclusão de 4 a 8 anos e o aumento de 1/3 ao dobro da pena acaso o crime seja praticado contra idoso ou vulnerável, com expectativa para prejudicar a prática delituosa.

Cabe destacar também a alteração quanto a competência para apuração do estelionato por fraude mediante cheque ou transferência bancária, o código de processo penal previa que a competência era do local do banco sacado, o que muitas vezes dificultava a apuração do crime, até pela localização da vítima que nem sempre residia no mesmo local do banco sacado, competência esta alterada para o domicílio da vítima pela Lei 14.155/21.

Por fim, a execução da lei e a responsabilização dos golpistas submete-se a conduta das autoridades capazes, para investigar, processar e julgar os casos de estelionato digital, como a polícia e o poder judiciário.

4 O HISTÓRICO DA PRÁTICA DO ESTELIONATO DIGITAL E OS REFLEXOS DA LEI 14.155 FRENTE A VULNERABILIDADE DA VÍTIMA.

Como já demonstrado, o estelionato digital foi uma modalidade que cresceu esporadicamente com o advento da internet e o constante avanço da tecnologia, mas também teve um de seus marcos recentemente, em 2020, com crescimento exponencial pela pandemia da covid 19 que possibilitou mais “vítimas” online.

Relativizando em números, o país registrou um aumento ainda mais expressivo que o estelionato comum quando em sua modalidade virtual, com direta relação a pandemia, em 2021 houve 120.470 (cento e cinto mil, quatrocentos e setenta) casos registrados, já em 2022 foram registrados 200.322 (duzentos mil, trezentos e vinte e dois) casos, um aumento de 66,2% (sessenta e seis virgula dois por cento) de acordo com os dados do Fórum Brasileiro de Segurança Pública (FBSP).

Foram registrados em 2021 115 (cento e quinze) estelionatos a cada 100 (cem) mil habitantes no país, já no ano seguinte foram registrados 189,9 (cento e oitenta e nove virgula nove), um aumento de 65,1% (sessenta e cinco vírgula um porcento), ainda de acordo com a FBSP o estado que detém o recorde de casos registrados de estelionato em sua modalidade digital é Santa Catarina, com 64.230 (sessenta e quatro mil, duzentos e trinta) registros em 2022 o que representa 32% (trinta e dois porcento) dos casos do país, ressalvando que Bahia, Ceará, Rio de Janeiro, Rio Grande do Norte, Rio Grande do Sul e São Paulo não tinham ou não disponibilizaram dados.

Cabe destacar que, além de Santa Catarina, tiveram relevantes aumentos Minas Gerais que passou de 25.574 (vinte e cinco mil, quinhentos e setenta e quatro)

casos em 2021 para 35.749 (trinta e cinco mil, setecentos e quarenta e nove) em 2022, um aumento de 49,4% (quarenta e nove vírgula quatro porcento), Distrito Federal que passou de 10.049 (dez mil e quarenta e nove) casos em 2021 para 15.580 (quinze mil, quinhentos e oitenta) em 2022, registrando um aumento de 55% (cinquenta e cinco porcento), e o Espírito Santo que passou de 10.545 (dez mil, quinhentos e quarenta e cinco) casos em 2021 para 15.277 (quinze mil, duzentos e setenta e sete) casos em 2022, o que resultou em um aumento de 44,8% (quarenta e quatro vírgula oito por cento).

Dentre todos esses dados disponibilizados pela FBSP cabe destacar por fim os Estados que mais sofreram variações em seus índices, quais sejam Roraima que passou de 59 (cinquenta e nove) casos em 2021 para absurdos 759 (setecentos e cinquenta e nove) em 2022 acarretando um aumento de 1.186% (mil, cento e oitenta e seis por cento) e Goiás com um aumento de 1.041% (mil e quarenta e um porcento), passando de 128 (cento e vinte e oito) casos em 2021 para 1.461 (mil, quatrocentos e sessenta e um) casos em 2022.

Ainda sobre o marco recente que corroborou com a prática do referido delito é reiterado pelo Fórum Brasileiro de Segurança Pública (FBSP) que:

> A digitalização das finanças, de serviço e do comércio, especialmente impulsionada durante o período pandêmico, contribui com a formação de um ambiente propício ao desenvolvimento de modalidades criminais que exploram vulnerabilidade nestes segmentos. (FBSP 2022, p. 6).

Conforme já citado, a modalidade de estelionato digital foi inserida ao Código Penal em meados de 2021 pela Lei nº 14.155/21 que também especificou o estelionato praticado na modalidade digital, por meio cibernético. Essa lei trouxe novidades legislativas que no geral foram positivas com relação a vulnerabilidade da vítima.

Destarte podemos citar que invadir dispositivo informático de uso alheio, ressalvando que conectado ou não a internet, com o fim de obter vantagem ilícita terá pena de reclusão de 4 (quatro) a 8 (oito) anos e multa, com suas devidas especificações, demonstrando assim a preocupação do legislador com as vítimas que infelizmente só estavam crescendo no país e isso refletiu no agravamento da pena que antigamente era disposta no crime de invasão de dispositivo informático, criando uma resistência ao criminoso na medida em que vê o crime como algo mais grave, mediante nova pena mais severa.

Ainda quanto aos reflexos dessa lei frente a vulnerabilidade da vítima podem-se listar os agravantes trazidos em sua redação quanto ao furto, com pena de reclusão de 4 a 8 anos, para o crime nessa modalidade realizado com o uso de dispositivos eletrônicos, conectados ou não a internet, por meio de uso de sistemas invasores ou violação de senha, além do agravamento se praticado contra idosos ou vulnerável com consequente aumento de pena de 1/3 ao dobro, ainda na hipótese de ser praticado por servidor fora do território nacional aumenta a pena de 1/3 (um terço) a 2/3 (dois terços).

Quanto ao estelionato também tornou-se agravante o furto qualificado no âmbito cibernético, com igual pena de reclusão de 4 (quatro) a 8 (oito) anos, além de possível multa e pode ter pena aumentada de 1/3 (um terço) a 2/3 (dois terços) acaso seja praticada por servidor fora do território nacional e acaso praticada contra idoso ou vulnerável poderá ter a pena aumentada de 1/3 (um terço) ao dobro.

Por fim, no que tange a invasão de aparelhos para obtenção de dados, a lei passou de detenção de 3 (três) meses a 1 (um) ano para reclusão de 1 (um) a 4 (quatro) anos. Ainda na hipótese de resultar em obtenção de informações sigilosos pode ser majorada de reclusão de 2 (dois) a 5 (cinco) anos e multa, com agravante de 1/3 (um terço) a 2/3 (dois terços) caso ocorra prejuízo econômico decorrente da invasão.

Assim, as novidades legislativas trazidas pela lei confortam brasileiros que podem ser vítimas de criminosos fora do território nacional, o que é plenamente possível pelo advento da internet e também a população mais velha que, em suma maioria, não tem familiaridade com as ferramentas e linguagens online, não tendo manejo e trato com os meios digitais o que por muitas vezes os torna os principiais focos dos criminosos pela “facilidade” e “inocência” desses usuários em específico, assim como os vulneráveis.

Portanto, resta claro que o legislador buscou efetivamente ampliar a guarda dos direitos, de modo a, buscar uma equidade entre diversos grupos de pessoas/possíveis vítimas, resultando em maior segurança, de modo que passa a observar significativas mudanças objetificando proteger os direitos do usuário e penalizando de forma mais grave os criminosos.

5 CONCLUSÃO.

O presente artigo, por meio da análise de dados estatísticos, legislação e julgados, buscou tecer uma análise crítica da disciplina normativa do estelionato digital, suas formas de conduta e as possíveis consequências sociais.

Demonstrando que a sociedade está cada vez mais conectada e as redes sociais têm uma função muito importante nessa interação, ocorre que o aumento desenfreado de pessoas conectadas à internet propiciou um ambiente para prática de crimes e com diversas possibilidades de artimanhas dos criminosos, que enxergam a internet como “terra sem lei”, para obtenção da vantagem ilícita virtualmente, caracterizando o estelionato digital.

Dentre as diversas artimanhas utilizadas pelos estelionatários destacarm-se o “phishing”, utilizada para enganar os usuários e conseguir informações privadas, “vishing” popularmente conhecido por “phishing por voz” quando o ato é realizado por ligações ou envio de áudios com o mesmo intuito de ludibriar a vítima, mas para divulgar dados pessoais e “smishing” modalidade em que a vítima é provocada a acessar link que corrompe seu aparelho, além de outros golpes como investimentos fraudulentos, promessas de retornos financeiros utopicamente elevados e esquema de pirâmides, esses golpistas beneficiam-se da leiguice de suas vítimas no âmbito de investimento financeiro com falsas promessas de enriquecimento acelerado para enganá-las.

Assim, restou demonstrado que os golpistas tem o mesmo fito, qual seja a obtenção da vantagem ilícita fazendo uso do ambiente cibernético, enquadrando-os no âmbito de estelionatários digitais.

Nesta senda, ainda não existia um enquadramento específico para conter o avanço do referido ilícito que muitas vezes poderia ser caracterizado como tentativa de extorsão ou crimes análogos o que obrigou o poder legislativo a se atualizar. Para “frear” o avanço do crime foi introduzida a Lei 12.737/2012, popularmente conhecida por “Lei Carolina Dieckmann”, que surgiu após um incidente em que a atriz teve seu aparelho pessoal invadido e com isso o vazamento de fotos íntimas na rede.

A introdução da Lei “Carolina Dieckmann” mostrou-se muito importante por iniciar a caminhada rumo a tipificada do crime de estelionato em sua modalidade digital, ocorre que a tecnologia seguiu se modernizando trazendo novas oportunidades para inovação dos criminosos que vivem as sombras da internet. Com o estabelecimento de modalidades de transferência eletrônica como “TED” e “PIX”

tornou-se cada vez mais comum o embate entre as autoridades e os golpistas, já demonstrando a necessidade de nova atualização da legislação atinente ao tema.

Quanto a responsabilidade do crime no âmbito jurídico restou pacificado pelas jurisprudências pátrias que torna-se direta em relação ao Autor, sendo aferida pelo Estado que tem o dever de tutelar a convivência no âmbito cibernético. Cumpre destacar que nem sempre a responsabilidade é exclusiva do Autor, podendo recair de forma subjetiva ou objetiva para um terceiro da relação que deveria zelar pela segurança dos dados pessoais do usuário, tais como bancos, tomadores de serviço...

O marco de crescimento registrado no crime de estelionato na sua modalidade virtual foi durante a pandemia de covid 19, época em que foi necessário a reclusão da população em casa o que gerou aumento exponencial de usuários online na rede e, em paralelo, oportunidade para os criminosos inovarem suas artimanhas.

Para combater essa crescente negativa no âmbito jurídico nacional entrou em vigor a lei 14.155/21, de 27 de maio de 2021 trazendo enrijecimento das penas e tipificação de novos crimes, como estelionato contra idoso ou vulnerável e fraude eletrônica, intentando ainda em penas mais rigorosas que podem ser alongadas a depender do caso e alteração de competência para estelionato por fraude mediante cheque ou transferência bancária, submetendo a execução da lei e responsabilização dos golpistas a conduta das autoridades capazes.

O que se conclui é que, com o passar dos anos as leis e medidas tomadas se tornam ultrapassadas vide o “aperfeiçoamento” dos criminosos, portanto, com o fito do controle do Estado se tornar uma manutenção mais célere se mostrou necessário inserção de um sistema de inovação e renovação legislativa.

Ora, restou comprovado que o âmbito jurídico sempre buscou acompanhar a inovação criminosa trazendo atualizações a legislação para coibir a progressão desses ataques criminosos, mas igualmente restou comprovado que apenas acompanhar não está mais sendo o suficiente, tornando tendência o adiantamento aos movimentos da marginalidade com sucessivo progresso de imersão tecnológica das autoridades para se adiantar ao crime com a devida manutenção das leis de forma mais célere objetivando deter o claro avanço da criminalidade hodierna.

REFERÊNCIAS

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez.

BRASIL, DECRETO-LEI NO 2.848, DE 7 DE DEZEMBRO DE 1940. Código Penal. Rio de Janeiro, 7 de dezembro de 1940; 119º da Independência e 52º da República. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 08/06/2023.

BRASIL. LEI Nº 14.155, DE 27 DE MAIO DE 2021. Lei de Invasão a Dispositivo Informático [Internet]. Disponível em: https://www.in.gov.br/en/web/dou/-/lei-n-14.155-de-27-de-maio-de-2021-322698993. Acesso em: 24 nov. 2023

BRASIL. LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012. Lei de Invasão a Dispositivo Informático [Internet]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em:
24 nov. 2023.

BRASIL. LEI Nº 14.155, DE 27 DE MAIO DE 2021. Lei de Invasão a Dispositivo Informático [Internet]. Disponível em: https://www.in.gov.br/en/web/dou/-/lei-nº 14.155-de-27-de-maio-de-2021-322698993. Acesso em: 13 dez. 2023.

BRASIL. Tribunal de Justiça do Paraná. TJ-PR - Recurso Inominado XXXXX-67.2020.8.16.0136 PR. Relator Nestario da Silva Queiroz. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-pr/1511018743. Acesso em: 25 nov. 2023

BRASIL. Tribunal de Justiça do Rio Grande do Sul. TJ-RS - Apelação Cível XXXXX-22.2020.8.21.7000 RS. Relator Giovanni Conti. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-rs/932015329. Acesso em: 25 nov. 2023

BRITO, Auriney. Direito penal informático. São Paulo: Saraiva, 2013, p.189.

CAMPOS, Pedro Franco de [et al.]. Direito penal aplicado: parte geral e parte especial do Código Penal. - 6ª. Ed. – São Paulo: Saraiva, 2016.

CASSANTI, Moisés de Oliveira. Crimes virtuais, vítimas reais. 1ª ed. Rio de Janeiro: Brasport, 2014, p.6.

CHAVES, Fábio Barbosa; TEIXEIRA, Filipe Silva. Os crimes de fraude e estelionato cibernético e a proteção do consumidor no e-commerce. 2020. Disponível em: <https://conteudojuridico.com.br>. Acesso em: 12/06/2023.

COELHO, Yuri Carneiro. Curso de Direito Penal Didático. vol. único, 2ª ed. – São Paulo: Atlas, 2015.

CÔRREA, Gustavo Testa. Aspectos jurídicos da internet. 5. ed. rev. e atual. São Paulo, Saraiva, 2010.

CUNHA, Rogério Sanches. Manual de direito penal: parte especial (arts. 121 ao 361). 11. ed. rev., ampl. e atual. Salvador: JusPODIVM, 2019.

CUNHA, Rogério Sanches. Lei 14.155/21 e os crimes de fraude digital - primeiras impressões e reflexos no CP e no CPP. Meu Site Jurídico (JusPodivm), 2021. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2021/05/28/lei-14-15521-e-os-crimes-de-fraude-digital-primeiras-impressoes-e-reflexos-no-cp-e-no-cpp/. Acesso em: 13 dez. 2023.

FBSP. Fórum Brasileiro de Segurança Pública. Os crimes patrimoniais no Brasil: entre novas e velhas dinâmicas. Anuário Brasileiro de Segurança Pública, 2022. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2022/07/07-anuario-2022-os-crimes-patrimoniais-no-brasil-entre-novas-e-velhas-dinamicas.pdf. Acesso em 24 nov. 2023.

GENNARINI, Juliana. Revista de Direito Penal e Processo Penal, ISSN 2674-6093, v. 2, n. 2, jul./dez. 2020.

GONÇALVES, Victor Eduardo Rios. Direito penal esquematizado: parte especial do Código Penal. - 8. ed. – São Paulo: Saraiva Educação, 2018.
GRECO, Rogério. Curso de Direito Penal: parte especial. v. III. 7. ed. Rio de Janeiro: Ed. Impetus, 2010.

GOUSSINSKY, Eugenio. Crimes digitais têm forte alta em vários estados; saiba como prevenir. Portal R7, 2021. Disponível em: https://noticias.r7.com/tecnologia-e-ciencia/crimes-digitais-tem-forte-alta-em-varios-estados-saiba-como-prevenir-05052021. Acesso em: 12 dez. 2023.

GRECO, Rogério. Curso de Direito Penal: parte especial. v. III. 7. ed. Rio de Janeiro: Ed. Impetus, 2010, p. 228.

HUNGRIA, Nelson. Comentários ao Código Penal – Vol. IX. Rio de Janeiro: Forense, 1958.

MIRABETE, Júlio Fabbrini e FABBRINI, Renato N./ Manual de direito penal: parte especial: arts. 121 a 234-B do CP – volume 2, 36° edição, São Paulo, Atlas, 2021.

Relatório do Software Anti-plágio CopySpider
Para mais detalhes sobre o CopySpider, acesse: https://copyspider.com.br

Instruções
Este relatório apresenta na próxima página uma tabela na qual cada linha associa o conteúdo do arquivo de entrada com um documento encontrado na internet (para "Busca em arquivos da internet") ou do arquivo de entrada com outro arquivo em seu computador (para "Pesquisa em arquivos locais"). A quantidade de termos comuns representa um fator utilizado no cálculo de Similaridade dos arquivos sendo comparados. Quanto maior a quantidade de termos comuns, maior a similaridade entre os arquivos. É importante destacar que o limite de 3% representa uma estatística de semelhança e não um "índice de plágio". Por exemplo, documentos que citam de forma direta (transcrição) outros documentos, podem ter uma similaridade maior do que 3% e ainda assim não podem ser caracterizados como plágio. Há sempre a necessidade do avaliador fazer uma análise para decidir se as semelhanças encontradas caracterizam ou não o problema de plágio ou mesmo de erro de formatação ou adequação às normas de referências bibliográficas. Para cada par de arquivos, apresenta-se uma comparação dos termos semelhantes, os quais aparecem em vermelho.
Veja também:
Analisando o resultado do CopySpider
Qual o percentual aceitável para ser considerado plágio?

Versão do CopySpider: 2.2.0
Relatório gerado por: rafaelgarcia2321@gmail.com
Modo: web / normal

Arquivos	Termos comuns	Similaridade
Trabalho de ConclusÃ£o de Curso - Rafael Garcia.pdf X https://www.conjur.com.br/2021-jun-14/bitencourt-furto-mediante-uso-dispositivo-eletronico-ou-informatico	99	1,17
Trabalho de ConclusÃ£o de Curso - Rafael Garcia.pdf X https://www.avg.com/pt/signal/what-is-a-vishing-attack	19	0,20
Trabalho de ConclusÃ£o de Curso - Rafael Garcia.pdf X https://www.redpoints.com/blog/prevent-digital-fraud	3	0,03
Trabalho de ConclusÃ£o de Curso - Rafael Garcia.pdf X https://www.ncbi.nlm.nih.gov/books/NBK537222	2	0,02
Trabalho de ConclusÃ£o de Curso - Rafael Garcia.pdf X https://www.un.org/en/un75/impact-digital-technologies	0	0,00
Trabalho de ConclusÃ£o de Curso - Rafael Garcia.pdf X https://www.datavisor.com/intelligence-center/reports/digital-fraud-trends-report-2021	0	0,00
Trabalho de ConclusÃ£o de Curso - Rafael Garcia.pdf X http://www.google.com.br/url?esrc=s	0	0,00
Arquivos com problema de download		
https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/12062022-Resultados-previstos--riscos-assumidos-o-dolo-eventual-no-crime-de-homicidio.aspx	Não foi possível baixar o arquivo. É recomendável baixar o arquivo manualmente e realizar a análise em conluio (Um contra todos). - Erro: Parece que o documento não existe ou não pode ser acessado. HTTP response code: 403 - Server returned HTTP response code: 403 for URL: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/12062022-Resultados-previstos--riscos-assumidos-o-dolo-eventual-no-crime-de-homicidio.aspx	
https://www.f5.com/labs/articles/cisotociso/the-ins-and-outs-of-digital-fraud	Não foi possível baixar o arquivo. É recomendável baixar o arquivo manualmente e realizar a análise em conluio (Um contra todos). - Index 30 out of bounds for length 30	
https://www.cloudflare.com/pt-br/learning/email-security/what-is-vishing	Não foi possível baixar o arquivo. É recomendável baixar o arquivo manualmente e realizar a análise em conluio (Um contra todos). - Erro: Parece que o documento não existe ou não pode ser acessado. HTTP response code: 403 - Server returned HTTP response code: 403 for URL: https://www.cloudflare.com/pt-br/learning/email-security/what-is-vishing	

ESTELIONATO DIGITAL: UMA ANÁLISE CRÍTICA DA DISCIPLINA NORMATIVA, SUAS FORMAS DE CONDUTA E AS POSSÍVEIS CONSEQUÊNCIAS SOCIAIS

Rafael Lemos Garcia de Oliveira1
Ricardo Simões Xavier dos Santos2

Resumo
O presente artigo discorre sobre a figura do estelionato digital, fazendo uma análise crítica da disciplina normativa, suas formas de conduta e as possíveis consequências sociais. É notório que a atual legislação do país tem avançado, conforme mencionado, na forma que tipifica os crimes que ocorrem em meios virtuais, todavia as sanções ainda são moderadas e as normas devem avançar no sentido de impedir a prática dos crimes virtuais. Para que seja viável a hipótese narrada, o Estado tem o dever de incrementar métodos novos de apuração e averiguação e aprimorar os recursos tecnológicos e digitais que estão à disposição das autoridades responsáveis. Nesse sentido, é necessário compreender o que é o estelionato digital, suas características, maneiras de prevenção e formas em que pode aparecer no dia a dia dos usuários da rede, compactuando com a legislação penal e o cabimento de penalização para os criminosos que praticam esse crime. Por fim, conclui-se que a legislação penal brasileira vem evoluindo, mas para que alcance um nível suficiente de eficácia no combate a esse crime é necessário compreender o que é o estelionato digital, suas características, maneiras de prevenção e formas em que pode aparecer no dia a dia dos usuários da rede, compactuando com a legislação penal e o cabimento de penalização para os criminosos que praticam esse crime.

PALAVRAS-CHAVE: Internet. Crime Cibernético. Estelionato Digital. Código Penal.

1 Graduando em bacharelado em direito pela UCSAL. E-mail: rafaell.oliveira@ucsal.edu.br

2 Doutor em Políticas Sociais e Cidadania pela Universidade Católica do Salvador ? UCSal. E-mail: ricardo.santos@pro.ucsal.br
2

ABSTRACT: This article discusses the figure of digital fraud, making a critical analysis of the normative discipline, its forms of conduct and the possible social consequences. It is notable that the country's current legislation has advanced, as mentioned, in the way it typifies crimes that occur in virtual media, however sanctions are still moderate and standards must advance in order to prevent the practice of virtual crimes. In order for the narrated hypothesis to be viable, the State has the duty to increase new methods of investigation and investigation and improve the technological and digital resources that are available to the responsible authorities. In this sense, it is necessary to understand what digital fraud is, its characteristics, methods of prevention and ways in which it can appear in the daily lives of network users, in agreement with criminal legislation and the appropriateness of penalizing criminals who practice this crime. Finally, it is concluded that Brazilian criminal legislation has been evolving, but in order to achieve a sufficient level of effectiveness in combating this crime, it is necessary to understand what digital fraud is, its characteristics, methods of prevention and forms in which it can appear. in the daily lives of network users, complying with criminal legislation and the appropriateness of penalizing criminals who commit this crime.

KEYWORDS: Internet. Cybercrime. Digital Fraud. Penal Code.

SUMÁRIO: 1 INTRODUÇÃO. 2 CONDUTA DO ESTELIONATO DIGITAL: CONCEITOS PRÉVIOS, DISCUSSÕES INICIAIS E FORMAS APRESENTADAS. 2.1 Análise acerca das eventuais consequências sociais advindas da conduta do estelionato digital 3 A RESPONSABILIZAÇÃO DO CRIME DE ESTELIONATO DIGITAL NO ÂMBITO JURÍDICO 3.1 Concepção das normas jurídicas atualizadas e formas de punição do crime do estelionato digital 4 O HISTÓRICO DA PRÁTICA DO ESTELIONATO DIGITAL E OS REFLEXOS DA LEI 14.155 FRENTE A VULNERABILIDADE DA VÍTIMA 5 CONCLUSÃO 6 REFERÊNCIAS

1 INTRODUÇÃO

No âmbito penalista são diversos os crimes que têm como objetivo a obtenção de lucros financeiros da vítima, o referido trabalho tem como objetivo abordar o estelionato digital fazendo uma análise crítica da disciplina normativa, apresentando suas formas de conduta e relacionando a suas possíveis consequências sociais.
3

Há uma previsão legal do Código Penal em garantir que todos os cidadãos lesados por práticas de golpes, em que são utilizados artifícios ou qualquer meio fraudulento, podem ingressar no juízo criminal a fim de prosseguirem com a punição penal e com o ressarcimento dos prejuízos.

Para breve introito, o estelionato é 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.
Dentre os crimes mais comuns no Brasil e no mundo pode-se destacar o estelionato, além do meio físico os criminosos procuram pela navegação na rede com o fito de obtenção de dados e informações das pessoas que tem perfil para serem suas possíveis vítimas, pondo em prática das mais diversas maneiras tais como ligações, mensagens, falsificação de identidade, haja vista que todos os dias, a população vive a internet, cadastrando senhas, trocando mensagens, adentrando redes sociais, fazendo negócios pela internet...
Nesse sentido, acompanhando o aumento dos usuários das redes a realização de crimes online cresceu consideravelmente, obviamente relacionado a simplicidade de manejo dos meios virtuais e pela dificuldade de identificação dos criminosos para posterior punição, haja vista ausência de legislações específicas e supressão das identidades.
A realização de golpes e fraudes cometendo ilícitos para obter vantagem sob outras pessoas é prática recorrente e por muitas vezes impune no Brasil, com o estelionato digital não é diferente.
Em sua esfera digital ele se configura quando o criminoso submete o aparelho da vítima e sincroniza-o a demais sistemas de informação ou, em outra hipótese, quando a vítima é posta em uma conjuntura de sensibilidade para obtenção de vantagem ilícita. Na atualidade é mais comum do que se imagina conhecer alguém que tenha passado por essa situação e caído nesse golpe, desde ligações de números sem chamador ou desconhecidos a e-mails/mensagens com ofertas incríveis.
Outro ponto importante que contribuiu para esse aumento, além da facilidade no manejo dos meios virtuais foi o advento da pandemia do Covid-19, as práticas desses crimes se multiplicaram, haja vista que, relevante porcentagem da população tanto brasileira quanto mundial, se viu obrigada a passar mais tempo em casa, o que, em consequência, ampliou o número de pessoas online, acessando a rede. Neste liame, os criminosos têm agido cada vez mais e feito várias vítimas no mundo virtual.
4

Para que o crime possa ser classificado como estelionato digital é imprescindível que a entrega das informações pela vítima seja de forma voluntária, haja vista que a obtenção dos dados se deu por outros meios, o crime pode ter outra classificação, tal como ?furto mediante fraude eletrônica?.
Dentre as principais vítimas desse crime tão comum na atualidade estão as pessoas desatentas e que não tomam total atenção para se esquivar dos estelionatários, seguindo as hipóteses de compra e venda pela internet não verificando a fonte, se é de confiança etc., links enviados de números aleatórios possibilitando o acesso do criminoso a rede da vítima entre outros...
A despeito da clara regulação e evolução da internet e redes sociais, os conselhos e observações para a premeditação dos crimes digitais em geral continua sendo de cuidado e cautela com os dados pessoais e sua divulgação, ainda com o

remetente e usuários/links que adentra. É necessário que sempre pense que tudo que identifique quem você é ou que busque saber informações que só você teria acesso são o alerta inicial para entender se não se está diante de uma possível tentativa de estelionato digital.
É notório que a atual legislação do país tem avançado, conforme mencionado, na forma que tipifica os crimes que ocorrem em meios virtuais, todavia as sanções ainda são moderadas e as normas devem avançar no sentido de impedir a prática dos crimes virtuais. Para que seja viável a hipótese narrada, o Estado tem o dever de incrementar métodos novos de apuração e averiguação e aprimorar os recursos tecnológicos e digitais que estão à disposição das autoridades responsáveis.
Nesse sentido, é necessário compreender o que é o estelionato digital, suas características, maneiras de prevenção e formas em que pode aparecer no dia a dia dos usuários da rede, compactuando com a legislação penal e o cabimento de penalização para os criminosos que praticam esse crime.
Assim, as perguntas que ficam são quais as formas de conduta do estelionato digital e seus impactos na sociedade, além do questionamento acerca das normas brasileiras, nosso sistema jurídico atual contempla qual espécie de responsabilização para o crime de estelionato digital, alinhado a isso, como o Estado Democrático Brasileiro pode melhorar para combater o aumento desse crime.
No presente artigo, seguindo após a introdução para o capítulo ?2? onde serão apresentadas as condutas do estelionato digital, seus conceitos prévios e formas apresentadas, a diferença entre o estelionato e outros crimes contra o patrimônio e
5

sua forma de proliferação pela rede mediante sites falsos, mensagens e e-mails. O capítulo ?2? contém ainda um subtópico ?2.1? onde serão analisadas as consequências sociais advindas da conduta do estelionato digital, desde a inovação dos criminosos partindo para o meio digital até os ?traumas? das vítimas e sua repercussão na sociedade.
Já no capítulo ?3? será amplamente explicada a quem deve ser dirigida a responsabilidade pelo crime do estelionato digital, no âmbito jurídico, já que o crime na grande maioria das vezes tem por conclusão a ?fuga? do criminoso pelo meio cibernético. Ainda no capítulo ?3? serão exploradas, mediante subtópico ?3.1?, as normas jurídicas atualizadas e formas de punição do crime tendo relação direta com a ampla possibilidade de escape do criminoso.
Por fim, em capítulo ?4?, será demonstrado o histórico da prática do estelionato digital, sua evolução paralela ao avanço da tecnologia na sociedade e os reflexos da Lei 14.155, instituída em 2021 especialmente para tornar mais grave a pena de estelionato cometido de forma eletrônica pela internet, frente ainda a vulnerabilidade da vítima. Seguidos da conclusão e as referências bibliográficas.
De certo, cumpre-se destacar que a pesquisa em questão, valeu-se do método da revisão bibliográfica de trabalhos científicos atualizados das áreas penal e constitucional, frente às questões sociais, publicadas em periódicos nacionais e internacionais, qualificados como publicações de A1, assim como B1. Além de

importantes nomes do cenário retrato, ao passo que se cita Rogério Greco e Fabio Barbosa Chavez, bem como análise jurisprudencial e legislativa da lei 14.155.
Compreende-se então, que a escolha metodológica se justifica de base teórica, fundada em estudos atualizados sobre o estelionato digital, suas formas de conduta e as consequências sociais.
O foco da pesquisa bibliográfica foi de apresentar informações e dados específicos sobre a evolução dos crimes digitais, exibindo o progresso do direito penal frente os crimes digitais, através da análise filosófica e de referenciais teóricos de artigos, códigos e outros trabalhos sobre a mesma questão jurídica. Assim, o método empregado é de leitura e análise de material doutrinário especializado já existente sobre o tema de Direito Penal, tal como de jurisprudência, dados, legislação e artigos científicos.

6

2 CONDUTA DO ESTELIONATO DIGITAL: CONCEITOS PRÉVIOS, DISCUSSÕES INICIAIS E FORMAS APRESENTADAS.

O termo estelionato está disposta no Art. 171 do Código Penal como:

Art. 171. Obter, para si ou para outrem, vantagem ilícita em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: pena ? Reclusão, de 1 (um) a 5 (cinco) anos, de multa.

Trata-se de crime contra o patrimônio onde a legislação penal visa proteger a inviolabilidade patrimonial orientada pela prática de atos que visam enganar a vítima e beneficiar o agente (CUNHA, 2019, p. 345).
Assim, pode-se inferir que a diferença entre o estelionato e os diversos crimes contra o patrimônio, ou seja, crimes que tenham por objetivo atentar contra o patrimônio de uma pessoa ou organização, é que no estelionato não é utilizada a força para obtenção de ?vantagem?. É sabido, portanto, que essa atitude é conhecida há muitos anos, de modo que Greco cita que:

Desde que surgiram as relações sociais, o homem se vale da fraude para dissimular seus verdadeiros sentimentos e intenções para, de alguma forma, ocultar ou falsear a verdade, a fim de obter vantagens que, em tese, lhe seriam indevidas (GRECO, 2019, p. 228).

Ressalta-se que o crime existe apenas na modalidade dolosa, sem previsão na forma culposa.
A respeito da expressão ?vantagem ilícita?, Fernando Capez (2020) ensina que, esta, trata-se do objeto material do crime e, caso o agente esteja agindo em razão de uma vantagem devida, a conduta é tipificada como exercício arbitrário das próprias razões, delito previsto no art. 345, do Código Penal.

De acordo com o que se retira do artigo 171, do supramencionado dispositivo legal, o estelionato pode ser cometido mediante artificio, ardil ou qualquer outro meio fraudulento. Em relação ao termo ?artificio?, o doutrinador Júlio Fabbrini Mirabete ensina o seguinte:

?o artifício existe quando o agente se utilizar de um aparato que modifica, ao menos aparentemente, o aspecto material da coisa, figurando entre esses meios o documento falso ou outra falsificação qualquer, o disfarce, a modificação por aparelhos mecânicos ou elétricos, filmes, efeitos de luz etc.? (MIRABETE, 2021, pag. 325).

Em sua modalidade digital o estelionato ocorre através de sites falsos, mensagens e até e-mail, sendo prioritariamente focado no âmbito virtual. É bastante
7

normal que o consumidor busque virtualmente os mesmos bens desejados fisicamente, mas com a comodidade de não se deslocar e em grande maioria dos casos a acessibilidade com preços menores, levando a promessa da oferta muitas vezes a encantar o consumidor que não percebe a fraude.
Dentre as formas de conduta do referido crime podem ser listadas as mais comuns sendo: vendas falsas em sua maioria quando os estelionatários oferecem serviços ou produtos inexistentes em redes sociais e/ou sites e links de comércio eletrônico; ?phishing?, uma artimanha utilizada pelos criminosos para enganar os usuários e conseguir informações privadas, tais como senhas, detalhes de cartões de crédito, comumente realizado por meio do envio de mensagens eletrônicas se passando por instituições de confiança, pode ser realizado por sites e por redes sociais também, mas sempre com o intuito de prejudicar e obter vantagem, ?vishing? popularmente conhecido por ?phishing por voz? quando o ato é realizado por ligações ou envio de áudios com o mesmo intuito de ludibriar a vítima, mas para divulgar dados pessoais, ?smishing? realizada também por mensagem, mas nessa modalidade a vítima é provocada a acessar link que corrompe seu aparelho, e por último os golpes de investimentos fraudulentos que podem acontecer de diversas maneiras, tais como promessas de retornos financeiros utopicamente elevados e esquema de pirâmides, esses golpistas beneficiam-se da leiguice de suas vítimas no âmbito de investimento financeiro com falsas promessas de enriquecimento acelerado para enganá-las.
No Art. 171 do Código Penal, o estelionato possui a pena de reclusão de 1 a 5 anos e multa. Diante disso, o crime admite suspensão condicional no processo de acordo com o art. 89, § 1ª, da Lei dos Juizados Especiais - Lei n. 9099/95:

Art. 89. Nos crimes em que a pena mínima cominada for igual ou inferior a um ano, abrangidas ou não por esta Lei, o Ministério Público, ao oferecer a denúncia, poderá propor a suspensão do processo, por dois a quatro anos, desde que o acusado não esteja sendo processado ou não tenha sido condenado por outro crime, presentes os demais requisitos que autorizariam

a suspensão condicional da pena (art. 77 do Código Penal).

Conforme dito, o crime de estelionato digital, no sistema jurídico atual do Brasil, é apreciado no âmbito do Direito Penal o qual pressupõe responsabilização penal para esse tipo de ato, o qual era equiparado ao crime de estelionato, previsto no artigo 171 do Código Penal, ocorre que ainda no caminhar para a especificação do crime de estelionato na modalidade digital foi introduzida a Lei 12.737/2012, ou como é popularmente conhecida a ?Lei Carolina Dieckmann?, que surgiu após um incidente
8

em que a atriz teve seu aparelho pessoal invadido e com isso o vazamento de fotos íntimas na rede, mediante ainda tentativa de extorsão.
Na época em questão os criminosos seriam apenas denunciados pelo crime de tentativa de extorsão, haja vista ausência de legislação específica quanto aos crimes digitais, assim vários projetos de lei foram analisados para tentar tipificar condutas para crimes semelhantes ao sofrido pela atriz e findada essa fase foi sancionada a Lei 12.737/2012 que entrou em vigor em 02 de abril de 2013.
A lei visava combater o vazamento de informações pessoais dos usuários das redes, zelando pela proteção da privacidade dos mesmos, ainda acrescentou ao Código Penal, mais especificamente no Decreto-Lei 2848, os artigos 154-A e 154-B.

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

A lei se demonstrou efetiva a época da sanção sendo citada como um marco legislativo por muitos autores, desde que entrou em vigor a invasão de computadores, celulares, tablets...no geral dispositivos informáticos alheios passou a ser crime.
Cabe destacar que execução da lei e a responsabilização dos golpistas submete-se a conduta das autoridades capazes, para investigar, processar e julgar os casos de estelionato digital, como a polícia e o Poder Judiciário.

2.1 ANÁLISE ACERCA DAS EVENTUAIS CONSEQUÊNCIAS SOCIAIS ADVINDAS DA CONDUTA DO ESTELIONATO DIGITAL.

A sociedade está cada vez mais conectada e as redes sociais têm uma função

muito importante nessa interação, vez que o ser humano sempre precisou de convívio social. Assim, tais ferramentas estão presentes na vida de muitos brasileiros e esse ambiente digital, como já evidenciado, tornou-se, também, um meio para a prática de crimes, seja pela facilidade de acesso e/ou pelo grande número de usuários.
9

Na atualidade existe uma grande facilidade na obtenção de produtos, sendo de maneira virtual, de modo que não existe mais a necessidade do consumidor se deslocar até o fornecedor para adquirir o produto, nesta feita, é notório que a compra virtual vem amadurecendo cada vez mais, o que consequentemente ocasiona um aumento dos crimes cibernéticos. Nesse contexto, Chaves e Teixeira destacam que:

Com a investigação correta é possível localizar e punir os criminosos que causaram prejuízo a essa nova espécie de consumidores. Todavia, no mesmo ritmo que a internet evolui, os fraudadores também se renovam com novas modalidades de golpes, alguns tão específicos que são até difíceis de definir qual a punição correta a ser aplicada (CHAVES e TEIXEIRA, 2019, p. 119).

Conforme já citado a inovação dos criminosos acompanha em paralelo o avanço da tecnologia pela sociedade, de modo que muitos usuários têm a sensação de que a internet é ?terra sem lei? fomentando sua ?liberdade tecnológica? em pequenos delitos, tais como injúria, difamação... Ao passo em que não imaginam ter a sua responsabilidade realmente comprovada, agindo por trás da tela do celular ou computador.
Perpassando por isso os criminosos buscam a obtenção de vantagem ilícita e veem na internet uma oportunidade recheada de opções, possuídos pela sensação de impunidade e munidos das mais diversas artimanhas para concluir seu objetivo.
Cumpre ressaltar que sociedade caminha para um futuro mais tecnológico e os criminosos ?surfam nessa onda?.
A cada dia que passa resta mais rudimentar os métodos de pagamento por cédulas ou moedas, a trajetória da população tem destino eletrônico, de modo que é fato notório o quão comum se tornaram os sistemas de pagamento eletrônico, estando já alguns mais rudimentares como a transferência ?TED?.
A popularização dos sistemas de pagamento eletrônico, a exemplo do ?pix?, propicia diariamente um combate necessário entre as autoridades e os golpistas. Já é rotina na sociedade a divulgação de novos meios de golpes cibernéticos com o fito de alertar os usuários a se precaverem mais, infelizmente nem sempre todo cuidado é tomado e as consequências podem ser desastrosas para os consumidores da rede.
O prejuízo causado a essa nova espécie de consumidores afeta tanto de forma direta as vítimas quanto a sociedade, de maneira geral. Dentre as consequências sociais advindas dessa conduta resta mister destacar o impacto financeiro nas vítimas, de forma direta, que podem encarar perdas financeiras o que acarreta
10

problemas emocionais e instabilidade, perda de confiança no meio digital para compras que também gera impacto na maneira como as pessoas conduzem negócios online.
Além do consumidor direto, as instituições financeiras também sofrem em muitos casos ressarcindo o valor perdido por seus clientes lesados, arcando com o custo de fraude e também no investimento em segurança virtual, mesmo ainda tendo um receio a implantação dos pagamentos digitais buscando ao máximo reforçar sua segurança desde confirmação por ?face id? quanto senhas regularmente trocadas e ?tokens digitais?, sempre tentando confirmar que é realmente o usuário da conta quem realmente está fazendo a operação e não um terceiro. Frisa-se que essas consequências sociais acarretam, num todo, impacto na economia.
Felizmente, não são somente os consumidores que passam pelo processo de consequências negativas, mas também os fraudadores. Mesmo diante da crescente a qual ocorre o ?fenômeno? do estelionato digital, os criminosos não restam imunes a responsabilização pelo seu crime. Conforme será demonstrado no presente artigo, a legislação do país delimita o crime e suas consequências, assim como as penalidades que podem levar os fraudadores a condenação pelas atividades ilícitas.
Nesse sentido, o avanço da tecnologia com o passar dos tempos corroborou indiretamente para que os criminosos inovassem seus meios ilícitos para obtenção de vantagens, causando diversos impactos na sociedade que não teriam como ser positivos, sendo alguns dos principais o prejuízo financeiro as vítimas; perda de confiança na segurança online e transações digitais, além do choque nos sistemas judiciais, de segurança e nas bases digitais o que consequentemente requer mecanismos e investimentos relevantes de atribuição das empresas e do judiciário.
Sendo assim, infere-se que ainda existe certa dificuldade para identificação dos golpistas o que, alternativamente, tem relação com a legislação brasileira que tem avançado na tipificação dos crimes cibernéticos, todavia as sanções ainda são moderadas e as normas devem acompanhar no sentido de bridar a prática desses crimes na modalidade virtual.

3 A RESPONSABILIZAÇÃO DO CRIME DE ESTELIONATO DIGITAL NO ÂMBITO JURÍDICO.

11

É claro que a internet e toda a esfera digital não foi inserida na sociedade com o intuito ou sequer resguarda em relação a possibilidade do advento de crimes em paralelo a isso, mas como toda imprevisão, a criminalidade evoluiu em conjunto deixando cada vez mais vulnerável a segurança dos usuários na rede, como amplamente demonstrado no presente trabalho, os golpes digitais se aperfeiçoam com o passar dos anos, com ênfase para o estelionato que conta hoje com diversos tipos de obtenção de vantagem ilícita na sua modalidade digital.
A internet tornou-se essencial na rotina da população, interligando usuários e

pessoas conectadas a rede, assim, como bem destacou Uchoa de Brito:

(...) O problema da internet passou a ser identificado quando a tecnologia incrementou e complicou as relações sociais consideradas, até então, pacíficas e controladas, possibilitando algumas experiências socialmente desagradáveis e indesejadas, como a sua utilização para a prática de crimes, e a criação de novos contatos que colocam em risco bens que ainda não tiveram sua relevância reconhecida pelo Direito. (BRITO, 2013, p. 9).

Assim, a prática do estelionato na modalidade virtual cresceu ao longo dos anos, sempre com a tentativa em paralelo do Direito Penal de acompanhar para poder punir em cerceamento legislativo, com projetos de lei, inovações e acréscimos a legislações já vigentes.
Quanto a responsabilização do crime em questão torna-se direta em relação ao Autor, sendo aferida pelo Estado, mesmo em sua modalidade digital, haja vista que tem o encargo de combater, controlar e reprimir tais práticas tanto no mundo ?real? quanto no ambiente digital, além de ser responsável por tutelar a convivência e atuação neste âmbito cibernético.
Além da responsabilização direta quanto ao autor do delito, muitas vezes a responsabilidade também recai de forma subjetiva ou objetiva para um terceiro da relação que deveria zelar pela segurança dos dados pessoais do usuário, grandes exemplos são os de vazamento de dados bancários online após invasão por hackers, recaindo responsabilidade também para os bancos que deveriam proteger o consumidor.

APELAÇÃO CÍVEL. NEGÓCIOS JURÍDICOS BANCÁRIOS. AÇÃO DE INDENIZAÇÃO POR DANOS MATERIAIS. RESSARCIMENTO DE VALORES. TRANSAÇÃO BANCÁRIA REALIZADA DE FORMA FRAUDULENTA POR TERCEIROS. INTERNET BANKING. RESPONSABILIDADE DO BANCO. SUMULA 479 DO STJ. SENTENÇA MANTIDA. As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias. Súmula 479 do STJ. Art. 14 do CDC. Para
12

responsabilização do prestador de serviços a existência de culpa ou dolo, exige-se apenas a conduta ilícita e a existência de dano, bem como nexo de causalidade entre eles. Caso. Autora que foi vítima de estelionato praticado por terceiro. Empréstimo autorizado pela instituição financeira. Nesse ponto, desimporta que a fraude tenha se perpetrado através dos canais de atendimento via internet (internet banking), porquanto a parte autora negou ter sido a autora dos saques, e o banco não se desincumbiu do ônus de demonstrar a regularidade das transações impugnadas pelo cliente. NEGARAM PROVIMENTO AO APELO. UNÂNIME.

Entre outros exemplos de golpes como os já citados ?phishing?, ?vishing? e ?smishing? que buscam a obtenção de vantagem ilícita frente as vítimas, muitas vezes fazendo uso de um terceiro como ponte para alçar seu objetivo fraudulento, ocorre que, como mencionado, mesmo esse terceiro não tendo o dolo na prática do crime deve garantir a segurança e impermeabilidade do seu sistema para que isso não ocorra, contando com a obrigação de assegurar os direitos do consumidor e usuário.
Este é o entendimento das jurisprudências pátrias:
RECURSO INOMINADO. AÇÃO DECLARATÓRIA DE INEXISTÊNCIA DE DÉBITO C/C INDENIZAÇÃO POR DANOS MORAIS. PRELIMINAR DE VIOLAÇÃO AO PRINCÍPIO DA DIALETICDADE. INOCORRÊNCIA. BANCÁRIO. TRANSFERÊNCIA DE VALORES REALIZADA POR TERCEIRO. FRAUDE EVIDENCIADA. CULPA DA VÍTIMA NÃO CONFIGURADA. INSTITUIÇÃO FINANCEIRA QUE NÃO APRESENTOU PROVAS ACERCA DA SEGURANÇA, AUTENTICAÇÃO OU IDENTIFICAÇÃO DA OPERAÇÃO. FALHA NA PRESTAÇÃO DO SERVIÇO CONFIGURADA. RESPONSABILIDADE OBJETIVA DO BANCO. APLICAÇÃO DA SÚMULA 479 DO STJ. RESTITUIÇÃO DEVIDA. AUSÊNCIA DE SOLUÇÃO ADMINISTRATIVA. DANO MORAL CONFIGURADO NO CASO CONCRETO. QUANTUM ARBITRADO EM R$ 2.000,00 (DOIS MIL REAIS) QUE COMPORTA MAJORAÇÃO PARA R$ 3.000,00 (TRÊS MIL REAIS). OBSERVÂNCIA AOS PRINCÍPIOS DA PROPORCIONALIDADE E RAZOABILIDADE. SENTENÇA PARCIALMENTE REFORMADA. Recurso da autora conhecido e provido.Recurso do réu conhecido e desprovido. (TJPR - 1ª Turma Recursal - 0003317-67.2020.8.16.0136 - Pitanga - Rel.: JUIZ DE DIREITO DA TURMA RECURSAL DOS JUIZADOS ESPECIAIS NESTARIO DA SILVA QUEIROZ - J. 23.05.2022)
(TJ-PR - RI: 00033176720208160136 Pitanga 0003317-67.2020.8.16.0136 (Acórdão), Relator: Nestario da Silva Queiroz, Data de Julgamento: 23/05/2022, 1ª Turma Recursal, Data de Publicação: 23/05/2022)

Ressalta-se que o estelionato na sua modalidade digital é considerado crime de ação penal pública incondicionada, ou seja, a responsabilidade para conduzir o procedimento é do Ministério Público, independente de manifestação de vontade da vítima, a natureza dessa ação ressalva a relevância de tratar esse delito de forma mais eficaz, independente da vontade da vítima de ver o autor do crime responsabilizado, com o fito de preservar a ordem social e diminuir o índice de novos casos.
13

Nesse sentido, cumpre destacar que mesmo a responsabilidade do crime ser direta em relação ao Autor, também pode abranger mais partes do processo dependendo da especificada do caso. A jurisprudência entende que a responsabilidade não é apenas do Estado, mas também da empresa, entidade ou

qualquer terceiro que tenha a obrigação de tornar o ambiente digital seguro para o usuário.

3.1 CONCEPÇÃO DAS NORMAS JURÍDICAS ATUALIZADAS E FORMAS DE PUNIÇÃO DO CRIME DO ESTELIONATO DIGITAL.

Como já explicitado, um grande fator que desencadeou o aumento da efetivação do crime em questão foi a pandemia, de modo que, com o advento do Covid-19, foi necessário que a população se protegesse em suas casas para corroborar com o distanciamento social e assim evitar a proliferação do vírus, ocorre que em contrapartida a isso foi destaque a aproximação online dos usuários que culminou em oportunidade para os criminosos inovarem suas artimanhas, contando com a suposta sensação de anonimato.
O crime de estelionato digital, no sistema jurídico atual do Brasil, é apreciado no âmbito do Direito Penal, o qual pressupõe responsabilização para esse tipo de ato, que era equiparado ao crime de estelionato, previsto no artigo 171 do Código Penal.
A Lei 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann, entrou em vigor como uma tentativa inicial de tipificar a conduta dos crimes na modalidade virtual para proteção dos dados pessoais da população em face aos criminosos virtuais, ocorre que com o passar dos anos se mostrou necessária a inclusão de novas medidas frente a progressão da criminalidade no país, em específico os crimes virtuais.
Para combater essa crescente negativa no âmbito jurídico nacional entrou em vigor a lei 14.155/21, de 27 de maio de 2021, que incluiu e modificou alguns parágrafos no supramencionado dispositivo legal, alterando algumas regras para julgar o crime.

Art. 1º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar com as seguintes alterações:
?Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
14

§ 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.
§ 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso:
I ? 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;
II ? Aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra

idoso ou vulnerável. Pena ? reclusão, de 1 (um) a 4 (quatro) anos, e multa.
§ 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. Pena ? reclusão, de 2 (dois) a 5 (cinco) anos, e multa.

Dentre as alterações, foram incluídos os § § 2º-A e 2º-B, que tratam de fraude eletrônica, sendo o § 2º-A qualificadora para o crime de estelionato que não é praticado na modalidade presencial, ou seja, quando a frade é cometida com uso de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de reses sociais ou qualquer outro meio fraudulento análogo.

Fraude eletrônica
§ 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.
§ 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.
Estelionato contra idoso ou vulnerável
§ 4º A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso.
Art. 2º O art. 70 do Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), passa a vigorar acrescido do seguinte § 4º:
§ 4º Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção.? (NR).

Nesse sentido, observa-se que foram elencados os crimes específicos mediante fraude eletrônica objetivando tornar mais rigorosa a lei, ainda tentando acompanhar o avanço da criminalidade. Frisa-se que a Lei 14.155/21 deu ênfase também ao aumento da pena para esse crime na modalidade virtual, com pena de reclusão de 4 a 8 anos e o aumento de 1/3 ao dobro da pena acaso o crime seja praticado contra idoso ou vulnerável, com expectativa para prejudicar a prática delituosa.
15

Cabe destacar também a alteração quanto a competência para apuração do

estelionato por fraude mediante cheque ou transferência bancária, o código de processo penal previa que a competência era do local do banco sacado, o que muitas vezes dificultava a apuração do crime, até pela localização da vítima que nem sempre residia no mesmo local do banco sacado, competência esta alterada para o domicílio da vítima pela Lei 14.155/21.
Por fim, a execução da lei e a responsabilização dos golpistas submete-se a conduta das autoridades capazes, para investigar, processar e julgar os casos de estelionato digital, como a polícia e o poder judiciário.

4 O HISTÓRICO DA PRÁTICA DO ESTELIONATO DIGITAL E OS REFLEXOS DA LEI 14.155 FRENTE A VULNERABILIDADE DA VÍTIMA.

Como já demonstrado, o estelionato digital foi uma modalidade que cresceu esporadicamente com o advento da internet e o constante avanço da tecnologia, mas também teve um de seus marcos recentemente, em 2020, com crescimento exponencial pela pandemia da covid 19 que possibilitou mais ?vítimas? online.
Relativizando em números, o país registrou um aumento ainda mais expressivo que o estelionato comum quando em sua modalidade virtual, com direta relação a pandemia, em 2021 houve 120.470 (cento e cinto mil, quatrocentos e setenta) casos registrados, já em 2022 foram registrados 200.322 (duzentos mil, trezentos e vinte e dois) casos, um aumento de 66,2% (sessenta e seis virgula dois por cento) de acordo com os dados do Fórum Brasileiro de Segurança Pública (FBSP).
Foram registrados em 2021 115 (cento e quinze) estelionatos a cada 100 (cem) mil habitantes no país, já no ano seguinte foram registrados 189,9 (cento e oitenta e nove virgula nove), um aumento de 65,1% (sessenta e cinco vírgula um porcento), ainda de acordo com a FBSP o estado que detém o recorde de casos registrados de estelionato em sua modalidade digital é Santa Catarina, com 64.230 (sessenta e quatro mil, duzentos e trinta) registros em 2022 o que representa 32% (trinta e dois porcento) dos casos do país, ressalvando que Bahia, Ceará, Rio de Janeiro, Rio Grande do Norte, Rio Grande do Sul e São Paulo não tinham ou não disponibilizaram dados.
Cabe destacar que, além de Santa Catarina, tiveram relevantes aumentos Minas Gerais que passou de 25.574 (vinte e cinco mil, quinhentos e setenta e quatro)
16

casos em 2021 para 35.749 (trinta e cinco mil, setecentos e quarenta e nove) em 2022, um aumento de 49,4% (quarenta e nove vírgula quatro porcento), Distrito Federal que passou de 10.049 (dez mil e quarenta e nove) casos em 2021 para 15.580 (quinze mil, quinhentos e oitenta) em 2022, registrando um aumento de 55% (cinquenta e cinco porcento), e o Espírito Santo que passou de 10.545 (dez mil, quinhentos e quarenta e cinco) casos em 2021 para 15.277 (quinze mil, duzentos e setenta e sete) casos em 2022, o que resultou em um aumento de 44,8% (quarenta e quatro vírgula oito por cento).
Dentre todos esses dados disponibilizados pela FBSP cabe destacar por fim os

Estados que mais sofreram variações em seus índices, quais sejam Roraima que passou de 59 (cinquenta e nove) casos em 2021 para absurdos 759 (setecentos e cinquenta e nove) em 2022 acarretando um aumento de 1.186% (mil, cento e oitenta e seis por cento) e Goiás com um aumento de 1.041% (mil e quarenta e um porcento), passando de 128 (cento e vinte e oito) casos em 2021 para 1.461 (mil, quatrocentos e sessenta e um) casos em 2022.
Ainda sobre o marco recente que corroborou com a prática do referido delito é reiterado pelo Fórum Brasileiro de Segurança Pública (FBSP) que:

A digitalização das finanças, de serviço e do comércio, especialmente impulsionada durante o período pandêmico, contribui com a formação de um ambiente propício ao desenvolvimento de modalidades criminais que exploram vulnerabilidade nestes segmentos. (FBSP 2022, p. 6).

Conforme já citado, a modalidade de estelionato digital foi inserida ao Código Penal em meados de 2021 pela Lei nº 14.155/21 que também especificou o estelionato praticado na modalidade digital, por meio cibernético. Essa lei trouxe novidades legislativas que no geral foram positivas com relação a vulnerabilidade da vítima.
Destarte podemos citar que invadir dispositivo informático de uso alheio, ressalvando que conectado ou não a internet, com o fim de obter vantagem ilícita terá pena de reclusão de 4 (quatro) a 8 (oito) anos e multa, com suas devidas especificações, demonstrando assim a preocupação do legislador com as vítimas que infelizmente só estavam crescendo no país e isso refletiu no agravamento da pena que antigamente era disposta no crime de invasão de dispositivo informático, criando uma resistência ao criminoso na medida em que vê o crime como algo mais grave, mediante nova pena mais severa.
17

Ainda quanto aos reflexos dessa lei frente a vulnerabilidade da vítima podem-se listar os agravantes trazidos em sua redação quanto ao furto, com pena de reclusão de 4 a 8 anos, para o crime nessa modalidade realizado com o uso de dispositivos eletrônicos, conectados ou não a internet, por meio de uso de sistemas invasores ou violação de senha, além do agravamento se praticado contra idosos ou vulnerável com consequente aumento de pena de 1/3 ao dobro, ainda na hipótese de ser praticado por servidor fora do território nacional aumenta a pena de 1/3 (um terço) a 2/3 (dois terços).
Quanto ao estelionato também tornou-se agravante o furto qualificado no âmbito cibernético, com igual pena de reclusão de 4 (quatro) a 8 (oito) anos, além de possível multa e pode ter pena aumentada de 1/3 (um terço) a 2/3 (dois terços) acaso seja praticada por servidor fora do território nacional e acaso praticada contra idoso ou vulnerável poderá ter a pena aumentada de 1/3 (um terço) ao dobro.
Por fim, no que tange a invasão de aparelhos para obtenção de dados, a lei passou de detenção de 3 (três) meses a 1 (um) ano para reclusão de 1 (um) a 4

(quatro) anos. Ainda na hipótese de resultar em obtenção de informações sigilosos pode ser majorada de reclusão de 2 (dois) a 5 (cinco) anos e multa, com agravante de 1/3 (um terço) a 2/3 (dois terços) caso ocorra prejuízo econômico decorrente da invasão.
Assim, as novidades legislativas trazidas pela lei confortam brasileiros que podem ser vítimas de criminosos fora do território nacional, o que é plenamente possível pelo advento da internet e também a população mais velha que, em suma maioria, não tem familiaridade com as ferramentas e linguagens online, não tendo manejo e trato com os meios digitais o que por muitas vezes os torna os principiais focos dos criminosos pela ?facilidade? e ?inocência? desses usuários em específico, assim como os vulneráveis.
Portanto, resta claro que o legislador buscou efetivamente ampliar a guarda dos direitos, de modo a, buscar uma equidade entre diversos grupos de pessoas/possíveis vítimas, resultando em maior segurança, de modo que passa a observar significativas mudanças objetificando proteger os direitos do usuário e penalizando de forma mais grave os criminosos.

5 CONCLUSÃO.

O presente artigo, por meio da análise de dados estatísticos, legislação e julgados, buscou tecer uma análise crítica da disciplina normativa do estelionato digital, suas formas de conduta e as possíveis consequências sociais.
Demonstrando que a sociedade está cada vez mais conectada e as redes sociais têm uma função muito importante nessa interação, ocorre que o aumento desenfreado de pessoas conectadas à internet propiciou um ambiente para prática de crimes e com diversas possibilidades de artimanhas dos criminosos, que enxergam a internet como ?terra sem lei?, para obtenção da vantagem ilícita virtualmente, caracterizando o estelionato digital.
Dentre as diversas artimanhas utilizadas pelos estelionatários destacarm-se o ?phishing?, utilizada para enganar os usuários e conseguir informações privadas, ?vishing? popularmente conhecido por ?phishing por voz? quando o ato é realizado por ligações ou envio de áudios com o mesmo intuito de ludibriar a vítima, mas para divulgar dados pessoais e ?smishing? modalidade em que a vítima é provocada a acessar link que corrompe seu aparelho, além de outros golpes como investimentos fraudulentos, promessas de retornos financeiros utopicamente elevados e esquema de pirâmides, esses golpistas beneficiam-se da leiguice de suas vítimas no âmbito de investimento financeiro com falsas promessas de enriquecimento acelerado para enganá-las.
Assim, restou demonstrado que os golpistas tem o mesmo fito, qual seja a obtenção da vantagem ilícita fazendo uso do ambiente cibernético, enquadrando-os no âmbito de estelionatários digitais.
Nesta senda, ainda não existia um enquadramento específico para conter o

avanço do referido ilícito que muitas vezes poderia ser caracterizado como tentativa de extorsão ou crimes análogos o que obrigou o poder legislativo a se atualizar. Para ?frear? o avanço do crime foi introduzida a Lei 12.737/2012, popularmente conhecida por ?Lei Carolina Dieckmann?, que surgiu após um incidente em que a atriz teve seu aparelho pessoal invadido e com isso o vazamento de fotos íntimas na rede.
A introdução da Lei ?Carolina Dieckmann? mostrou-se muito importante por iniciar a caminhada rumo a tipificada do crime de estelionato em sua modalidade digital, ocorre que a tecnologia seguiu se modernizando trazendo novas oportunidades para inovação dos criminosos que vivem as sombras da internet. Com o estabelecimento de modalidades de transferência eletrônica como ?TED? e ?PIX?
19

tornou-se cada vez mais comum o embate entre as autoridades e os golpistas, já demonstrando a necessidade de nova atualização da legislação atinente ao tema.
Quanto a responsabilidade do crime no âmbito jurídico restou pacificado pelas jurisprudências pátrias que torna-se direta em relação ao Autor, sendo aferida pelo Estado que tem o dever de tutelar a convivência no âmbito cibernético. Cumpre destacar que nem sempre a responsabilidade é exclusiva do Autor, podendo recair de forma subjetiva ou objetiva para um terceiro da relação que deveria zelar pela segurança dos dados pessoais do usuário, tais como bancos, tomadores de serviço...
O marco de crescimento registrado no crime de estelionato na sua modalidade virtual foi durante a pandemia de covid 19, época em que foi necessário a reclusão da população em casa o que gerou aumento exponencial de usuários online na rede e, em paralelo, oportunidade para os criminosos inovarem suas artimanhas.
Para combater essa crescente negativa no âmbito jurídico nacional entrou em vigor a lei 14.155/21, de 27 de maio de 2021 trazendo enrijecimento das penas e tipificação de novos crimes, como estelionato contra idoso ou vulnerável e fraude eletrônica, intentando ainda em penas mais rigorosas que podem ser alongadas a depender do caso e alteração de competência para estelionato por fraude mediante cheque ou transferência bancária, submetendo a execução da lei e responsabilização dos golpistas a conduta das autoridades capazes.
O que se conclui é que, com o passar dos anos as leis e medidas tomadas se tornam ultrapassadas vide o ?aperfeiçoamento? dos criminosos, portanto, com o fito do controle do Estado se tornar uma manutenção mais célere se mostrou necessário inserção de um sistema de inovação e renovação legislativa.
Ora, restou comprovado que o âmbito jurídico sempre buscou acompanhar a inovação criminosa trazendo atualizações a legislação para coibir a progressão desses ataques criminosos, mas igualmente restou comprovado que apenas acompanhar não está mais sendo o suficiente, tornando tendência o adiantamento aos movimentos da marginalidade com sucessivo progresso de imersão tecnológica das autoridades para se adiantar ao crime com a devida manutenção das leis de forma mais célere objetivando deter o claro avanço da criminalidade hodierna.

REFERÊNCIAS

20

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez.

BRASIL, DECRETO-LEI NO 2.848, DE 7 DE DEZEMBRO DE 1940. Código Penal. Rio de Janeiro, 7 de dezembro de 1940; 119º da Independência e 52º da República. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 08/06/2023.

BRASIL. LEI Nº 14.155, DE 27 DE MAIO DE 2021. Lei de Invasão a Dispositivo Informático [Internet]. Disponível em: https://www.in.gov.br/en/web/dou/-/lei-n-14.155-de-27-de-maio-de-2021-322698993. Acesso em: 24 nov. 2023

BRASIL. LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012. Lei de Invasão a Dispositivo Informático [Internet]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em:
24 nov. 2023.

BRASIL. LEI Nº 14.155, DE 27 DE MAIO DE 2021. Lei de Invasão a Dispositivo Informático [Internet]. Disponível em: https://www.in.gov.br/en/web/dou/-/lei-nº 14.155-de-27-de-maio-de-2021-322698993. Acesso em: 13 dez. 2023.

BRASIL. Tribunal de Justiça do Paraná. TJ-PR - Recurso Inominado XXXXX-67.2020.8.16.0136 PR. Relator Nestario da Silva Queiroz. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-pr/1511018743. Acesso em: 25 nov. 2023

BRASIL. Tribunal de Justiça do Rio Grande do Sul. TJ-RS - Apelação Cível XXXXX-22.2020.8.21.7000 RS. Relator Giovanni Conti. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-rs/932015329. Acesso em: 25 nov. 2023

BRITO, Auriney. Direito penal informático. São Paulo: Saraiva, 2013, p.189.

CAMPOS, Pedro Franco de [et al.]. Direito penal aplicado: parte geral e parte especial do Código Penal. - 6ª. Ed. ? São Paulo: Saraiva, 2016.

CASSANTI, Moisés de Oliveira. Crimes virtuais, vítimas reais. 1ª ed. Rio de Janeiro: Brasport, 2014, p.6.

CHAVES, Fábio Barbosa; TEIXEIRA, Filipe Silva. Os crimes de fraude e estelionato cibernético e a proteção do consumidor no e-commerce. 2020. Disponível em: <https://conteudojuridico.com.br>. Acesso em: 12/06/2023.

COELHO, Yuri Carneiro. Curso de Direito Penal Didático. vol. único, 2ª ed. ? São Paulo: Atlas, 2015.

CÔRREA, Gustavo Testa. Aspectos jurídicos da internet. 5. ed. rev. e atual. São Paulo, Saraiva, 2010.

CUNHA, Rogério Sanches. Manual de direito penal: parte especial (arts. 121 ao 361). 11. ed. rev., ampl. e atual. Salvador: JusPODIVM, 2019.
21

CUNHA, Rogério Sanches. Lei 14.155/21 e os crimes de fraude digital - primeiras impressões e reflexos no CP e no CPP. Meu Site Jurídico (JusPodivm), 2021. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2021/05/28/lei-14-15521-e-os-crimes-de-fraude-digital-primeiras-impressoes-e-reflexos-no-cp-e-no-cpp/. Acesso em: 13 dez. 2023.

FBSP. Fórum Brasileiro de Segurança Pública. Os crimes patrimoniais no Brasil: entre novas e velhas dinâmicas. Anuário Brasileiro de Segurança Pública, 2022. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2022/07/07-anuario-2022-os-crimes-patrimoniais-no-brasil-entre-novas-e-velhas-dinamicas.pdf. Acesso em 24 nov. 2023.

GENNARINI, Juliana. Revista de Direito Penal e Processo Penal, ISSN 2674-6093, v. 2, n. 2, jul./dez. 2020.

GONÇALVES, Victor Eduardo Rios. Direito penal esquematizado: parte especial do Código Penal. - 8. ed. ? São Paulo: Saraiva Educação, 2018.
GRECO, Rogério. Curso de Direito Penal: parte especial. v. III. 7. ed. Rio de Janeiro: Ed. Impetus, 2010.

GOUSSINSKY, Eugenio. Crimes digitais têm forte alta em vários estados; saiba como prevenir. Portal R7, 2021. Disponível em: https://noticias.r7.com/tecnologia-e-ciencia/crimes-digitais-tem-forte-alta-em-varios-estados-saiba-como-prevenir-05052021. Acesso em: 12 dez. 2023.

GRECO, Rogério. Curso de Direito Penal: parte especial. v. III. 7. ed. Rio de Janeiro: Ed. Impetus, 2010, p. 228.

HUNGRIA, Nelson. Comentários ao Código Penal ? Vol. IX. Rio de Janeiro: Forense, 1958.

MIRABETE, Júlio Fabbrini e FABBRINI, Renato N./ Manual de direito penal: parte

especial: arts. 121 a 234-B do CP ? volume 2, 36° edição, São Paulo, Atlas, 2021.

==========

Arquivo 1: Trabalho de ConclusÃ£o de Curso - Rafael Garcia.pdf (6280 termos)
Arquivo 2: https://www.avg.com/pt/signal/what-is-a-vishing-attack (3004 termos)
Termos comuns: 19
Similaridade: 0,20%
O texto abaixo é o conteúdo do documento Trabalho de ConclusÃ£o de Curso - Rafael Garcia.pdf (6280 termos)
Os termos em vermelho foram encontrados no documento https://www.avg.com/pt/signal/what-is-a-vishing-attack (3004 termos)

==========

ESTELIONATO DIGITAL: UMA ANÁLISE CRÍTICA DA DISCIPLINA NORMATIVA, SUAS FORMAS DE CONDUTA E AS POSSÍVEIS CONSEQUÊNCIAS SOCIAIS

Rafael Lemos Garcia de Oliveira1
Ricardo Simões Xavier dos Santos2

Resumo
O presente artigo discorre sobre a figura do estelionato digital, fazendo uma análise crítica da disciplina normativa, suas formas de conduta e as possíveis consequências sociais. É notório que a atual legislação do país tem avançado, conforme mencionado, na forma que tipifica os crimes que ocorrem em meios virtuais, todavia as sanções ainda são moderadas e as normas devem avançar no sentido de impedir a prática dos crimes virtuais. Para que seja viável a hipótese narrada, o Estado tem o dever de incrementar métodos novos de apuração e averiguação e aprimorar os recursos tecnológicos e digitais que estão à disposição das autoridades responsáveis. Nesse sentido, é necessário compreender o que é o estelionato digital, suas características, maneiras de prevenção e formas em que pode aparecer no dia a dia dos usuários da rede, compactuando com a legislação penal e o cabimento de penalização para os criminosos que praticam esse crime. Por fim, conclui-se que a legislação penal brasileira vem evoluindo, mas para que alcance um nível suficiente de eficácia no combate a esse crime é necessário compreender o que é o estelionato digital, suas características, maneiras de prevenção e formas em que pode aparecer no dia a dia dos usuários da rede, compactuando com a legislação penal e o cabimento de penalização para os criminosos que praticam esse crime.

PALAVRAS-CHAVE: Internet. Crime Cibernético. Estelionato Digital. Código Penal.

1 Graduando em bacharelado em direito pela UCSAL. E-mail: rafaell.oliveira@ucsal.edu.br
2 Doutor em Políticas Sociais e Cidadania pela Universidade Católica do Salvador ? UCSal. E-mail:

ricardo.santos@pro.ucsal.br
2

ABSTRACT: This article discusses the figure of digital fraud, making a critical analysis of the normative discipline, its forms of conduct and the possible social consequences. It is notable that the country's current legislation has advanced, as mentioned, in the way it typifies crimes that occur in virtual media, however sanctions are still moderate and standards must advance in order to prevent the practice of virtual crimes. In order for the narrated hypothesis to be viable, the State has the duty to increase new methods of investigation and investigation and improve the technological and digital resources that are available to the responsible authorities. In this sense, it is necessary to understand what digital fraud is, its characteristics, methods of prevention and ways in which it can appear in the daily lives of network users, in agreement with criminal legislation and the appropriateness of penalizing criminals who practice this crime. Finally, it is concluded that Brazilian criminal legislation has been evolving, but in order to achieve a sufficient level of effectiveness in combating this crime, it is necessary to understand what digital fraud is, its characteristics, methods of prevention and forms in which it can appear. in the daily lives of network users, complying with criminal legislation and the appropriateness of penalizing criminals who commit this crime.

KEYWORDS: Internet. Cybercrime. Digital Fraud. Penal Code.

SUMÁRIO: 1 INTRODUÇÃO. 2 CONDUTA DO ESTELIONATO DIGITAL: CONCEITOS PRÉVIOS, DISCUSSÕES INICIAIS E FORMAS APRESENTADAS. 2.1 Análise acerca das eventuais consequências sociais advindas da conduta do estelionato digital 3 A RESPONSABILIZAÇÃO DO CRIME DE ESTELIONATO DIGITAL NO ÂMBITO JURÍDICO 3.1 Concepção das normas jurídicas atualizadas e formas de punição do crime do estelionato digital 4 O HISTÓRICO DA PRÁTICA DO ESTELIONATO DIGITAL E OS REFLEXOS DA LEI 14.155 FRENTE A VULNERABILIDADE DA VÍTIMA 5 CONCLUSÃO 6 REFERÊNCIAS

1 INTRODUÇÃO

No âmbito penalista são diversos os crimes que têm como objetivo a obtenção de lucros financeiros da vítima, o referido trabalho tem como objetivo abordar o estelionato digital fazendo uma análise crítica da disciplina normativa, apresentando suas formas de conduta e relacionando a suas possíveis consequências sociais.
3

Há uma previsão legal do Código Penal em garantir que todos os cidadãos lesados por práticas de golpes, em que são utilizados artifícios ou qualquer meio fraudulento, podem ingressar no juízo criminal a fim de prosseguirem com a punição penal e com o ressarcimento dos prejuízos.
Para breve introito, o estelionato é 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.
Dentre os crimes mais comuns no Brasil e no mundo pode-se destacar o estelionato, além do meio físico os criminosos procuram pela navegação na rede com o fito de obtenção de dados e informações das pessoas que tem perfil para serem suas possíveis vítimas, pondo em prática das mais diversas maneiras tais como ligações, mensagens, falsificação de identidade, haja vista que todos os dias, a população vive a internet, cadastrando senhas, trocando mensagens, adentrando redes sociais, fazendo negócios pela internet...
Nesse sentido, acompanhando o aumento dos usuários das redes a realização de crimes online cresceu consideravelmente, obviamente relacionado a simplicidade de manejo dos meios virtuais e pela dificuldade de identificação dos criminosos para posterior punição, haja vista ausência de legislações específicas e supressão das identidades.
A realização de golpes e fraudes cometendo ilícitos para obter vantagem sob outras pessoas é prática recorrente e por muitas vezes impune no Brasil, com o estelionato digital não é diferente.
Em sua esfera digital ele se configura quando o criminoso submete o aparelho da vítima e sincroniza-o a demais sistemas de informação ou, em outra hipótese, quando a vítima é posta em uma conjuntura de sensibilidade para obtenção de vantagem ilícita. Na atualidade é mais comum do que se imagina conhecer alguém que tenha passado por essa situação e caído nesse golpe, desde ligações de números sem chamador ou desconhecidos a e-mails/mensagens com ofertas incríveis.
Outro ponto importante que contribuiu para esse aumento, além da facilidade no manejo dos meios virtuais foi o advento da pandemia do Covid-19, as práticas desses crimes se multiplicaram, haja vista que, relevante porcentagem da população tanto brasileira quanto mundial, se viu obrigada a passar mais tempo em casa, o que, em consequência, ampliou o número de pessoas online, acessando a rede. Neste liame, os criminosos têm agido cada vez mais e feito várias vítimas no mundo virtual.
4

Para que o crime possa ser classificado como estelionato digital é imprescindível que a entrega das informações pela vítima seja de forma voluntária, haja vista que a obtenção dos dados se deu por outros meios, o crime pode ter outra classificação, tal como ?furto mediante fraude eletrônica?.
Dentre as principais vítimas desse crime tão comum na atualidade estão as pessoas desatentas e que não tomam total atenção para se esquivar dos estelionatários, seguindo as hipóteses de compra e venda pela internet não verificando a fonte, se é de confiança etc., links enviados de números aleatórios possibilitando o acesso do criminoso a rede da vítima entre outros...
A despeito da clara regulação e evolução da internet e redes sociais, os conselhos e observações para a premeditação dos crimes digitais em geral continua sendo de cuidado e cautela com os dados pessoais e sua divulgação, ainda com o remetente e usuários/links que adentra. É necessário que sempre pense que tudo que

identifique quem você é ou que busque saber informações que só você teria acesso são o alerta inicial para entender se não se está diante de uma possível tentativa de estelionato digital.
É notório que a atual legislação do país tem avançado, conforme mencionado, na forma que tipifica os crimes que ocorrem em meios virtuais, todavia as sanções ainda são moderadas e as normas devem avançar no sentido de impedir a prática dos crimes virtuais. Para que seja viável a hipótese narrada, o Estado tem o dever de incrementar métodos novos de apuração e averiguação e aprimorar os recursos tecnológicos e digitais que estão à disposição das autoridades responsáveis.
Nesse sentido, é necessário compreender o que é o estelionato digital, suas características, maneiras de prevenção e formas em que pode aparecer no dia a dia dos usuários da rede, compactuando com a legislação penal e o cabimento de penalização para os criminosos que praticam esse crime.
Assim, as perguntas que ficam são quais as formas de conduta do estelionato digital e seus impactos na sociedade, além do questionamento acerca das normas brasileiras, nosso sistema jurídico atual contempla qual espécie de responsabilização para o crime de estelionato digital, alinhado a isso, como o Estado Democrático Brasileiro pode melhorar para combater o aumento desse crime.
No presente artigo, seguindo após a introdução para o capítulo ?2? onde serão apresentadas as condutas do estelionato digital, seus conceitos prévios e formas apresentadas, a diferença entre o estelionato e outros crimes contra o patrimônio e
5

sua forma de proliferação pela rede mediante sites falsos, mensagens e e-mails. O capítulo ?2? contém ainda um subtópico ?2.1? onde serão analisadas as consequências sociais advindas da conduta do estelionato digital, desde a inovação dos criminosos partindo para o meio digital até os ?traumas? das vítimas e sua repercussão na sociedade.
Já no capítulo ?3? será amplamente explicada a quem deve ser dirigida a responsabilidade pelo crime do estelionato digital, no âmbito jurídico, já que o crime na grande maioria das vezes tem por conclusão a ?fuga? do criminoso pelo meio cibernético. Ainda no capítulo ?3? serão exploradas, mediante subtópico ?3.1?, as normas jurídicas atualizadas e formas de punição do crime tendo relação direta com a ampla possibilidade de escape do criminoso.
Por fim, em capítulo ?4?, será demonstrado o histórico da prática do estelionato digital, sua evolução paralela ao avanço da tecnologia na sociedade e os reflexos da Lei 14.155, instituída em 2021 especialmente para tornar mais grave a pena de estelionato cometido de forma eletrônica pela internet, frente ainda a vulnerabilidade da vítima. Seguidos da conclusão e as referências bibliográficas.
De certo, cumpre-se destacar que a pesquisa em questão, valeu-se do método da revisão bibliográfica de trabalhos científicos atualizados das áreas penal e constitucional, frente às questões sociais, publicadas em periódicos nacionais e internacionais, qualificados como publicações de A1, assim como B1. Além de importantes nomes do cenário retrato, ao passo que se cita Rogério Greco e Fabio

Barbosa Chavez, bem como análise jurisprudencial e legislativa da lei 14.155.
Compreende-se então, que a escolha metodológica se justifica de base teórica, fundada em estudos atualizados sobre o estelionato digital, suas formas de conduta e as consequências sociais.
O foco da pesquisa bibliográfica foi de apresentar informações e dados específicos sobre a evolução dos crimes digitais, exibindo o progresso do direito penal frente os crimes digitais, através da análise filosófica e de referenciais teóricos de artigos, códigos e outros trabalhos sobre a mesma questão jurídica. Assim, o método empregado é de leitura e análise de material doutrinário especializado já existente sobre o tema de Direito Penal, tal como de jurisprudência, dados, legislação e artigos científicos.

6

2 CONDUTA DO ESTELIONATO DIGITAL: CONCEITOS PRÉVIOS, DISCUSSÕES INICIAIS E FORMAS APRESENTADAS.

O termo estelionato está disposta no Art. 171 do Código Penal como:

Art. 171. Obter, para si ou para outrem, vantagem ilícita em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: pena ? Reclusão, de 1 (um) a 5 (cinco) anos, de multa.

Trata-se de crime contra o patrimônio onde a legislação penal visa proteger a inviolabilidade patrimonial orientada pela prática de atos que visam enganar a vítima e beneficiar o agente (CUNHA, 2019, p. 345).
Assim, pode-se inferir que a diferença entre o estelionato e os diversos crimes contra o patrimônio, ou seja, crimes que tenham por objetivo atentar contra o patrimônio de uma pessoa ou organização, é que no estelionato não é utilizada a força para obtenção de ?vantagem?. É sabido, portanto, que essa atitude é conhecida há muitos anos, de modo que Greco cita que:

Desde que surgiram as relações sociais, o homem se vale da fraude para dissimular seus verdadeiros sentimentos e intenções para, de alguma forma, ocultar ou falsear a verdade, a fim de obter vantagens que, em tese, lhe seriam indevidas (GRECO, 2019, p. 228).

Ressalta-se que o crime existe apenas na modalidade dolosa, sem previsão na forma culposa.
A respeito da expressão ?vantagem ilícita?, Fernando Capez (2020) ensina que, esta, trata-se do objeto material do crime e, caso o agente esteja agindo em razão de uma vantagem devida, a conduta é tipificada como exercício arbitrário das próprias razões, delito previsto no art. 345, do Código Penal.
De acordo com o que se retira do artigo 171, do supramencionado dispositivo

legal, o estelionato pode ser cometido mediante artificio, ardil ou qualquer outro meio fraudulento. Em relação ao termo ?artificio?, o doutrinador Júlio Fabbrini Mirabete ensina o seguinte:

?o artifício existe quando o agente se utilizar de um aparato que modifica, ao menos aparentemente, o aspecto material da coisa, figurando entre esses meios o documento falso ou outra falsificação qualquer, o disfarce, a modificação por aparelhos mecânicos ou elétricos, filmes, efeitos de luz etc.? (MIRABETE, 2021, pag. 325).

Em sua modalidade digital o estelionato ocorre através de sites falsos, mensagens e até e-mail, sendo prioritariamente focado no âmbito virtual. É bastante
7

normal que o consumidor busque virtualmente os mesmos bens desejados fisicamente, mas com a comodidade de não se deslocar e em grande maioria dos casos a acessibilidade com preços menores, levando a promessa da oferta muitas vezes a encantar o consumidor que não percebe a fraude.
Dentre as formas de conduta do referido crime podem ser listadas as mais comuns sendo: vendas falsas em sua maioria quando os estelionatários oferecem serviços ou produtos inexistentes em redes sociais e/ou sites e links de comércio eletrônico; ?phishing?, uma artimanha utilizada pelos criminosos para enganar os usuários e conseguir informações privadas, tais como senhas, detalhes de cartões de crédito, comumente realizado por meio do envio de mensagens eletrônicas se passando por instituições de confiança, pode ser realizado por sites e por redes sociais também, mas sempre com o intuito de prejudicar e obter vantagem, ?vishing? popularmente conhecido por ?phishing por voz? quando o ato é realizado por ligações ou envio de áudios com o mesmo intuito de ludibriar a vítima, mas para divulgar dados pessoais, ?smishing? realizada também por mensagem, mas nessa modalidade a vítima é provocada a acessar link que corrompe seu aparelho, e por último os golpes de investimentos fraudulentos que podem acontecer de diversas maneiras, tais como promessas de retornos financeiros utopicamente elevados e esquema de pirâmides, esses golpistas beneficiam-se da leiguice de suas vítimas no âmbito de investimento financeiro com falsas promessas de enriquecimento acelerado para enganá-las.
No Art. 171 do Código Penal, o estelionato possui a pena de reclusão de 1 a 5 anos e multa. Diante disso, o crime admite suspensão condicional no processo de acordo com o art. 89, § 1ª, da Lei dos Juizados Especiais - Lei n. 9099/95:

Art. 89. Nos crimes em que a pena mínima cominada for igual ou inferior a um ano, abrangidas ou não por esta Lei, o Ministério Público, ao oferecer a denúncia, poderá propor a suspensão do processo, por dois a quatro anos, desde que o acusado não esteja sendo processado ou não tenha sido condenado por outro crime, presentes os demais requisitos que autorizariam a suspensão condicional da pena (art. 77 do Código Penal).

Conforme dito, o crime de estelionato digital, no sistema jurídico atual do Brasil, é apreciado no âmbito do Direito Penal o qual pressupõe responsabilização penal para esse tipo de ato, o qual era equiparado ao crime de estelionato, previsto no artigo 171 do Código Penal, ocorre que ainda no caminhar para a especificação do crime de estelionato na modalidade digital foi introduzida a Lei 12.737/2012, ou como é popularmente conhecida a ?Lei Carolina Dieckmann?, que surgiu após um incidente 8

em que a atriz teve seu aparelho pessoal invadido e com isso o vazamento de fotos íntimas na rede, mediante ainda tentativa de extorsão.
Na época em questão os criminosos seriam apenas denunciados pelo crime de tentativa de extorsão, haja vista ausência de legislação específica quanto aos crimes digitais, assim vários projetos de lei foram analisados para tentar tipificar condutas para crimes semelhantes ao sofrido pela atriz e findada essa fase foi sancionada a Lei 12.737/2012 que entrou em vigor em 02 de abril de 2013.
A lei visava combater o vazamento de informações pessoais dos usuários das redes, zelando pela proteção da privacidade dos mesmos, ainda acrescentou ao Código Penal, mais especificamente no Decreto-Lei 2848, os artigos 154-A e 154-B.

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

A lei se demonstrou efetiva a época da sanção sendo citada como um marco legislativo por muitos autores, desde que entrou em vigor a invasão de computadores, celulares, tablets...no geral dispositivos informáticos alheios passou a ser crime.
Cabe destacar que execução da lei e a responsabilização dos golpistas submete-se a conduta das autoridades capazes, para investigar, processar e julgar os casos de estelionato digital, como a polícia e o Poder Judiciário.

2.1 ANÁLISE ACERCA DAS EVENTUAIS CONSEQUÊNCIAS SOCIAIS ADVINDAS DA CONDUTA DO ESTELIONATO DIGITAL.

A sociedade está cada vez mais conectada e as redes sociais têm uma função muito importante nessa interação, vez que o ser humano sempre precisou de convívio

social. Assim, tais ferramentas estão presentes na vida de muitos brasileiros e esse ambiente digital, como já evidenciado, tornou-se, também, um meio para a prática de crimes, seja pela facilidade de acesso e/ou pelo grande número de usuários.
9

Na atualidade existe uma grande facilidade na obtenção de produtos, sendo de maneira virtual, de modo que não existe mais a necessidade do consumidor se deslocar até o fornecedor para adquirir o produto, nesta feita, é notório que a compra virtual vem amadurecendo cada vez mais, o que consequentemente ocasiona um aumento dos crimes cibernéticos. Nesse contexto, Chaves e Teixeira destacam que:

Com a investigação correta é possível localizar e punir os criminosos que causaram prejuízo a essa nova espécie de consumidores. Todavia, no mesmo ritmo que a internet evolui, os fraudadores também se renovam com novas modalidades de golpes, alguns tão específicos que são até difíceis de definir qual a punição correta a ser aplicada (CHAVES e TEIXEIRA, 2019, p. 119).

Conforme já citado a inovação dos criminosos acompanha em paralelo o avanço da tecnologia pela sociedade, de modo que muitos usuários têm a sensação de que a internet é ?terra sem lei? fomentando sua ?liberdade tecnológica? em pequenos delitos, tais como injúria, difamação... Ao passo em que não imaginam ter a sua responsabilidade realmente comprovada, agindo por trás da tela do celular ou computador.
Perpassando por isso os criminosos buscam a obtenção de vantagem ilícita e veem na internet uma oportunidade recheada de opções, possuídos pela sensação de impunidade e munidos das mais diversas artimanhas para concluir seu objetivo. Cumpre ressaltar que sociedade caminha para um futuro mais tecnológico e os criminosos ?surfam nessa onda?.
A cada dia que passa resta mais rudimentar os métodos de pagamento por cédulas ou moedas, a trajetória da população tem destino eletrônico, de modo que é fato notório o quão comum se tornaram os sistemas de pagamento eletrônico, estando já alguns mais rudimentares como a transferência ?TED?.
A popularização dos sistemas de pagamento eletrônico, a exemplo do ?pix?, propicia diariamente um combate necessário entre as autoridades e os golpistas. Já é rotina na sociedade a divulgação de novos meios de golpes cibernéticos com o fito de alertar os usuários a se precaverem mais, infelizmente nem sempre todo cuidado é tomado e as consequências podem ser desastrosas para os consumidores da rede.
O prejuízo causado a essa nova espécie de consumidores afeta tanto de forma direta as vítimas quanto a sociedade, de maneira geral. Dentre as consequências sociais advindas dessa conduta resta mister destacar o impacto financeiro nas vítimas, de forma direta, que podem encarar perdas financeiras o que acarreta
10

problemas emocionais e instabilidade, perda de confiança no meio digital para compras que também gera impacto na maneira como as pessoas conduzem negócios online.
Além do consumidor direto, as instituições financeiras também sofrem em muitos casos ressarcindo o valor perdido por seus clientes lesados, arcando com o custo de fraude e também no investimento em segurança virtual, mesmo ainda tendo um receio a implantação dos pagamentos digitais buscando ao máximo reforçar sua segurança desde confirmação por ?face id? quanto senhas regularmente trocadas e ?tokens digitais?, sempre tentando confirmar que é realmente o usuário da conta quem realmente está fazendo a operação e não um terceiro. Frisa-se que essas consequências sociais acarretam, num todo, impacto na economia.
Felizmente, não são somente os consumidores que passam pelo processo de consequências negativas, mas também os fraudadores. Mesmo diante da crescente a qual ocorre o ?fenômeno? do estelionato digital, os criminosos não restam imunes a responsabilização pelo seu crime. Conforme será demonstrado no presente artigo, a legislação do país delimita o crime e suas consequências, assim como as penalidades que podem levar os fraudadores a condenação pelas atividades ilícitas.
Nesse sentido, o avanço da tecnologia com o passar dos tempos corroborou indiretamente para que os criminosos inovassem seus meios ilícitos para obtenção de vantagens, causando diversos impactos na sociedade que não teriam como ser positivos, sendo alguns dos principais o prejuízo financeiro as vítimas; perda de confiança na segurança online e transações digitais, além do choque nos sistemas judiciais, de segurança e nas bases digitais o que consequentemente requer mecanismos e investimentos relevantes de atribuição das empresas e do judiciário.
Sendo assim, infere-se que ainda existe certa dificuldade para identificação dos golpistas o que, alternativamente, tem relação com a legislação brasileira que tem avançado na tipificação dos crimes cibernéticos, todavia as sanções ainda são moderadas e as normas devem acompanhar no sentido de bridar a prática desses crimes na modalidade virtual.

3 A RESPONSABILIZAÇÃO DO CRIME DE ESTELIONATO DIGITAL NO ÂMBITO JURÍDICO.

11

É claro que a internet e toda a esfera digital não foi inserida na sociedade com o intuito ou sequer resguarda em relação a possibilidade do advento de crimes em paralelo a isso, mas como toda imprevisão, a criminalidade evoluiu em conjunto deixando cada vez mais vulnerável a segurança dos usuários na rede, como amplamente demonstrado no presente trabalho, os golpes digitais se aperfeiçoam com o passar dos anos, com ênfase para o estelionato que conta hoje com diversos tipos de obtenção de vantagem ilícita na sua modalidade digital.
A internet tornou-se essencial na rotina da população, interligando usuários e pessoas conectadas a rede, assim, como bem destacou Uchoa de Brito:

(...) O problema da internet passou a ser identificado quando a tecnologia incrementou e complicou as relações sociais consideradas, até então, pacíficas e controladas, possibilitando algumas experiências socialmente desagradáveis e indesejadas, como a sua utilização para a prática de crimes, e a criação de novos contatos que colocam em risco bens que ainda não tiveram sua relevância reconhecida pelo Direito. (BRITO, 2013, p. 9).

Assim, a prática do estelionato na modalidade virtual cresceu ao longo dos anos, sempre com a tentativa em paralelo do Direito Penal de acompanhar para poder punir em cerceamento legislativo, com projetos de lei, inovações e acréscimos a legislações já vigentes.
Quanto a responsabilização do crime em questão torna-se direta em relação ao Autor, sendo aferida pelo Estado, mesmo em sua modalidade digital, haja vista que tem o encargo de combater, controlar e reprimir tais práticas tanto no mundo ?real? quanto no ambiente digital, além de ser responsável por tutelar a convivência e atuação neste âmbito cibernético.
Além da responsabilização direta quanto ao autor do delito, muitas vezes a responsabilidade também recai de forma subjetiva ou objetiva para um terceiro da relação que deveria zelar pela segurança dos dados pessoais do usuário, grandes exemplos são os de vazamento de dados bancários online após invasão por hackers, recaindo responsabilidade também para os bancos que deveriam proteger o consumidor.

APELAÇÃO CÍVEL. NEGÓCIOS JURÍDICOS BANCÁRIOS. AÇÃO DE INDENIZAÇÃO POR DANOS MATERIAIS. RESSARCIMENTO DE VALORES. TRANSAÇÃO BANCÁRIA REALIZADA DE FORMA FRAUDULENTA POR TERCEIROS. INTERNET BANKING. RESPONSABILIDADE DO BANCO. SUMULA 479 DO STJ. SENTENÇA MANTIDA. As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias. Súmula 479 do STJ. Art. 14 do CDC. Para
12

responsabilização do prestador de serviços a existência de culpa ou dolo, exige-se apenas a conduta ilícita e a existência de dano, bem como nexo de causalidade entre eles. Caso. Autora que foi vítima de estelionato praticado por terceiro. Empréstimo autorizado pela instituição financeira. Nesse ponto, desimporta que a fraude tenha se perpetrado através dos canais de atendimento via internet (internet banking), porquanto a parte autora negou ter sido a autora dos saques, e o banco não se desincumbiu do ônus de demonstrar a regularidade das transações impugnadas pelo cliente. NEGARAM PROVIMENTO AO APELO. UNÂNIME.

Entre outros exemplos de golpes como os já citados ?phishing?, ?vishing? e ?smishing? que buscam a obtenção de vantagem ilícita frente as vítimas, muitas vezes fazendo uso de um terceiro como ponte para alçar seu objetivo fraudulento, ocorre que, como mencionado, mesmo esse terceiro não tendo o dolo na prática do crime deve garantir a segurança e impermeabilidade do seu sistema para que isso não ocorra, contando com a obrigação de assegurar os direitos do consumidor e usuário. Este é o entendimento das jurisprudências pátrias:
RECURSO INOMINADO. AÇÃO DECLARATÓRIA DE INEXISTÊNCIA DE DÉBITO C/C INDENIZAÇÃO POR DANOS MORAIS. PRELIMINAR DE VIOLAÇÃO AO PRINCÍPIO DA DIALETICDADE. INOCORRÊNCIA. BANCÁRIO. TRANSFERÊNCIA DE VALORES REALIZADA POR TERCEIRO. FRAUDE EVIDENCIADA. CULPA DA VÍTIMA NÃO CONFIGURADA. INSTITUIÇÃO FINANCEIRA QUE NÃO APRESENTOU PROVAS ACERCA DA SEGURANÇA, AUTENTICAÇÃO OU IDENTIFICAÇÃO DA OPERAÇÃO. FALHA NA PRESTAÇÃO DO SERVIÇO CONFIGURADA. RESPONSABILIDADE OBJETIVA DO BANCO. APLICAÇÃO DA SÚMULA 479 DO STJ. RESTITUIÇÃO DEVIDA. AUSÊNCIA DE SOLUÇÃO ADMINISTRATIVA. DANO MORAL CONFIGURADO NO CASO CONCRETO. QUANTUM ARBITRADO EM R$ 2.000,00 (DOIS MIL REAIS) QUE COMPORTA MAJORAÇÃO PARA R$ 3.000,00 (TRÊS MIL REAIS). OBSERVÂNCIA AOS PRINCÍPIOS DA PROPORCIONALIDADE E RAZOABILIDADE. SENTENÇA PARCIALMENTE REFORMADA. Recurso da autora conhecido e provido.Recurso do réu conhecido e desprovido. (TJPR - 1ª Turma Recursal - 0003317-67.2020.8.16.0136 - Pitanga - Rel.: JUIZ DE DIREITO DA TURMA RECURSAL DOS JUIZADOS ESPECIAIS NESTARIO DA SILVA QUEIROZ - J. 23.05.2022)
(TJ-PR - RI: 00033176720208160136 Pitanga 0003317-67.2020.8.16.0136 (Acórdão), Relator: Nestario da Silva Queiroz, Data de Julgamento: 23/05/2022, 1ª Turma Recursal, Data de Publicação: 23/05/2022)

Ressalta-se que o estelionato na sua modalidade digital é considerado crime de ação penal pública incondicionada, ou seja, a responsabilidade para conduzir o procedimento é do Ministério Público, independente de manifestação de vontade da vítima, a natureza dessa ação ressalva a relevância de tratar esse delito de forma mais eficaz, independente da vontade da vítima de ver o autor do crime responsabilizado, com o fito de preservar a ordem social e diminuir o índice de novos casos.
13

Nesse sentido, cumpre destacar que mesmo a responsabilidade do crime ser direta em relação ao Autor, também pode abranger mais partes do processo dependendo da especificada do caso. A jurisprudência entende que a responsabilidade não é apenas do Estado, mas também da empresa, entidade ou qualquer terceiro que tenha a obrigação de tornar o ambiente digital seguro para o

usuário.

3.1 CONCEPÇÃO DAS NORMAS JURÍDICAS ATUALIZADAS E FORMAS DE PUNIÇÃO DO CRIME DO ESTELIONATO DIGITAL.

Como já explicitado, um grande fator que desencadeou o aumento da efetivação do crime em questão foi a pandemia, de modo que, com o advento do Covid-19, foi necessário que a população se protegesse em suas casas para corroborar com o distanciamento social e assim evitar a proliferação do vírus, ocorre que em contrapartida a isso foi destaque a aproximação online dos usuários que culminou em oportunidade para os criminosos inovarem suas artimanhas, contando com a suposta sensação de anonimato.
O crime de estelionato digital, no sistema jurídico atual do Brasil, é apreciado no âmbito do Direito Penal, o qual pressupõe responsabilização para esse tipo de ato, que era equiparado ao crime de estelionato, previsto no artigo 171 do Código Penal.
A Lei 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann, entrou em vigor como uma tentativa inicial de tipificar a conduta dos crimes na modalidade virtual para proteção dos dados pessoais da população em face aos criminosos virtuais, ocorre que com o passar dos anos se mostrou necessária a inclusão de novas medidas frente a progressão da criminalidade no país, em específico os crimes virtuais.
Para combater essa crescente negativa no âmbito jurídico nacional entrou em vigor a lei 14.155/21, de 27 de maio de 2021, que incluiu e modificou alguns parágrafos no supramencionado dispositivo legal, alterando algumas regras para julgar o crime.

Art. 1º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar com as seguintes alterações:
?Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
14

§ 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.
§ 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso:
I ? 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;
II ? Aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável. Pena ? reclusão, de 1 (um) a 4 (quatro) anos, e multa.

§ 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. Pena ? reclusão, de 2 (dois) a 5 (cinco) anos, e multa.

Dentre as alterações, foram incluídos os § § 2º-A e 2º-B, que tratam de fraude eletrônica, sendo o § 2º-A qualificadora para o crime de estelionato que não é praticado na modalidade presencial, ou seja, quando a frade é cometida com uso de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de reses sociais ou qualquer outro meio fraudulento análogo.

Fraude eletrônica
§ 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.
§ 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.
Estelionato contra idoso ou vulnerável
§ 4º A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso.
Art. 2º O art. 70 do Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), passa a vigorar acrescido do seguinte § 4º:
§ 4º Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção.? (NR).

Nesse sentido, observa-se que foram elencados os crimes específicos mediante fraude eletrônica objetivando tornar mais rigorosa a lei, ainda tentando acompanhar o avanço da criminalidade. Frisa-se que a Lei 14.155/21 deu ênfase também ao aumento da pena para esse crime na modalidade virtual, com pena de reclusão de 4 a 8 anos e o aumento de 1/3 ao dobro da pena acaso o crime seja praticado contra idoso ou vulnerável, com expectativa para prejudicar a prática delituosa.
15

Cabe destacar também a alteração quanto a competência para apuração do estelionato por fraude mediante cheque ou transferência bancária, o código de

processo penal previa que a competência era do local do banco sacado, o que muitas vezes dificultava a apuração do crime, até pela localização da vítima que nem sempre residia no mesmo local do banco sacado, competência esta alterada para o domicílio da vítima pela Lei 14.155/21.
Por fim, a execução da lei e a responsabilização dos golpistas submete-se a conduta das autoridades capazes, para investigar, processar e julgar os casos de estelionato digital, como a polícia e o poder judiciário.

4 O HISTÓRICO DA PRÁTICA DO ESTELIONATO DIGITAL E OS REFLEXOS DA LEI 14.155 FRENTE A VULNERABILIDADE DA VÍTIMA.

Como já demonstrado, o estelionato digital foi uma modalidade que cresceu esporadicamente com o advento da internet e o constante avanço da tecnologia, mas também teve um de seus marcos recentemente, em 2020, com crescimento exponencial pela pandemia da covid 19 que possibilitou mais ?vítimas? online.
Relativizando em números, o país registrou um aumento ainda mais expressivo que o estelionato comum quando em sua modalidade virtual, com direta relação a pandemia, em 2021 houve 120.470 (cento e cinto mil, quatrocentos e setenta) casos registrados, já em 2022 foram registrados 200.322 (duzentos mil, trezentos e vinte e dois) casos, um aumento de 66,2% (sessenta e seis virgula dois por cento) de acordo com os dados do Fórum Brasileiro de Segurança Pública (FBSP).
Foram registrados em 2021 115 (cento e quinze) estelionatos a cada 100 (cem) mil habitantes no país, já no ano seguinte foram registrados 189,9 (cento e oitenta e nove virgula nove), um aumento de 65,1% (sessenta e cinco vírgula um porcento), ainda de acordo com a FBSP o estado que detém o recorde de casos registrados de estelionato em sua modalidade digital é Santa Catarina, com 64.230 (sessenta e quatro mil, duzentos e trinta) registros em 2022 o que representa 32% (trinta e dois porcento) dos casos do país, ressalvando que Bahia, Ceará, Rio de Janeiro, Rio Grande do Norte, Rio Grande do Sul e São Paulo não tinham ou não disponibilizaram dados.
Cabe destacar que, além de Santa Catarina, tiveram relevantes aumentos Minas Gerais que passou de 25.574 (vinte e cinco mil, quinhentos e setenta e quatro)
16

casos em 2021 para 35.749 (trinta e cinco mil, setecentos e quarenta e nove) em 2022, um aumento de 49,4% (quarenta e nove vírgula quatro porcento), Distrito Federal que passou de 10.049 (dez mil e quarenta e nove) casos em 2021 para 15.580 (quinze mil, quinhentos e oitenta) em 2022, registrando um aumento de 55% (cinquenta e cinco porcento), e o Espírito Santo que passou de 10.545 (dez mil, quinhentos e quarenta e cinco) casos em 2021 para 15.277 (quinze mil, duzentos e setenta e sete) casos em 2022, o que resultou em um aumento de 44,8% (quarenta e quatro vírgula oito por cento).
Dentre todos esses dados disponibilizados pela FBSP cabe destacar por fim os Estados que mais sofreram variações em seus índices, quais sejam Roraima que

passou de 59 (cinquenta e nove) casos em 2021 para absurdos 759 (setecentos e cinquenta e nove) em 2022 acarretando um aumento de 1.186% (mil, cento e oitenta e seis por cento) e Goiás com um aumento de 1.041% (mil e quarenta e um porcento), passando de 128 (cento e vinte e oito) casos em 2021 para 1.461 (mil, quatrocentos e sessenta e um) casos em 2022.
Ainda sobre o marco recente que corroborou com a prática do referido delito é reiterado pelo Fórum Brasileiro de Segurança Pública (FBSP) que:

A digitalização das finanças, de serviço e do comércio, especialmente impulsionada durante o período pandêmico, contribui com a formação de um ambiente propício ao desenvolvimento de modalidades criminais que exploram vulnerabilidade nestes segmentos. (FBSP 2022, p. 6).

Conforme já citado, a modalidade de estelionato digital foi inserida ao Código Penal em meados de 2021 pela Lei nº 14.155/21 que também especificou o estelionato praticado na modalidade digital, por meio cibernético. Essa lei trouxe novidades legislativas que no geral foram positivas com relação a vulnerabilidade da vítima.
Destarte podemos citar que invadir dispositivo informático de uso alheio, ressalvando que conectado ou não a internet, com o fim de obter vantagem ilícita terá pena de reclusão de 4 (quatro) a 8 (oito) anos e multa, com suas devidas especificações, demonstrando assim a preocupação do legislador com as vítimas que infelizmente só estavam crescendo no país e isso refletiu no agravamento da pena que antigamente era disposta no crime de invasão de dispositivo informático, criando uma resistência ao criminoso na medida em que vê o crime como algo mais grave, mediante nova pena mais severa.
17

Ainda quanto aos reflexos dessa lei frente a vulnerabilidade da vítima podem-se listar os agravantes trazidos em sua redação quanto ao furto, com pena de reclusão de 4 a 8 anos, para o crime nessa modalidade realizado com o uso de dispositivos eletrônicos, conectados ou não a internet, por meio de uso de sistemas invasores ou violação de senha, além do agravamento se praticado contra idosos ou vulnerável com consequente aumento de pena de 1/3 ao dobro, ainda na hipótese de ser praticado por servidor fora do território nacional aumenta a pena de 1/3 (um terço) a 2/3 (dois terços).
Quanto ao estelionato também tornou-se agravante o furto qualificado no âmbito cibernético, com igual pena de reclusão de 4 (quatro) a 8 (oito) anos, além de possível multa e pode ter pena aumentada de 1/3 (um terço) a 2/3 (dois terços) acaso seja praticada por servidor fora do território nacional e acaso praticada contra idoso ou vulnerável poderá ter a pena aumentada de 1/3 (um terço) ao dobro.
Por fim, no que tange a invasão de aparelhos para obtenção de dados, a lei passou de detenção de 3 (três) meses a 1 (um) ano para reclusão de 1 (um) a 4 (quatro) anos. Ainda na hipótese de resultar em obtenção de informações sigilosos

pode ser majorada de reclusão de 2 (dois) a 5 (cinco) anos e multa, com agravante de 1/3 (um terço) a 2/3 (dois terços) caso ocorra prejuízo econômico decorrente da invasão.
Assim, as novidades legislativas trazidas pela lei confortam brasileiros que podem ser vítimas de criminosos fora do território nacional, o que é plenamente possível pelo advento da internet e também a população mais velha que, em suma maioria, não tem familiaridade com as ferramentas e linguagens online, não tendo manejo e trato com os meios digitais o que por muitas vezes os torna os principiais focos dos criminosos pela ?facilidade? e ?inocência? desses usuários em específico, assim como os vulneráveis.
Portanto, resta claro que o legislador buscou efetivamente ampliar a guarda dos direitos, de modo a, buscar uma equidade entre diversos grupos de pessoas/possíveis vítimas, resultando em maior segurança, de modo que passa a observar significativas mudanças objetificando proteger os direitos do usuário e penalizando de forma mais grave os criminosos.

5 CONCLUSÃO.

18

O presente artigo, por meio da análise de dados estatísticos, legislação e julgados, buscou tecer uma análise crítica da disciplina normativa do estelionato digital, suas formas de conduta e as possíveis consequências sociais.
Demonstrando que a sociedade está cada vez mais conectada e as redes sociais têm uma função muito importante nessa interação, ocorre que o aumento desenfreado de pessoas conectadas à internet propiciou um ambiente para prática de crimes e com diversas possibilidades de artimanhas dos criminosos, que enxergam a internet como ?terra sem lei?, para obtenção da vantagem ilícita virtualmente, caracterizando o estelionato digital.
Dentre as diversas artimanhas utilizadas pelos estelionatários destacarm-se o ?phishing?, utilizada para enganar os usuários e conseguir informações privadas, ?vishing? popularmente conhecido por ?phishing por voz? quando o ato é realizado por ligações ou envio de áudios com o mesmo intuito de ludibriar a vítima, mas para divulgar dados pessoais e ?smishing? modalidade em que a vítima é provocada a acessar link que corrompe seu aparelho, além de outros golpes como investimentos fraudulentos, promessas de retornos financeiros utopicamente elevados e esquema de pirâmides, esses golpistas beneficiam-se da leiguice de suas vítimas no âmbito de investimento financeiro com falsas promessas de enriquecimento acelerado para enganá-las.
Assim, restou demonstrado que os golpistas tem o mesmo fito, qual seja a obtenção da vantagem ilícita fazendo uso do ambiente cibernético, enquadrando-os no âmbito de estelionatários digitais.
Nesta senda, ainda não existia um enquadramento específico para conter o avanço do referido ilícito que muitas vezes poderia ser caracterizado como tentativa

de extorsão ou crimes análogos o que obrigou o poder legislativo a se atualizar. Para ?frear? o avanço do crime foi introduzida a Lei 12.737/2012, popularmente conhecida por ?Lei Carolina Dieckmann?, que surgiu após um incidente em que a atriz teve seu aparelho pessoal invadido e com isso o vazamento de fotos íntimas na rede.
A introdução da Lei ?Carolina Dieckmann? mostrou-se muito importante por iniciar a caminhada rumo a tipificada do crime de estelionato em sua modalidade digital, ocorre que a tecnologia seguiu se modernizando trazendo novas oportunidades para inovação dos criminosos que vivem as sombras da internet. Com o estabelecimento de modalidades de transferência eletrônica como ?TED? e ?PIX? 19

tornou-se cada vez mais comum o embate entre as autoridades e os golpistas, já demonstrando a necessidade de nova atualização da legislação atinente ao tema.
Quanto a responsabilidade do crime no âmbito jurídico restou pacificado pelas jurisprudências pátrias que torna-se direta em relação ao Autor, sendo aferida pelo Estado que tem o dever de tutelar a convivência no âmbito cibernético. Cumpre destacar que nem sempre a responsabilidade é exclusiva do Autor, podendo recair de forma subjetiva ou objetiva para um terceiro da relação que deveria zelar pela segurança dos dados pessoais do usuário, tais como bancos, tomadores de serviço...
O marco de crescimento registrado no crime de estelionato na sua modalidade virtual foi durante a pandemia de covid 19, época em que foi necessário a reclusão da população em casa o que gerou aumento exponencial de usuários online na rede e, em paralelo, oportunidade para os criminosos inovarem suas artimanhas.
Para combater essa crescente negativa no âmbito jurídico nacional entrou em vigor a lei 14.155/21, de 27 de maio de 2021 trazendo enrijecimento das penas e tipificação de novos crimes, como estelionato contra idoso ou vulnerável e fraude eletrônica, intentando ainda em penas mais rigorosas que podem ser alongadas a depender do caso e alteração de competência para estelionato por fraude mediante cheque ou transferência bancária, submetendo a execução da lei e responsabilização dos golpistas a conduta das autoridades capazes.
O que se conclui é que, com o passar dos anos as leis e medidas tomadas se tornam ultrapassadas vide o ?aperfeiçoamento? dos criminosos, portanto, com o fito do controle do Estado se tornar uma manutenção mais célere se mostrou necessário inserção de um sistema de inovação e renovação legislativa.
Ora, restou comprovado que o âmbito jurídico sempre buscou acompanhar a inovação criminosa trazendo atualizações a legislação para coibir a progressão desses ataques criminosos, mas igualmente restou comprovado que apenas acompanhar não está mais sendo o suficiente, tornando tendência o adiantamento aos movimentos da marginalidade com sucessivo progresso de imersão tecnológica das autoridades para se adiantar ao crime com a devida manutenção das leis de forma mais célere objetivando deter o claro avanço da criminalidade hodierna.

REFERÊNCIAS

20

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez.

BRASIL, DECRETO-LEI NO 2.848, DE 7 DE DEZEMBRO DE 1940. Código Penal. Rio de Janeiro, 7 de dezembro de 1940; 119º da Independência e 52º da República. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 08/06/2023.

BRASIL. LEI Nº 14.155, DE 27 DE MAIO DE 2021. Lei de Invasão a Dispositivo Informático [Internet]. Disponível em: https://www.in.gov.br/en/web/dou/-/lei-n-14.155-de-27-de-maio-de-2021-322698993. Acesso em: 24 nov. 2023

BRASIL. LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012. Lei de Invasão a Dispositivo Informático [Internet]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em:
24 nov. 2023.

BRASIL. LEI Nº 14.155, DE 27 DE MAIO DE 2021. Lei de Invasão a Dispositivo Informático [Internet]. Disponível em: https://www.in.gov.br/en/web/dou/-/lei-nº 14.155-de-27-de-maio-de-2021-322698993. Acesso em: 13 dez. 2023.

BRASIL. Tribunal de Justiça do Paraná. TJ-PR - Recurso Inominado XXXXX-67.2020.8.16.0136 PR. Relator Nestario da Silva Queiroz. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-pr/1511018743. Acesso em: 25 nov. 2023

BRASIL. Tribunal de Justiça do Rio Grande do Sul. TJ-RS - Apelação Cível XXXXX-22.2020.8.21.7000 RS. Relator Giovanni Conti. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-rs/932015329. Acesso em: 25 nov. 2023

BRITO, Auriney. Direito penal informático. São Paulo: Saraiva, 2013, p.189.

CAMPOS, Pedro Franco de [et al.]. Direito penal aplicado: parte geral e parte especial do Código Penal. - 6ª. Ed. ? São Paulo: Saraiva, 2016.

CASSANTI, Moisés de Oliveira. Crimes virtuais, vítimas reais. 1ª ed. Rio de Janeiro: Brasport, 2014, p.6.

CHAVES, Fábio Barbosa; TEIXEIRA, Filipe Silva. Os crimes de fraude e estelionato cibernético e a proteção do consumidor no e-commerce. 2020. Disponível em: <https://conteudojuridico.com.br>. Acesso em: 12/06/2023.

COELHO, Yuri Carneiro. Curso de Direito Penal Didático. vol. único, 2ª ed. ? São Paulo: Atlas, 2015.

CÔRREA, Gustavo Testa. Aspectos jurídicos da internet. 5. ed. rev. e atual. São Paulo, Saraiva, 2010.

CUNHA, Rogério Sanches. Manual de direito penal: parte especial (arts. 121 ao 361). 11. ed. rev., ampl. e atual. Salvador: JusPODIVM, 2019.
21

CUNHA, Rogério Sanches. Lei 14.155/21 e os crimes de fraude digital - primeiras impressões e reflexos no CP e no CPP. Meu Site Jurídico (JusPodivm), 2021. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2021/05/28/lei-14-15521-e-os-crimes-de-fraude-digital-primeiras-impressoes-e-reflexos-no-cp-e-no-cpp/. Acesso em: 13 dez. 2023.

FBSP. Fórum Brasileiro de Segurança Pública. Os crimes patrimoniais no Brasil: entre novas e velhas dinâmicas. Anuário Brasileiro de Segurança Pública, 2022. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2022/07/07-anuario-2022-os-crimes-patrimoniais-no-brasil-entre-novas-e-velhas-dinamicas.pdf. Acesso em 24 nov. 2023.

GENNARINI, Juliana. Revista de Direito Penal e Processo Penal, ISSN 2674-6093, v. 2, n. 2, jul./dez. 2020.

GONÇALVES, Victor Eduardo Rios. Direito penal esquematizado: parte especial do Código Penal. - 8. ed. ? São Paulo: Saraiva Educação, 2018.
GRECO, Rogério. Curso de Direito Penal: parte especial. v. III. 7. ed. Rio de Janeiro: Ed. Impetus, 2010.

GOUSSINSKY, Eugenio. Crimes digitais têm forte alta em vários estados; saiba como prevenir. Portal R7, 2021. Disponível em: https://noticias.r7.com/tecnologia-e-ciencia/crimes-digitais-tem-forte-alta-em-varios-estados-saiba-como-prevenir-05052021. Acesso em: 12 dez. 2023.

GRECO, Rogério. Curso de Direito Penal: parte especial. v. III. 7. ed. Rio de Janeiro: Ed. Impetus, 2010, p. 228.

HUNGRIA, Nelson. Comentários ao Código Penal ? Vol. IX. Rio de Janeiro: Forense, 1958.

MIRABETE, Júlio Fabbrini e FABBRINI, Renato N./ Manual de direito penal: parte especial: arts. 121 a 234-B do CP ? volume 2, 36° edição, São Paulo, Atlas, 2021.

==========

Arquivo 1: Trabalho de ConclusÃ£o de Curso - Rafael Garcia.pdf (6280 termos)
Arquivo 2: https://www.redpoints.com/blog/prevent-digital-fraud (2153 termos)
Termos comuns: 3
Similaridade: 0,03%
O texto abaixo é o conteúdo do documento Trabalho de ConclusÃ£o de Curso - Rafael Garcia.pdf (6280 termos)
Os termos em vermelho foram encontrados no documento https://www.redpoints.com/blog/prevent-digital-fraud (2153 termos)

==========

ESTELIONATO DIGITAL: UMA ANÁLISE CRÍTICA DA DISCIPLINA NORMATIVA, SUAS FORMAS DE CONDUTA E AS POSSÍVEIS CONSEQUÊNCIAS SOCIAIS

Rafael Lemos Garcia de Oliveira1
Ricardo Simões Xavier dos Santos2

Resumo
O presente artigo discorre sobre a figura do estelionato digital, fazendo uma análise crítica da disciplina normativa, suas formas de conduta e as possíveis consequências sociais. É notório que a atual legislação do país tem avançado, conforme mencionado, na forma que tipifica os crimes que ocorrem em meios virtuais, todavia as sanções ainda são moderadas e as normas devem avançar no sentido de impedir a prática dos crimes virtuais. Para que seja viável a hipótese narrada, o Estado tem o dever de incrementar métodos novos de apuração e averiguação e aprimorar os recursos tecnológicos e digitais que estão à disposição das autoridades responsáveis. Nesse sentido, é necessário compreender o que é o estelionato digital, suas características, maneiras de prevenção e formas em que pode aparecer no dia a dia dos usuários da rede, compactuando com a legislação penal e o cabimento de penalização para os criminosos que praticam esse crime. Por fim, conclui-se que a legislação penal brasileira vem evoluindo, mas para que alcance um nível suficiente de eficácia no combate a esse crime é necessário compreender o que é o estelionato digital, suas características, maneiras de prevenção e formas em que pode aparecer no dia a dia dos usuários da rede, compactuando com a legislação penal e o cabimento de penalização para os criminosos que praticam esse crime.

PALAVRAS-CHAVE: Internet. Crime Cibernético. Estelionato Digital. Código Penal.

1 Graduando em bacharelado em direito pela UCSAL. E-mail: rafaell.oliveira@ucsal.edu.br
2 Doutor em Políticas Sociais e Cidadania pela Universidade Católica do Salvador ? UCSal. E-mail:

ricardo.santos@pro.ucsal.br
2

ABSTRACT: This article discusses the figure of digital fraud, making a critical analysis of the normative discipline, its forms of conduct and the possible social consequences. It is notable that the country's current legislation has advanced, as mentioned, in the way it typifies crimes that occur in virtual media, however sanctions are still moderate and standards must advance in order to prevent the practice of virtual crimes. In order for the narrated hypothesis to be viable, the State has the duty to increase new methods of investigation and investigation and improve the technological and digital resources that are available to the responsible authorities. In this sense, it is necessary to understand what digital fraud is, its characteristics, methods of prevention and ways in which it can appear in the daily lives of network users, in agreement with criminal legislation and the appropriateness of penalizing criminals who practice this crime. Finally, it is concluded that Brazilian criminal legislation has been evolving, but in order to achieve a sufficient level of effectiveness in combating this crime, it is necessary to understand what digital fraud is, its characteristics, methods of prevention and forms in which it can appear. in the daily lives of network users, complying with criminal legislation and the appropriateness of penalizing criminals who commit this crime.

KEYWORDS: Internet. Cybercrime. Digital Fraud. Penal Code.

SUMÁRIO: 1 INTRODUÇÃO. 2 CONDUTA DO ESTELIONATO DIGITAL: CONCEITOS PRÉVIOS, DISCUSSÕES INICIAIS E FORMAS APRESENTADAS. 2.1 Análise acerca das eventuais consequências sociais advindas da conduta do estelionato digital 3 A RESPONSABILIZAÇÃO DO CRIME DE ESTELIONATO DIGITAL NO ÂMBITO JURÍDICO 3.1 Concepção das normas jurídicas atualizadas e formas de punição do crime do estelionato digital 4 O HISTÓRICO DA PRÁTICA DO ESTELIONATO DIGITAL E OS REFLEXOS DA LEI 14.155 FRENTE A VULNERABILIDADE DA VÍTIMA 5 CONCLUSÃO 6 REFERÊNCIAS

1 INTRODUÇÃO

No âmbito penalista são diversos os crimes que têm como objetivo a obtenção de lucros financeiros da vítima, o referido trabalho tem como objetivo abordar o estelionato digital fazendo uma análise crítica da disciplina normativa, apresentando suas formas de conduta e relacionando a suas possíveis consequências sociais.
3

Há uma previsão legal do Código Penal em garantir que todos os cidadãos lesados por práticas de golpes, em que são utilizados artifícios ou qualquer meio fraudulento, podem ingressar no juízo criminal a fim de prosseguirem com a punição penal e com o ressarcimento dos prejuízos.
Para breve introito, o estelionato é 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.
Dentre os crimes mais comuns no Brasil e no mundo pode-se destacar o estelionato, além do meio físico os criminosos procuram pela navegação na rede com o fito de obtenção de dados e informações das pessoas que tem perfil para serem suas possíveis vítimas, pondo em prática das mais diversas maneiras tais como ligações, mensagens, falsificação de identidade, haja vista que todos os dias, a população vive a internet, cadastrando senhas, trocando mensagens, adentrando redes sociais, fazendo negócios pela internet...
Nesse sentido, acompanhando o aumento dos usuários das redes a realização de crimes online cresceu consideravelmente, obviamente relacionado a simplicidade de manejo dos meios virtuais e pela dificuldade de identificação dos criminosos para posterior punição, haja vista ausência de legislações específicas e supressão das identidades.
A realização de golpes e fraudes cometendo ilícitos para obter vantagem sob outras pessoas é prática recorrente e por muitas vezes impune no Brasil, com o estelionato digital não é diferente.
Em sua esfera digital ele se configura quando o criminoso submete o aparelho da vítima e sincroniza-o a demais sistemas de informação ou, em outra hipótese, quando a vítima é posta em uma conjuntura de sensibilidade para obtenção de vantagem ilícita. Na atualidade é mais comum do que se imagina conhecer alguém que tenha passado por essa situação e caído nesse golpe, desde ligações de números sem chamador ou desconhecidos a e-mails/mensagens com ofertas incríveis.
Outro ponto importante que contribuiu para esse aumento, além da facilidade no manejo dos meios virtuais foi o advento da pandemia do Covid-19, as práticas desses crimes se multiplicaram, haja vista que, relevante porcentagem da população tanto brasileira quanto mundial, se viu obrigada a passar mais tempo em casa, o que, em consequência, ampliou o número de pessoas online, acessando a rede. Neste liame, os criminosos têm agido cada vez mais e feito várias vítimas no mundo virtual.
4

Para que o crime possa ser classificado como estelionato digital é imprescindível que a entrega das informações pela vítima seja de forma voluntária, haja vista que a obtenção dos dados se deu por outros meios, o crime pode ter outra classificação, tal como ?furto mediante fraude eletrônica?.
Dentre as principais vítimas desse crime tão comum na atualidade estão as pessoas desatentas e que não tomam total atenção para se esquivar dos estelionatários, seguindo as hipóteses de compra e venda pela internet não verificando a fonte, se é de confiança etc., links enviados de números aleatórios possibilitando o acesso do criminoso a rede da vítima entre outros...
A despeito da clara regulação e evolução da internet e redes sociais, os conselhos e observações para a premeditação dos crimes digitais em geral continua sendo de cuidado e cautela com os dados pessoais e sua divulgação, ainda com o remetente e usuários/links que adentra. É necessário que sempre pense que tudo que

identifique quem você é ou que busque saber informações que só você teria acesso são o alerta inicial para entender se não se está diante de uma possível tentativa de estelionato digital.
É notório que a atual legislação do país tem avançado, conforme mencionado, na forma que tipifica os crimes que ocorrem em meios virtuais, todavia as sanções ainda são moderadas e as normas devem avançar no sentido de impedir a prática dos crimes virtuais. Para que seja viável a hipótese narrada, o Estado tem o dever de incrementar métodos novos de apuração e averiguação e aprimorar os recursos tecnológicos e digitais que estão à disposição das autoridades responsáveis.
Nesse sentido, é necessário compreender o que é o estelionato digital, suas características, maneiras de prevenção e formas em que pode aparecer no dia a dia dos usuários da rede, compactuando com a legislação penal e o cabimento de penalização para os criminosos que praticam esse crime.
Assim, as perguntas que ficam são quais as formas de conduta do estelionato digital e seus impactos na sociedade, além do questionamento acerca das normas brasileiras, nosso sistema jurídico atual contempla qual espécie de responsabilização para o crime de estelionato digital, alinhado a isso, como o Estado Democrático Brasileiro pode melhorar para combater o aumento desse crime.
No presente artigo, seguindo após a introdução para o capítulo ?2? onde serão apresentadas as condutas do estelionato digital, seus conceitos prévios e formas apresentadas, a diferença entre o estelionato e outros crimes contra o patrimônio e
5

sua forma de proliferação pela rede mediante sites falsos, mensagens e e-mails. O capítulo ?2? contém ainda um subtópico ?2.1? onde serão analisadas as consequências sociais advindas da conduta do estelionato digital, desde a inovação dos criminosos partindo para o meio digital até os ?traumas? das vítimas e sua repercussão na sociedade.
Já no capítulo ?3? será amplamente explicada a quem deve ser dirigida a responsabilidade pelo crime do estelionato digital, no âmbito jurídico, já que o crime na grande maioria das vezes tem por conclusão a ?fuga? do criminoso pelo meio cibernético. Ainda no capítulo ?3? serão exploradas, mediante subtópico ?3.1?, as normas jurídicas atualizadas e formas de punição do crime tendo relação direta com a ampla possibilidade de escape do criminoso.
Por fim, em capítulo ?4?, será demonstrado o histórico da prática do estelionato digital, sua evolução paralela ao avanço da tecnologia na sociedade e os reflexos da Lei 14.155, instituída em 2021 especialmente para tornar mais grave a pena de estelionato cometido de forma eletrônica pela internet, frente ainda a vulnerabilidade da vítima. Seguidos da conclusão e as referências bibliográficas.
De certo, cumpre-se destacar que a pesquisa em questão, valeu-se do método da revisão bibliográfica de trabalhos científicos atualizados das áreas penal e constitucional, frente às questões sociais, publicadas em periódicos nacionais e internacionais, qualificados como publicações de A1, assim como B1. Além de importantes nomes do cenário retrato, ao passo que se cita Rogério Greco e Fabio

Barbosa Chavez, bem como análise jurisprudencial e legislativa da lei 14.155.
Compreende-se então, que a escolha metodológica se justifica de base teórica, fundada em estudos atualizados sobre o estelionato digital, suas formas de conduta e as consequências sociais.
O foco da pesquisa bibliográfica foi de apresentar informações e dados específicos sobre a evolução dos crimes digitais, exibindo o progresso do direito penal frente os crimes digitais, através da análise filosófica e de referenciais teóricos de artigos, códigos e outros trabalhos sobre a mesma questão jurídica. Assim, o método empregado é de leitura e análise de material doutrinário especializado já existente sobre o tema de Direito Penal, tal como de jurisprudência, dados, legislação e artigos científicos.

6

2 CONDUTA DO ESTELIONATO DIGITAL: CONCEITOS PRÉVIOS, DISCUSSÕES INICIAIS E FORMAS APRESENTADAS.

O termo estelionato está disposta no Art. 171 do Código Penal como:

Art. 171. Obter, para si ou para outrem, vantagem ilícita em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: pena ? Reclusão, de 1 (um) a 5 (cinco) anos, de multa.

Trata-se de crime contra o patrimônio onde a legislação penal visa proteger a inviolabilidade patrimonial orientada pela prática de atos que visam enganar a vítima e beneficiar o agente (CUNHA, 2019, p. 345).
Assim, pode-se inferir que a diferença entre o estelionato e os diversos crimes contra o patrimônio, ou seja, crimes que tenham por objetivo atentar contra o patrimônio de uma pessoa ou organização, é que no estelionato não é utilizada a força para obtenção de ?vantagem?. É sabido, portanto, que essa atitude é conhecida há muitos anos, de modo que Greco cita que:

Desde que surgiram as relações sociais, o homem se vale da fraude para dissimular seus verdadeiros sentimentos e intenções para, de alguma forma, ocultar ou falsear a verdade, a fim de obter vantagens que, em tese, lhe seriam indevidas (GRECO, 2019, p. 228).

Ressalta-se que o crime existe apenas na modalidade dolosa, sem previsão na forma culposa.
A respeito da expressão ?vantagem ilícita?, Fernando Capez (2020) ensina que, esta, trata-se do objeto material do crime e, caso o agente esteja agindo em razão de uma vantagem devida, a conduta é tipificada como exercício arbitrário das próprias razões, delito previsto no art. 345, do Código Penal.
De acordo com o que se retira do artigo 171, do supramencionado dispositivo

legal, o estelionato pode ser cometido mediante artificio, ardil ou qualquer outro meio fraudulento. Em relação ao termo ?artificio?, o doutrinador Júlio Fabbrini Mirabete ensina o seguinte:

?o artifício existe quando o agente se utilizar de um aparato que modifica, ao menos aparentemente, o aspecto material da coisa, figurando entre esses meios o documento falso ou outra falsificação qualquer, o disfarce, a modificação por aparelhos mecânicos ou elétricos, filmes, efeitos de luz etc.? (MIRABETE, 2021, pag. 325).

Em sua modalidade digital o estelionato ocorre através de sites falsos, mensagens e até e-mail, sendo prioritariamente focado no âmbito virtual. É bastante
7

normal que o consumidor busque virtualmente os mesmos bens desejados fisicamente, mas com a comodidade de não se deslocar e em grande maioria dos casos a acessibilidade com preços menores, levando a promessa da oferta muitas vezes a encantar o consumidor que não percebe a fraude.
Dentre as formas de conduta do referido crime podem ser listadas as mais comuns sendo: vendas falsas em sua maioria quando os estelionatários oferecem serviços ou produtos inexistentes em redes sociais e/ou sites e links de comércio eletrônico; ?phishing?, uma artimanha utilizada pelos criminosos para enganar os usuários e conseguir informações privadas, tais como senhas, detalhes de cartões de crédito, comumente realizado por meio do envio de mensagens eletrônicas se passando por instituições de confiança, pode ser realizado por sites e por redes sociais também, mas sempre com o intuito de prejudicar e obter vantagem, ?vishing? popularmente conhecido por ?phishing por voz? quando o ato é realizado por ligações ou envio de áudios com o mesmo intuito de ludibriar a vítima, mas para divulgar dados pessoais, ?smishing? realizada também por mensagem, mas nessa modalidade a vítima é provocada a acessar link que corrompe seu aparelho, e por último os golpes de investimentos fraudulentos que podem acontecer de diversas maneiras, tais como promessas de retornos financeiros utopicamente elevados e esquema de pirâmides, esses golpistas beneficiam-se da leiguice de suas vítimas no âmbito de investimento financeiro com falsas promessas de enriquecimento acelerado para enganá-las.
No Art. 171 do Código Penal, o estelionato possui a pena de reclusão de 1 a 5 anos e multa. Diante disso, o crime admite suspensão condicional no processo de acordo com o art. 89, § 1ª, da Lei dos Juizados Especiais - Lei n. 9099/95:

Art. 89. Nos crimes em que a pena mínima cominada for igual ou inferior a um ano, abrangidas ou não por esta Lei, o Ministério Público, ao oferecer a denúncia, poderá propor a suspensão do processo, por dois a quatro anos, desde que o acusado não esteja sendo processado ou não tenha sido condenado por outro crime, presentes os demais requisitos que autorizariam a suspensão condicional da pena (art. 77 do Código Penal).

Conforme dito, o crime de estelionato digital, no sistema jurídico atual do Brasil, é apreciado no âmbito do Direito Penal o qual pressupõe responsabilização penal para esse tipo de ato, o qual era equiparado ao crime de estelionato, previsto no artigo 171 do Código Penal, ocorre que ainda no caminhar para a especificação do crime de estelionato na modalidade digital foi introduzida a Lei 12.737/2012, ou como é popularmente conhecida a ?Lei Carolina Dieckmann?, que surgiu após um incidente 8

em que a atriz teve seu aparelho pessoal invadido e com isso o vazamento de fotos íntimas na rede, mediante ainda tentativa de extorsão.
Na época em questão os criminosos seriam apenas denunciados pelo crime de tentativa de extorsão, haja vista ausência de legislação específica quanto aos crimes digitais, assim vários projetos de lei foram analisados para tentar tipificar condutas para crimes semelhantes ao sofrido pela atriz e findada essa fase foi sancionada a Lei 12.737/2012 que entrou em vigor em 02 de abril de 2013.
A lei visava combater o vazamento de informações pessoais dos usuários das redes, zelando pela proteção da privacidade dos mesmos, ainda acrescentou ao Código Penal, mais especificamente no Decreto-Lei 2848, os artigos 154-A e 154-B.

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

A lei se demonstrou efetiva a época da sanção sendo citada como um marco legislativo por muitos autores, desde que entrou em vigor a invasão de computadores, celulares, tablets...no geral dispositivos informáticos alheios passou a ser crime.
Cabe destacar que execução da lei e a responsabilização dos golpistas submete-se a conduta das autoridades capazes, para investigar, processar e julgar os casos de estelionato digital, como a polícia e o Poder Judiciário.

2.1 ANÁLISE ACERCA DAS EVENTUAIS CONSEQUÊNCIAS SOCIAIS ADVINDAS DA CONDUTA DO ESTELIONATO DIGITAL.

A sociedade está cada vez mais conectada e as redes sociais têm uma função muito importante nessa interação, vez que o ser humano sempre precisou de convívio

social. Assim, tais ferramentas estão presentes na vida de muitos brasileiros e esse ambiente digital, como já evidenciado, tornou-se, também, um meio para a prática de crimes, seja pela facilidade de acesso e/ou pelo grande número de usuários.
9

Na atualidade existe uma grande facilidade na obtenção de produtos, sendo de maneira virtual, de modo que não existe mais a necessidade do consumidor se deslocar até o fornecedor para adquirir o produto, nesta feita, é notório que a compra virtual vem amadurecendo cada vez mais, o que consequentemente ocasiona um aumento dos crimes cibernéticos. Nesse contexto, Chaves e Teixeira destacam que:

Com a investigação correta é possível localizar e punir os criminosos que causaram prejuízo a essa nova espécie de consumidores. Todavia, no mesmo ritmo que a internet evolui, os fraudadores também se renovam com novas modalidades de golpes, alguns tão específicos que são até difíceis de definir qual a punição correta a ser aplicada (CHAVES e TEIXEIRA, 2019, p. 119).

Conforme já citado a inovação dos criminosos acompanha em paralelo o avanço da tecnologia pela sociedade, de modo que muitos usuários têm a sensação de que a internet é ?terra sem lei? fomentando sua ?liberdade tecnológica? em pequenos delitos, tais como injúria, difamação... Ao passo em que não imaginam ter a sua responsabilidade realmente comprovada, agindo por trás da tela do celular ou computador.
Perpassando por isso os criminosos buscam a obtenção de vantagem ilícita e veem na internet uma oportunidade recheada de opções, possuídos pela sensação de impunidade e munidos das mais diversas artimanhas para concluir seu objetivo. Cumpre ressaltar que sociedade caminha para um futuro mais tecnológico e os criminosos ?surfam nessa onda?.
A cada dia que passa resta mais rudimentar os métodos de pagamento por cédulas ou moedas, a trajetória da população tem destino eletrônico, de modo que é fato notório o quão comum se tornaram os sistemas de pagamento eletrônico, estando já alguns mais rudimentares como a transferência ?TED?.
A popularização dos sistemas de pagamento eletrônico, a exemplo do ?pix?, propicia diariamente um combate necessário entre as autoridades e os golpistas. Já é rotina na sociedade a divulgação de novos meios de golpes cibernéticos com o fito de alertar os usuários a se precaverem mais, infelizmente nem sempre todo cuidado é tomado e as consequências podem ser desastrosas para os consumidores da rede.
O prejuízo causado a essa nova espécie de consumidores afeta tanto de forma direta as vítimas quanto a sociedade, de maneira geral. Dentre as consequências sociais advindas dessa conduta resta mister destacar o impacto financeiro nas vítimas, de forma direta, que podem encarar perdas financeiras o que acarreta
10

problemas emocionais e instabilidade, perda de confiança no meio digital para compras que também gera impacto na maneira como as pessoas conduzem negócios online.
Além do consumidor direto, as instituições financeiras também sofrem em muitos casos ressarcindo o valor perdido por seus clientes lesados, arcando com o custo de fraude e também no investimento em segurança virtual, mesmo ainda tendo um receio a implantação dos pagamentos digitais buscando ao máximo reforçar sua segurança desde confirmação por ?face id? quanto senhas regularmente trocadas e ?tokens digitais?, sempre tentando confirmar que é realmente o usuário da conta quem realmente está fazendo a operação e não um terceiro. Frisa-se que essas consequências sociais acarretam, num todo, impacto na economia.
Felizmente, não são somente os consumidores que passam pelo processo de consequências negativas, mas também os fraudadores. Mesmo diante da crescente a qual ocorre o ?fenômeno? do estelionato digital, os criminosos não restam imunes a responsabilização pelo seu crime. Conforme será demonstrado no presente artigo, a legislação do país delimita o crime e suas consequências, assim como as penalidades que podem levar os fraudadores a condenação pelas atividades ilícitas.
Nesse sentido, o avanço da tecnologia com o passar dos tempos corroborou indiretamente para que os criminosos inovassem seus meios ilícitos para obtenção de vantagens, causando diversos impactos na sociedade que não teriam como ser positivos, sendo alguns dos principais o prejuízo financeiro as vítimas; perda de confiança na segurança online e transações digitais, além do choque nos sistemas judiciais, de segurança e nas bases digitais o que consequentemente requer mecanismos e investimentos relevantes de atribuição das empresas e do judiciário.
Sendo assim, infere-se que ainda existe certa dificuldade para identificação dos golpistas o que, alternativamente, tem relação com a legislação brasileira que tem avançado na tipificação dos crimes cibernéticos, todavia as sanções ainda são moderadas e as normas devem acompanhar no sentido de bridar a prática desses crimes na modalidade virtual.

3 A RESPONSABILIZAÇÃO DO CRIME DE ESTELIONATO DIGITAL NO ÂMBITO JURÍDICO.

11

É claro que a internet e toda a esfera digital não foi inserida na sociedade com o intuito ou sequer resguarda em relação a possibilidade do advento de crimes em paralelo a isso, mas como toda imprevisão, a criminalidade evoluiu em conjunto deixando cada vez mais vulnerável a segurança dos usuários na rede, como amplamente demonstrado no presente trabalho, os golpes digitais se aperfeiçoam com o passar dos anos, com ênfase para o estelionato que conta hoje com diversos tipos de obtenção de vantagem ilícita na sua modalidade digital.
A internet tornou-se essencial na rotina da população, interligando usuários e pessoas conectadas a rede, assim, como bem destacou Uchoa de Brito:

(...) O problema da internet passou a ser identificado quando a tecnologia incrementou e complicou as relações sociais consideradas, até então, pacíficas e controladas, possibilitando algumas experiências socialmente desagradáveis e indesejadas, como a sua utilização para a prática de crimes, e a criação de novos contatos que colocam em risco bens que ainda não tiveram sua relevância reconhecida pelo Direito. (BRITO, 2013, p. 9).

Assim, a prática do estelionato na modalidade virtual cresceu ao longo dos anos, sempre com a tentativa em paralelo do Direito Penal de acompanhar para poder punir em cerceamento legislativo, com projetos de lei, inovações e acréscimos a legislações já vigentes.
Quanto a responsabilização do crime em questão torna-se direta em relação ao Autor, sendo aferida pelo Estado, mesmo em sua modalidade digital, haja vista que tem o encargo de combater, controlar e reprimir tais práticas tanto no mundo ?real? quanto no ambiente digital, além de ser responsável por tutelar a convivência e atuação neste âmbito cibernético.
Além da responsabilização direta quanto ao autor do delito, muitas vezes a responsabilidade também recai de forma subjetiva ou objetiva para um terceiro da relação que deveria zelar pela segurança dos dados pessoais do usuário, grandes exemplos são os de vazamento de dados bancários online após invasão por hackers, recaindo responsabilidade também para os bancos que deveriam proteger o consumidor.

APELAÇÃO CÍVEL. NEGÓCIOS JURÍDICOS BANCÁRIOS. AÇÃO DE INDENIZAÇÃO POR DANOS MATERIAIS. RESSARCIMENTO DE VALORES. TRANSAÇÃO BANCÁRIA REALIZADA DE FORMA FRAUDULENTA POR TERCEIROS. INTERNET BANKING. RESPONSABILIDADE DO BANCO. SUMULA 479 DO STJ. SENTENÇA MANTIDA. As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias. Súmula 479 do STJ. Art. 14 do CDC. Para
12

responsabilização do prestador de serviços a existência de culpa ou dolo, exige-se apenas a conduta ilícita e a existência de dano, bem como nexo de causalidade entre eles. Caso. Autora que foi vítima de estelionato praticado por terceiro. Empréstimo autorizado pela instituição financeira. Nesse ponto, desimporta que a fraude tenha se perpetrado através dos canais de atendimento via internet (internet banking), porquanto a parte autora negou ter sido a autora dos saques, e o banco não se desincumbiu do ônus de demonstrar a regularidade das transações impugnadas pelo cliente. NEGARAM PROVIMENTO AO APELO. UNÂNIME.

Entre outros exemplos de golpes como os já citados ?phishing?, ?vishing? e ?smishing? que buscam a obtenção de vantagem ilícita frente as vítimas, muitas vezes fazendo uso de um terceiro como ponte para alçar seu objetivo fraudulento, ocorre que, como mencionado, mesmo esse terceiro não tendo o dolo na prática do crime deve garantir a segurança e impermeabilidade do seu sistema para que isso não ocorra, contando com a obrigação de assegurar os direitos do consumidor e usuário. Este é o entendimento das jurisprudências pátrias:
RECURSO INOMINADO. AÇÃO DECLARATÓRIA DE INEXISTÊNCIA DE DÉBITO C/C INDENIZAÇÃO POR DANOS MORAIS. PRELIMINAR DE VIOLAÇÃO AO PRINCÍPIO DA DIALETICDADE. INOCORRÊNCIA. BANCÁRIO. TRANSFERÊNCIA DE VALORES REALIZADA POR TERCEIRO. FRAUDE EVIDENCIADA. CULPA DA VÍTIMA NÃO CONFIGURADA. INSTITUIÇÃO FINANCEIRA QUE NÃO APRESENTOU PROVAS ACERCA DA SEGURANÇA, AUTENTICAÇÃO OU IDENTIFICAÇÃO DA OPERAÇÃO. FALHA NA PRESTAÇÃO DO SERVIÇO CONFIGURADA. RESPONSABILIDADE OBJETIVA DO BANCO. APLICAÇÃO DA SÚMULA 479 DO STJ. RESTITUIÇÃO DEVIDA. AUSÊNCIA DE SOLUÇÃO ADMINISTRATIVA. DANO MORAL CONFIGURADO NO CASO CONCRETO. QUANTUM ARBITRADO EM R$ 2.000,00 (DOIS MIL REAIS) QUE COMPORTA MAJORAÇÃO PARA R$ 3.000,00 (TRÊS MIL REAIS). OBSERVÂNCIA AOS PRINCÍPIOS DA PROPORCIONALIDADE E RAZOABILIDADE. SENTENÇA PARCIALMENTE REFORMADA. Recurso da autora conhecido e provido.Recurso do réu conhecido e desprovido. (TJPR - 1ª Turma Recursal - 0003317-67.2020.8.16.0136 - Pitanga - Rel.: JUIZ DE DIREITO DA TURMA RECURSAL DOS JUIZADOS ESPECIAIS NESTARIO DA SILVA QUEIROZ - J. 23.05.2022)
(TJ-PR - RI: 00033176720208160136 Pitanga 0003317-67.2020.8.16.0136 (Acórdão), Relator: Nestario da Silva Queiroz, Data de Julgamento: 23/05/2022, 1ª Turma Recursal, Data de Publicação: 23/05/2022)

Ressalta-se que o estelionato na sua modalidade digital é considerado crime de ação penal pública incondicionada, ou seja, a responsabilidade para conduzir o procedimento é do Ministério Público, independente de manifestação de vontade da vítima, a natureza dessa ação ressalva a relevância de tratar esse delito de forma mais eficaz, independente da vontade da vítima de ver o autor do crime responsabilizado, com o fito de preservar a ordem social e diminuir o índice de novos casos.
13

Nesse sentido, cumpre destacar que mesmo a responsabilidade do crime ser direta em relação ao Autor, também pode abranger mais partes do processo dependendo da especificada do caso. A jurisprudência entende que a responsabilidade não é apenas do Estado, mas também da empresa, entidade ou qualquer terceiro que tenha a obrigação de tornar o ambiente digital seguro para o

usuário.

3.1 CONCEPÇÃO DAS NORMAS JURÍDICAS ATUALIZADAS E FORMAS DE PUNIÇÃO DO CRIME DO ESTELIONATO DIGITAL.

Como já explicitado, um grande fator que desencadeou o aumento da efetivação do crime em questão foi a pandemia, de modo que, com o advento do Covid-19, foi necessário que a população se protegesse em suas casas para corroborar com o distanciamento social e assim evitar a proliferação do vírus, ocorre que em contrapartida a isso foi destaque a aproximação online dos usuários que culminou em oportunidade para os criminosos inovarem suas artimanhas, contando com a suposta sensação de anonimato.
O crime de estelionato digital, no sistema jurídico atual do Brasil, é apreciado no âmbito do Direito Penal, o qual pressupõe responsabilização para esse tipo de ato, que era equiparado ao crime de estelionato, previsto no artigo 171 do Código Penal.
A Lei 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann, entrou em vigor como uma tentativa inicial de tipificar a conduta dos crimes na modalidade virtual para proteção dos dados pessoais da população em face aos criminosos virtuais, ocorre que com o passar dos anos se mostrou necessária a inclusão de novas medidas frente a progressão da criminalidade no país, em específico os crimes virtuais.
Para combater essa crescente negativa no âmbito jurídico nacional entrou em vigor a lei 14.155/21, de 27 de maio de 2021, que incluiu e modificou alguns parágrafos no supramencionado dispositivo legal, alterando algumas regras para julgar o crime.

Art. 1º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar com as seguintes alterações:
?Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
14

§ 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.
§ 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso:
I ? 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;
II ? Aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável. Pena ? reclusão, de 1 (um) a 4 (quatro) anos, e multa.

§ 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. Pena ? reclusão, de 2 (dois) a 5 (cinco) anos, e multa.

Dentre as alterações, foram incluídos os § § 2º-A e 2º-B, que tratam de fraude eletrônica, sendo o § 2º-A qualificadora para o crime de estelionato que não é praticado na modalidade presencial, ou seja, quando a frade é cometida com uso de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de reses sociais ou qualquer outro meio fraudulento análogo.

Fraude eletrônica
§ 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.
§ 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.
Estelionato contra idoso ou vulnerável
§ 4º A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso.
Art. 2º O art. 70 do Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), passa a vigorar acrescido do seguinte § 4º:
§ 4º Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção.? (NR).

Nesse sentido, observa-se que foram elencados os crimes específicos mediante fraude eletrônica objetivando tornar mais rigorosa a lei, ainda tentando acompanhar o avanço da criminalidade. Frisa-se que a Lei 14.155/21 deu ênfase também ao aumento da pena para esse crime na modalidade virtual, com pena de reclusão de 4 a 8 anos e o aumento de 1/3 ao dobro da pena acaso o crime seja praticado contra idoso ou vulnerável, com expectativa para prejudicar a prática delituosa.
15

Cabe destacar também a alteração quanto a competência para apuração do estelionato por fraude mediante cheque ou transferência bancária, o código de

processo penal previa que a competência era do local do banco sacado, o que muitas vezes dificultava a apuração do crime, até pela localização da vítima que nem sempre residia no mesmo local do banco sacado, competência esta alterada para o domicílio da vítima pela Lei 14.155/21.
Por fim, a execução da lei e a responsabilização dos golpistas submete-se a conduta das autoridades capazes, para investigar, processar e julgar os casos de estelionato digital, como a polícia e o poder judiciário.

4 O HISTÓRICO DA PRÁTICA DO ESTELIONATO DIGITAL E OS REFLEXOS DA LEI 14.155 FRENTE A VULNERABILIDADE DA VÍTIMA.

Como já demonstrado, o estelionato digital foi uma modalidade que cresceu esporadicamente com o advento da internet e o constante avanço da tecnologia, mas também teve um de seus marcos recentemente, em 2020, com crescimento exponencial pela pandemia da covid 19 que possibilitou mais ?vítimas? online.
Relativizando em números, o país registrou um aumento ainda mais expressivo que o estelionato comum quando em sua modalidade virtual, com direta relação a pandemia, em 2021 houve 120.470 (cento e cinto mil, quatrocentos e setenta) casos registrados, já em 2022 foram registrados 200.322 (duzentos mil, trezentos e vinte e dois) casos, um aumento de 66,2% (sessenta e seis virgula dois por cento) de acordo com os dados do Fórum Brasileiro de Segurança Pública (FBSP).
Foram registrados em 2021 115 (cento e quinze) estelionatos a cada 100 (cem) mil habitantes no país, já no ano seguinte foram registrados 189,9 (cento e oitenta e nove virgula nove), um aumento de 65,1% (sessenta e cinco vírgula um porcento), ainda de acordo com a FBSP o estado que detém o recorde de casos registrados de estelionato em sua modalidade digital é Santa Catarina, com 64.230 (sessenta e quatro mil, duzentos e trinta) registros em 2022 o que representa 32% (trinta e dois porcento) dos casos do país, ressalvando que Bahia, Ceará, Rio de Janeiro, Rio Grande do Norte, Rio Grande do Sul e São Paulo não tinham ou não disponibilizaram dados.
Cabe destacar que, além de Santa Catarina, tiveram relevantes aumentos Minas Gerais que passou de 25.574 (vinte e cinco mil, quinhentos e setenta e quatro)
16

casos em 2021 para 35.749 (trinta e cinco mil, setecentos e quarenta e nove) em 2022, um aumento de 49,4% (quarenta e nove vírgula quatro porcento), Distrito Federal que passou de 10.049 (dez mil e quarenta e nove) casos em 2021 para 15.580 (quinze mil, quinhentos e oitenta) em 2022, registrando um aumento de 55% (cinquenta e cinco porcento), e o Espírito Santo que passou de 10.545 (dez mil, quinhentos e quarenta e cinco) casos em 2021 para 15.277 (quinze mil, duzentos e setenta e sete) casos em 2022, o que resultou em um aumento de 44,8% (quarenta e quatro vírgula oito por cento).
Dentre todos esses dados disponibilizados pela FBSP cabe destacar por fim os Estados que mais sofreram variações em seus índices, quais sejam Roraima que

passou de 59 (cinquenta e nove) casos em 2021 para absurdos 759 (setecentos e cinquenta e nove) em 2022 acarretando um aumento de 1.186% (mil, cento e oitenta e seis por cento) e Goiás com um aumento de 1.041% (mil e quarenta e um porcento), passando de 128 (cento e vinte e oito) casos em 2021 para 1.461 (mil, quatrocentos e sessenta e um) casos em 2022.
Ainda sobre o marco recente que corroborou com a prática do referido delito é reiterado pelo Fórum Brasileiro de Segurança Pública (FBSP) que:

A digitalização das finanças, de serviço e do comércio, especialmente impulsionada durante o período pandêmico, contribui com a formação de um ambiente propício ao desenvolvimento de modalidades criminais que exploram vulnerabilidade nestes segmentos. (FBSP 2022, p. 6).

Conforme já citado, a modalidade de estelionato digital foi inserida ao Código Penal em meados de 2021 pela Lei nº 14.155/21 que também especificou o estelionato praticado na modalidade digital, por meio cibernético. Essa lei trouxe novidades legislativas que no geral foram positivas com relação a vulnerabilidade da vítima.
Destarte podemos citar que invadir dispositivo informático de uso alheio, ressalvando que conectado ou não a internet, com o fim de obter vantagem ilícita terá pena de reclusão de 4 (quatro) a 8 (oito) anos e multa, com suas devidas especificações, demonstrando assim a preocupação do legislador com as vítimas que infelizmente só estavam crescendo no país e isso refletiu no agravamento da pena que antigamente era disposta no crime de invasão de dispositivo informático, criando uma resistência ao criminoso na medida em que vê o crime como algo mais grave, mediante nova pena mais severa.
17

Ainda quanto aos reflexos dessa lei frente a vulnerabilidade da vítima podem-se listar os agravantes trazidos em sua redação quanto ao furto, com pena de reclusão de 4 a 8 anos, para o crime nessa modalidade realizado com o uso de dispositivos eletrônicos, conectados ou não a internet, por meio de uso de sistemas invasores ou violação de senha, além do agravamento se praticado contra idosos ou vulnerável com consequente aumento de pena de 1/3 ao dobro, ainda na hipótese de ser praticado por servidor fora do território nacional aumenta a pena de 1/3 (um terço) a 2/3 (dois terços).
Quanto ao estelionato também tornou-se agravante o furto qualificado no âmbito cibernético, com igual pena de reclusão de 4 (quatro) a 8 (oito) anos, além de possível multa e pode ter pena aumentada de 1/3 (um terço) a 2/3 (dois terços) acaso seja praticada por servidor fora do território nacional e acaso praticada contra idoso ou vulnerável poderá ter a pena aumentada de 1/3 (um terço) ao dobro.
Por fim, no que tange a invasão de aparelhos para obtenção de dados, a lei passou de detenção de 3 (três) meses a 1 (um) ano para reclusão de 1 (um) a 4 (quatro) anos. Ainda na hipótese de resultar em obtenção de informações sigilosos

pode ser majorada de reclusão de 2 (dois) a 5 (cinco) anos e multa, com agravante de 1/3 (um terço) a 2/3 (dois terços) caso ocorra prejuízo econômico decorrente da invasão.
Assim, as novidades legislativas trazidas pela lei confortam brasileiros que podem ser vítimas de criminosos fora do território nacional, o que é plenamente possível pelo advento da internet e também a população mais velha que, em suma maioria, não tem familiaridade com as ferramentas e linguagens online, não tendo manejo e trato com os meios digitais o que por muitas vezes os torna os principiais focos dos criminosos pela ?facilidade? e ?inocência? desses usuários em específico, assim como os vulneráveis.
Portanto, resta claro que o legislador buscou efetivamente ampliar a guarda dos direitos, de modo a, buscar uma equidade entre diversos grupos de pessoas/possíveis vítimas, resultando em maior segurança, de modo que passa a observar significativas mudanças objetificando proteger os direitos do usuário e penalizando de forma mais grave os criminosos.

5 CONCLUSÃO.

18

O presente artigo, por meio da análise de dados estatísticos, legislação e julgados, buscou tecer uma análise crítica da disciplina normativa do estelionato digital, suas formas de conduta e as possíveis consequências sociais.
Demonstrando que a sociedade está cada vez mais conectada e as redes sociais têm uma função muito importante nessa interação, ocorre que o aumento desenfreado de pessoas conectadas à internet propiciou um ambiente para prática de crimes e com diversas possibilidades de artimanhas dos criminosos, que enxergam a internet como ?terra sem lei?, para obtenção da vantagem ilícita virtualmente, caracterizando o estelionato digital.
Dentre as diversas artimanhas utilizadas pelos estelionatários destacarm-se o ?phishing?, utilizada para enganar os usuários e conseguir informações privadas, ?vishing? popularmente conhecido por ?phishing por voz? quando o ato é realizado por ligações ou envio de áudios com o mesmo intuito de ludibriar a vítima, mas para divulgar dados pessoais e ?smishing? modalidade em que a vítima é provocada a acessar link que corrompe seu aparelho, além de outros golpes como investimentos fraudulentos, promessas de retornos financeiros utopicamente elevados e esquema de pirâmides, esses golpistas beneficiam-se da leiguice de suas vítimas no âmbito de investimento financeiro com falsas promessas de enriquecimento acelerado para enganá-las.
Assim, restou demonstrado que os golpistas tem o mesmo fito, qual seja a obtenção da vantagem ilícita fazendo uso do ambiente cibernético, enquadrando-os no âmbito de estelionatários digitais.
Nesta senda, ainda não existia um enquadramento específico para conter o avanço do referido ilícito que muitas vezes poderia ser caracterizado como tentativa

de extorsão ou crimes análogos o que obrigou o poder legislativo a se atualizar. Para ?frear? o avanço do crime foi introduzida a Lei 12.737/2012, popularmente conhecida por ?Lei Carolina Dieckmann?, que surgiu após um incidente em que a atriz teve seu aparelho pessoal invadido e com isso o vazamento de fotos íntimas na rede.
A introdução da Lei ?Carolina Dieckmann? mostrou-se muito importante por iniciar a caminhada rumo a tipificada do crime de estelionato em sua modalidade digital, ocorre que a tecnologia seguiu se modernizando trazendo novas oportunidades para inovação dos criminosos que vivem as sombras da internet. Com o estabelecimento de modalidades de transferência eletrônica como ?TED? e ?PIX? 19

tornou-se cada vez mais comum o embate entre as autoridades e os golpistas, já demonstrando a necessidade de nova atualização da legislação atinente ao tema.
Quanto a responsabilidade do crime no âmbito jurídico restou pacificado pelas jurisprudências pátrias que torna-se direta em relação ao Autor, sendo aferida pelo Estado que tem o dever de tutelar a convivência no âmbito cibernético. Cumpre destacar que nem sempre a responsabilidade é exclusiva do Autor, podendo recair de forma subjetiva ou objetiva para um terceiro da relação que deveria zelar pela segurança dos dados pessoais do usuário, tais como bancos, tomadores de serviço...
O marco de crescimento registrado no crime de estelionato na sua modalidade virtual foi durante a pandemia de covid 19, época em que foi necessário a reclusão da população em casa o que gerou aumento exponencial de usuários online na rede e, em paralelo, oportunidade para os criminosos inovarem suas artimanhas.
Para combater essa crescente negativa no âmbito jurídico nacional entrou em vigor a lei 14.155/21, de 27 de maio de 2021 trazendo enrijecimento das penas e tipificação de novos crimes, como estelionato contra idoso ou vulnerável e fraude eletrônica, intentando ainda em penas mais rigorosas que podem ser alongadas a depender do caso e alteração de competência para estelionato por fraude mediante cheque ou transferência bancária, submetendo a execução da lei e responsabilização dos golpistas a conduta das autoridades capazes.
O que se conclui é que, com o passar dos anos as leis e medidas tomadas se tornam ultrapassadas vide o ?aperfeiçoamento? dos criminosos, portanto, com o fito do controle do Estado se tornar uma manutenção mais célere se mostrou necessário inserção de um sistema de inovação e renovação legislativa.
Ora, restou comprovado que o âmbito jurídico sempre buscou acompanhar a inovação criminosa trazendo atualizações a legislação para coibir a progressão desses ataques criminosos, mas igualmente restou comprovado que apenas acompanhar não está mais sendo o suficiente, tornando tendência o adiantamento aos movimentos da marginalidade com sucessivo progresso de imersão tecnológica das autoridades para se adiantar ao crime com a devida manutenção das leis de forma mais célere objetivando deter o claro avanço da criminalidade hodierna.

REFERÊNCIAS

20

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez.

BRASIL, DECRETO-LEI NO 2.848, DE 7 DE DEZEMBRO DE 1940. Código Penal. Rio de Janeiro, 7 de dezembro de 1940; 119º da Independência e 52º da República. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 08/06/2023.

BRASIL. LEI Nº 14.155, DE 27 DE MAIO DE 2021. Lei de Invasão a Dispositivo Informático [Internet]. Disponível em: https://www.in.gov.br/en/web/dou/-/lei-n-14.155-de-27-de-maio-de-2021-322698993. Acesso em: 24 nov. 2023

BRASIL. LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012. Lei de Invasão a Dispositivo Informático [Internet]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em:
24 nov. 2023.

BRASIL. LEI Nº 14.155, DE 27 DE MAIO DE 2021. Lei de Invasão a Dispositivo Informático [Internet]. Disponível em: https://www.in.gov.br/en/web/dou/-/lei-nº 14.155-de-27-de-maio-de-2021-322698993. Acesso em: 13 dez. 2023.

BRASIL. Tribunal de Justiça do Paraná. TJ-PR - Recurso Inominado XXXXX-67.2020.8.16.0136 PR. Relator Nestario da Silva Queiroz. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-pr/1511018743. Acesso em: 25 nov. 2023

BRASIL. Tribunal de Justiça do Rio Grande do Sul. TJ-RS - Apelação Cível XXXXX-22.2020.8.21.7000 RS. Relator Giovanni Conti. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-rs/932015329. Acesso em: 25 nov. 2023

BRITO, Auriney. Direito penal informático. São Paulo: Saraiva, 2013, p.189.

CAMPOS, Pedro Franco de [et al.]. Direito penal aplicado: parte geral e parte especial do Código Penal. - 6ª. Ed. ? São Paulo: Saraiva, 2016.

CASSANTI, Moisés de Oliveira. Crimes virtuais, vítimas reais. 1ª ed. Rio de Janeiro: Brasport, 2014, p.6.

CHAVES, Fábio Barbosa; TEIXEIRA, Filipe Silva. Os crimes de fraude e estelionato cibernético e a proteção do consumidor no e-commerce. 2020. Disponível em: <https://conteudojuridico.com.br>. Acesso em: 12/06/2023.

COELHO, Yuri Carneiro. Curso de Direito Penal Didático. vol. único, 2ª ed. ? São Paulo: Atlas, 2015.

CÔRREA, Gustavo Testa. Aspectos jurídicos da internet. 5. ed. rev. e atual. São Paulo, Saraiva, 2010.

CUNHA, Rogério Sanches. Manual de direito penal: parte especial (arts. 121 ao 361). 11. ed. rev., ampl. e atual. Salvador: JusPODIVM, 2019.
21

CUNHA, Rogério Sanches. Lei 14.155/21 e os crimes de fraude digital - primeiras impressões e reflexos no CP e no CPP. Meu Site Jurídico (JusPodivm), 2021. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2021/05/28/lei-14-15521-e-os-crimes-de-fraude-digital-primeiras-impressoes-e-reflexos-no-cp-e-no-cpp/. Acesso em: 13 dez. 2023.

FBSP. Fórum Brasileiro de Segurança Pública. Os crimes patrimoniais no Brasil: entre novas e velhas dinâmicas. Anuário Brasileiro de Segurança Pública, 2022. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2022/07/07-anuario-2022-os-crimes-patrimoniais-no-brasil-entre-novas-e-velhas-dinamicas.pdf. Acesso em 24 nov. 2023.

GENNARINI, Juliana. Revista de Direito Penal e Processo Penal, ISSN 2674-6093, v. 2, n. 2, jul./dez. 2020.

GONÇALVES, Victor Eduardo Rios. Direito penal esquematizado: parte especial do Código Penal. - 8. ed. ? São Paulo: Saraiva Educação, 2018.
GRECO, Rogério. Curso de Direito Penal: parte especial. v. III. 7. ed. Rio de Janeiro: Ed. Impetus, 2010.

GOUSSINSKY, Eugenio. Crimes digitais têm forte alta em vários estados; saiba como prevenir. Portal R7, 2021. Disponível em: https://noticias.r7.com/tecnologia-e-ciencia/crimes-digitais-tem-forte-alta-em-varios-estados-saiba-como-prevenir-05052021. Acesso em: 12 dez. 2023.

GRECO, Rogério. Curso de Direito Penal: parte especial. v. III. 7. ed. Rio de Janeiro: Ed. Impetus, 2010, p. 228.

HUNGRIA, Nelson. Comentários ao Código Penal ? Vol. IX. Rio de Janeiro: Forense, 1958.

MIRABETE, Júlio Fabbrini e FABBRINI, Renato N./ Manual de direito penal: parte especial: arts. 121 a 234-B do CP ? volume 2, 36° edição, São Paulo, Atlas, 2021.

ESTELIONATO DIGITAL: UMA ANÁLISE CRÍTICA DA DISCIPLINA NORMATIVA, SUAS FORMAS DE CONDUTA E AS POSSÍVEIS CONSEQUÊNCIAS SOCIAIS

Rafael Lemos Garcia de Oliveira1
Ricardo Simões Xavier dos Santos2

Resumo
O presente artigo discorre sobre a figura do estelionato digital, fazendo uma análise crítica da disciplina normativa, suas formas de conduta e as possíveis consequências sociais. É notório que a atual legislação do país tem avançado, conforme mencionado, na forma que tipifica os crimes que ocorrem em meios virtuais, todavia as sanções ainda são moderadas e as normas devem avançar no sentido de impedir a prática dos crimes virtuais. Para que seja viável a hipótese narrada, o Estado tem o dever de incrementar métodos novos de apuração e averiguação e aprimorar os recursos tecnológicos e digitais que estão à disposição das autoridades responsáveis. Nesse sentido, é necessário compreender o que é o estelionato digital, suas características, maneiras de prevenção e formas em que pode aparecer no dia a dia dos usuários da rede, compactuando com a legislação penal e o cabimento de penalização para os criminosos que praticam esse crime. Por fim, conclui-se que a legislação penal brasileira vem evoluindo, mas para que alcance um nível suficiente de eficácia no combate a esse crime é necessário compreender o que é o estelionato digital, suas características, maneiras de prevenção e formas em que pode aparecer no dia a dia dos usuários da rede, compactuando com a legislação penal e o cabimento de penalização para os criminosos que praticam esse crime.

PALAVRAS-CHAVE: Internet. Crime Cibernético. Estelionato Digital. Código Penal.

1 Graduando em bacharelado em direito pela UCSAL. E-mail: rafaell.oliveira@ucsal.edu.br
2 Doutor em Políticas Sociais e Cidadania pela Universidade Católica do Salvador ? UCSal. E-mail:

ricardo.santos@pro.ucsal.br
2

ABSTRACT: This article discusses the figure of digital fraud, making a critical analysis of the normative discipline, its forms of conduct and the possible social consequences. It is notable that the country's current legislation has advanced, as mentioned, in the way it typifies crimes that occur in virtual media, however sanctions are still moderate and standards must advance in order to prevent the practice of virtual crimes. In order for the narrated hypothesis to be viable, the State has the duty to increase new methods of investigation and investigation and improve the technological and digital resources that are available to the responsible authorities. In this sense, it is necessary to understand what digital fraud is, its characteristics, methods of prevention and ways in which it can appear in the daily lives of network users, in agreement with criminal legislation and the appropriateness of penalizing criminals who practice this crime. Finally, it is concluded that Brazilian criminal legislation has been evolving, but in order to achieve a sufficient level of effectiveness in combating this crime, it is necessary to understand what digital fraud is, its characteristics, methods of prevention and forms in which it can appear. in the daily lives of network users, complying with criminal legislation and the appropriateness of penalizing criminals who commit this crime.

KEYWORDS: Internet. Cybercrime. Digital Fraud. Penal Code.

SUMÁRIO: 1 INTRODUÇÃO. 2 CONDUTA DO ESTELIONATO DIGITAL: CONCEITOS PRÉVIOS, DISCUSSÕES INICIAIS E FORMAS APRESENTADAS. 2.1 Análise acerca das eventuais consequências sociais advindas da conduta do estelionato digital 3 A RESPONSABILIZAÇÃO DO CRIME DE ESTELIONATO DIGITAL NO ÂMBITO JURÍDICO 3.1 Concepção das normas jurídicas atualizadas e formas de punição do crime do estelionato digital 4 O HISTÓRICO DA PRÁTICA DO ESTELIONATO DIGITAL E OS REFLEXOS DA LEI 14.155 FRENTE A VULNERABILIDADE DA VÍTIMA 5 CONCLUSÃO 6 REFERÊNCIAS

1 INTRODUÇÃO

No âmbito penalista são diversos os crimes que têm como objetivo a obtenção de lucros financeiros da vítima, o referido trabalho tem como objetivo abordar o estelionato digital fazendo uma análise crítica da disciplina normativa, apresentando suas formas de conduta e relacionando a suas possíveis consequências sociais.
3

Há uma previsão legal do Código Penal em garantir que todos os cidadãos lesados por práticas de golpes, em que são utilizados artifícios ou qualquer meio fraudulento, podem ingressar no juízo criminal a fim de prosseguirem com a punição penal e com o ressarcimento dos prejuízos.
Para breve introito, o estelionato é 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.
Dentre os crimes mais comuns no Brasil e no mundo pode-se destacar o estelionato, além do meio físico os criminosos procuram pela navegação na rede com o fito de obtenção de dados e informações das pessoas que tem perfil para serem suas possíveis vítimas, pondo em prática das mais diversas maneiras tais como ligações, mensagens, falsificação de identidade, haja vista que todos os dias, a população vive a internet, cadastrando senhas, trocando mensagens, adentrando redes sociais, fazendo negócios pela internet...
Nesse sentido, acompanhando o aumento dos usuários das redes a realização de crimes online cresceu consideravelmente, obviamente relacionado a simplicidade de manejo dos meios virtuais e pela dificuldade de identificação dos criminosos para posterior punição, haja vista ausência de legislações específicas e supressão das identidades.
A realização de golpes e fraudes cometendo ilícitos para obter vantagem sob outras pessoas é prática recorrente e por muitas vezes impune no Brasil, com o estelionato digital não é diferente.
Em sua esfera digital ele se configura quando o criminoso submete o aparelho da vítima e sincroniza-o a demais sistemas de informação ou, em outra hipótese, quando a vítima é posta em uma conjuntura de sensibilidade para obtenção de vantagem ilícita. Na atualidade é mais comum do que se imagina conhecer alguém que tenha passado por essa situação e caído nesse golpe, desde ligações de números sem chamador ou desconhecidos a e-mails/mensagens com ofertas incríveis.
Outro ponto importante que contribuiu para esse aumento, além da facilidade no manejo dos meios virtuais foi o advento da pandemia do Covid-19, as práticas desses crimes se multiplicaram, haja vista que, relevante porcentagem da população tanto brasileira quanto mundial, se viu obrigada a passar mais tempo em casa, o que, em consequência, ampliou o número de pessoas online, acessando a rede. Neste liame, os criminosos têm agido cada vez mais e feito várias vítimas no mundo virtual.
4

Para que o crime possa ser classificado como estelionato digital é imprescindível que a entrega das informações pela vítima seja de forma voluntária, haja vista que a obtenção dos dados se deu por outros meios, o crime pode ter outra classificação, tal como ?furto mediante fraude eletrônica?.
Dentre as principais vítimas desse crime tão comum na atualidade estão as pessoas desatentas e que não tomam total atenção para se esquivar dos estelionatários, seguindo as hipóteses de compra e venda pela internet não verificando a fonte, se é de confiança etc., links enviados de números aleatórios possibilitando o acesso do criminoso a rede da vítima entre outros...
A despeito da clara regulação e evolução da internet e redes sociais, os conselhos e observações para a premeditação dos crimes digitais em geral continua sendo de cuidado e cautela com os dados pessoais e sua divulgação, ainda com o remetente e usuários/links que adentra. É necessário que sempre pense que tudo que

identifique quem você é ou que busque saber informações que só você teria acesso são o alerta inicial para entender se não se está diante de uma possível tentativa de estelionato digital.
É notório que a atual legislação do país tem avançado, conforme mencionado, na forma que tipifica os crimes que ocorrem em meios virtuais, todavia as sanções ainda são moderadas e as normas devem avançar no sentido de impedir a prática dos crimes virtuais. Para que seja viável a hipótese narrada, o Estado tem o dever de incrementar métodos novos de apuração e averiguação e aprimorar os recursos tecnológicos e digitais que estão à disposição das autoridades responsáveis.
Nesse sentido, é necessário compreender o que é o estelionato digital, suas características, maneiras de prevenção e formas em que pode aparecer no dia a dia dos usuários da rede, compactuando com a legislação penal e o cabimento de penalização para os criminosos que praticam esse crime.
Assim, as perguntas que ficam são quais as formas de conduta do estelionato digital e seus impactos na sociedade, além do questionamento acerca das normas brasileiras, nosso sistema jurídico atual contempla qual espécie de responsabilização para o crime de estelionato digital, alinhado a isso, como o Estado Democrático Brasileiro pode melhorar para combater o aumento desse crime.
No presente artigo, seguindo após a introdução para o capítulo ?2? onde serão apresentadas as condutas do estelionato digital, seus conceitos prévios e formas apresentadas, a diferença entre o estelionato e outros crimes contra o patrimônio e
5

sua forma de proliferação pela rede mediante sites falsos, mensagens e e-mails. O capítulo ?2? contém ainda um subtópico ?2.1? onde serão analisadas as consequências sociais advindas da conduta do estelionato digital, desde a inovação dos criminosos partindo para o meio digital até os ?traumas? das vítimas e sua repercussão na sociedade.
Já no capítulo ?3? será amplamente explicada a quem deve ser dirigida a responsabilidade pelo crime do estelionato digital, no âmbito jurídico, já que o crime na grande maioria das vezes tem por conclusão a ?fuga? do criminoso pelo meio cibernético. Ainda no capítulo ?3? serão exploradas, mediante subtópico ?3.1?, as normas jurídicas atualizadas e formas de punição do crime tendo relação direta com a ampla possibilidade de escape do criminoso.
Por fim, em capítulo ?4?, será demonstrado o histórico da prática do estelionato digital, sua evolução paralela ao avanço da tecnologia na sociedade e os reflexos da Lei 14.155, instituída em 2021 especialmente para tornar mais grave a pena de estelionato cometido de forma eletrônica pela internet, frente ainda a vulnerabilidade da vítima. Seguidos da conclusão e as referências bibliográficas.
De certo, cumpre-se destacar que a pesquisa em questão, valeu-se do método da revisão bibliográfica de trabalhos científicos atualizados das áreas penal e constitucional, frente às questões sociais, publicadas em periódicos nacionais e internacionais, qualificados como publicações de A1, assim como B1. Além de importantes nomes do cenário retrato, ao passo que se cita Rogério Greco e Fabio

Barbosa Chavez, bem como análise jurisprudencial e legislativa da lei 14.155.
Compreende-se então, que a escolha metodológica se justifica de base teórica, fundada em estudos atualizados sobre o estelionato digital, suas formas de conduta e as consequências sociais.
O foco da pesquisa bibliográfica foi de apresentar informações e dados específicos sobre a evolução dos crimes digitais, exibindo o progresso do direito penal frente os crimes digitais, através da análise filosófica e de referenciais teóricos de artigos, códigos e outros trabalhos sobre a mesma questão jurídica. Assim, o método empregado é de leitura e análise de material doutrinário especializado já existente sobre o tema de Direito Penal, tal como de jurisprudência, dados, legislação e artigos científicos.

6

2 CONDUTA DO ESTELIONATO DIGITAL: CONCEITOS PRÉVIOS, DISCUSSÕES INICIAIS E FORMAS APRESENTADAS.

O termo estelionato está disposta no Art. 171 do Código Penal como:

Art. 171. Obter, para si ou para outrem, vantagem ilícita em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: pena ? Reclusão, de 1 (um) a 5 (cinco) anos, de multa.

Trata-se de crime contra o patrimônio onde a legislação penal visa proteger a inviolabilidade patrimonial orientada pela prática de atos que visam enganar a vítima e beneficiar o agente (CUNHA, 2019, p. 345).
Assim, pode-se inferir que a diferença entre o estelionato e os diversos crimes contra o patrimônio, ou seja, crimes que tenham por objetivo atentar contra o patrimônio de uma pessoa ou organização, é que no estelionato não é utilizada a força para obtenção de ?vantagem?. É sabido, portanto, que essa atitude é conhecida há muitos anos, de modo que Greco cita que:

Desde que surgiram as relações sociais, o homem se vale da fraude para dissimular seus verdadeiros sentimentos e intenções para, de alguma forma, ocultar ou falsear a verdade, a fim de obter vantagens que, em tese, lhe seriam indevidas (GRECO, 2019, p. 228).

Ressalta-se que o crime existe apenas na modalidade dolosa, sem previsão na forma culposa.
A respeito da expressão ?vantagem ilícita?, Fernando Capez (2020) ensina que, esta, trata-se do objeto material do crime e, caso o agente esteja agindo em razão de uma vantagem devida, a conduta é tipificada como exercício arbitrário das próprias razões, delito previsto no art. 345, do Código Penal.
De acordo com o que se retira do artigo 171, do supramencionado dispositivo

legal, o estelionato pode ser cometido mediante artificio, ardil ou qualquer outro meio fraudulento. Em relação ao termo ?artificio?, o doutrinador Júlio Fabbrini Mirabete ensina o seguinte:

?o artifício existe quando o agente se utilizar de um aparato que modifica, ao menos aparentemente, o aspecto material da coisa, figurando entre esses meios o documento falso ou outra falsificação qualquer, o disfarce, a modificação por aparelhos mecânicos ou elétricos, filmes, efeitos de luz etc.? (MIRABETE, 2021, pag. 325).

Em sua modalidade digital o estelionato ocorre através de sites falsos, mensagens e até e-mail, sendo prioritariamente focado no âmbito virtual. É bastante
7

normal que o consumidor busque virtualmente os mesmos bens desejados fisicamente, mas com a comodidade de não se deslocar e em grande maioria dos casos a acessibilidade com preços menores, levando a promessa da oferta muitas vezes a encantar o consumidor que não percebe a fraude.
Dentre as formas de conduta do referido crime podem ser listadas as mais comuns sendo: vendas falsas em sua maioria quando os estelionatários oferecem serviços ou produtos inexistentes em redes sociais e/ou sites e links de comércio eletrônico; ?phishing?, uma artimanha utilizada pelos criminosos para enganar os usuários e conseguir informações privadas, tais como senhas, detalhes de cartões de crédito, comumente realizado por meio do envio de mensagens eletrônicas se passando por instituições de confiança, pode ser realizado por sites e por redes sociais também, mas sempre com o intuito de prejudicar e obter vantagem, ?vishing? popularmente conhecido por ?phishing por voz? quando o ato é realizado por ligações ou envio de áudios com o mesmo intuito de ludibriar a vítima, mas para divulgar dados pessoais, ?smishing? realizada também por mensagem, mas nessa modalidade a vítima é provocada a acessar link que corrompe seu aparelho, e por último os golpes de investimentos fraudulentos que podem acontecer de diversas maneiras, tais como promessas de retornos financeiros utopicamente elevados e esquema de pirâmides, esses golpistas beneficiam-se da leiguice de suas vítimas no âmbito de investimento financeiro com falsas promessas de enriquecimento acelerado para enganá-las.
No Art. 171 do Código Penal, o estelionato possui a pena de reclusão de 1 a 5 anos e multa. Diante disso, o crime admite suspensão condicional no processo de acordo com o art. 89, § 1ª, da Lei dos Juizados Especiais - Lei n. 9099/95:

Art. 89. Nos crimes em que a pena mínima cominada for igual ou inferior a um ano, abrangidas ou não por esta Lei, o Ministério Público, ao oferecer a denúncia, poderá propor a suspensão do processo, por dois a quatro anos, desde que o acusado não esteja sendo processado ou não tenha sido condenado por outro crime, presentes os demais requisitos que autorizariam a suspensão condicional da pena (art. 77 do Código Penal).

Conforme dito, o crime de estelionato digital, no sistema jurídico atual do Brasil, é apreciado no âmbito do Direito Penal o qual pressupõe responsabilização penal para esse tipo de ato, o qual era equiparado ao crime de estelionato, previsto no artigo 171 do Código Penal, ocorre que ainda no caminhar para a especificação do crime de estelionato na modalidade digital foi introduzida a Lei 12.737/2012, ou como é popularmente conhecida a ?Lei Carolina Dieckmann?, que surgiu após um incidente 8

em que a atriz teve seu aparelho pessoal invadido e com isso o vazamento de fotos íntimas na rede, mediante ainda tentativa de extorsão.
Na época em questão os criminosos seriam apenas denunciados pelo crime de tentativa de extorsão, haja vista ausência de legislação específica quanto aos crimes digitais, assim vários projetos de lei foram analisados para tentar tipificar condutas para crimes semelhantes ao sofrido pela atriz e findada essa fase foi sancionada a Lei 12.737/2012 que entrou em vigor em 02 de abril de 2013.
A lei visava combater o vazamento de informações pessoais dos usuários das redes, zelando pela proteção da privacidade dos mesmos, ainda acrescentou ao Código Penal, mais especificamente no Decreto-Lei 2848, os artigos 154-A e 154-B.

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

A lei se demonstrou efetiva a época da sanção sendo citada como um marco legislativo por muitos autores, desde que entrou em vigor a invasão de computadores, celulares, tablets...no geral dispositivos informáticos alheios passou a ser crime.
Cabe destacar que execução da lei e a responsabilização dos golpistas submete-se a conduta das autoridades capazes, para investigar, processar e julgar os casos de estelionato digital, como a polícia e o Poder Judiciário.

2.1 ANÁLISE ACERCA DAS EVENTUAIS CONSEQUÊNCIAS SOCIAIS ADVINDAS DA CONDUTA DO ESTELIONATO DIGITAL.

A sociedade está cada vez mais conectada e as redes sociais têm uma função muito importante nessa interação, vez que o ser humano sempre precisou de convívio

social. Assim, tais ferramentas estão presentes na vida de muitos brasileiros e esse ambiente digital, como já evidenciado, tornou-se, também, um meio para a prática de crimes, seja pela facilidade de acesso e/ou pelo grande número de usuários.
9

Na atualidade existe uma grande facilidade na obtenção de produtos, sendo de maneira virtual, de modo que não existe mais a necessidade do consumidor se deslocar até o fornecedor para adquirir o produto, nesta feita, é notório que a compra virtual vem amadurecendo cada vez mais, o que consequentemente ocasiona um aumento dos crimes cibernéticos. Nesse contexto, Chaves e Teixeira destacam que:

Com a investigação correta é possível localizar e punir os criminosos que causaram prejuízo a essa nova espécie de consumidores. Todavia, no mesmo ritmo que a internet evolui, os fraudadores também se renovam com novas modalidades de golpes, alguns tão específicos que são até difíceis de definir qual a punição correta a ser aplicada (CHAVES e TEIXEIRA, 2019, p. 119).

Conforme já citado a inovação dos criminosos acompanha em paralelo o avanço da tecnologia pela sociedade, de modo que muitos usuários têm a sensação de que a internet é ?terra sem lei? fomentando sua ?liberdade tecnológica? em pequenos delitos, tais como injúria, difamação... Ao passo em que não imaginam ter a sua responsabilidade realmente comprovada, agindo por trás da tela do celular ou computador.
Perpassando por isso os criminosos buscam a obtenção de vantagem ilícita e veem na internet uma oportunidade recheada de opções, possuídos pela sensação de impunidade e munidos das mais diversas artimanhas para concluir seu objetivo. Cumpre ressaltar que sociedade caminha para um futuro mais tecnológico e os criminosos ?surfam nessa onda?.
A cada dia que passa resta mais rudimentar os métodos de pagamento por cédulas ou moedas, a trajetória da população tem destino eletrônico, de modo que é fato notório o quão comum se tornaram os sistemas de pagamento eletrônico, estando já alguns mais rudimentares como a transferência ?TED?.
A popularização dos sistemas de pagamento eletrônico, a exemplo do ?pix?, propicia diariamente um combate necessário entre as autoridades e os golpistas. Já é rotina na sociedade a divulgação de novos meios de golpes cibernéticos com o fito de alertar os usuários a se precaverem mais, infelizmente nem sempre todo cuidado é tomado e as consequências podem ser desastrosas para os consumidores da rede.
O prejuízo causado a essa nova espécie de consumidores afeta tanto de forma direta as vítimas quanto a sociedade, de maneira geral. Dentre as consequências sociais advindas dessa conduta resta mister destacar o impacto financeiro nas vítimas, de forma direta, que podem encarar perdas financeiras o que acarreta
10

problemas emocionais e instabilidade, perda de confiança no meio digital para compras que também gera impacto na maneira como as pessoas conduzem negócios online.
Além do consumidor direto, as instituições financeiras também sofrem em muitos casos ressarcindo o valor perdido por seus clientes lesados, arcando com o custo de fraude e também no investimento em segurança virtual, mesmo ainda tendo um receio a implantação dos pagamentos digitais buscando ao máximo reforçar sua segurança desde confirmação por ?face id? quanto senhas regularmente trocadas e ?tokens digitais?, sempre tentando confirmar que é realmente o usuário da conta quem realmente está fazendo a operação e não um terceiro. Frisa-se que essas consequências sociais acarretam, num todo, impacto na economia.
Felizmente, não são somente os consumidores que passam pelo processo de consequências negativas, mas também os fraudadores. Mesmo diante da crescente a qual ocorre o ?fenômeno? do estelionato digital, os criminosos não restam imunes a responsabilização pelo seu crime. Conforme será demonstrado no presente artigo, a legislação do país delimita o crime e suas consequências, assim como as penalidades que podem levar os fraudadores a condenação pelas atividades ilícitas.
Nesse sentido, o avanço da tecnologia com o passar dos tempos corroborou indiretamente para que os criminosos inovassem seus meios ilícitos para obtenção de vantagens, causando diversos impactos na sociedade que não teriam como ser positivos, sendo alguns dos principais o prejuízo financeiro as vítimas; perda de confiança na segurança online e transações digitais, além do choque nos sistemas judiciais, de segurança e nas bases digitais o que consequentemente requer mecanismos e investimentos relevantes de atribuição das empresas e do judiciário.
Sendo assim, infere-se que ainda existe certa dificuldade para identificação dos golpistas o que, alternativamente, tem relação com a legislação brasileira que tem avançado na tipificação dos crimes cibernéticos, todavia as sanções ainda são moderadas e as normas devem acompanhar no sentido de bridar a prática desses crimes na modalidade virtual.

3 A RESPONSABILIZAÇÃO DO CRIME DE ESTELIONATO DIGITAL NO ÂMBITO JURÍDICO.

11

É claro que a internet e toda a esfera digital não foi inserida na sociedade com o intuito ou sequer resguarda em relação a possibilidade do advento de crimes em paralelo a isso, mas como toda imprevisão, a criminalidade evoluiu em conjunto deixando cada vez mais vulnerável a segurança dos usuários na rede, como amplamente demonstrado no presente trabalho, os golpes digitais se aperfeiçoam com o passar dos anos, com ênfase para o estelionato que conta hoje com diversos tipos de obtenção de vantagem ilícita na sua modalidade digital.
A internet tornou-se essencial na rotina da população, interligando usuários e pessoas conectadas a rede, assim, como bem destacou Uchoa de Brito:

(...) O problema da internet passou a ser identificado quando a tecnologia incrementou e complicou as relações sociais consideradas, até então, pacíficas e controladas, possibilitando algumas experiências socialmente desagradáveis e indesejadas, como a sua utilização para a prática de crimes, e a criação de novos contatos que colocam em risco bens que ainda não tiveram sua relevância reconhecida pelo Direito. (BRITO, 2013, p. 9).

Assim, a prática do estelionato na modalidade virtual cresceu ao longo dos anos, sempre com a tentativa em paralelo do Direito Penal de acompanhar para poder punir em cerceamento legislativo, com projetos de lei, inovações e acréscimos a legislações já vigentes.
Quanto a responsabilização do crime em questão torna-se direta em relação ao Autor, sendo aferida pelo Estado, mesmo em sua modalidade digital, haja vista que tem o encargo de combater, controlar e reprimir tais práticas tanto no mundo ?real? quanto no ambiente digital, além de ser responsável por tutelar a convivência e atuação neste âmbito cibernético.
Além da responsabilização direta quanto ao autor do delito, muitas vezes a responsabilidade também recai de forma subjetiva ou objetiva para um terceiro da relação que deveria zelar pela segurança dos dados pessoais do usuário, grandes exemplos são os de vazamento de dados bancários online após invasão por hackers, recaindo responsabilidade também para os bancos que deveriam proteger o consumidor.

APELAÇÃO CÍVEL. NEGÓCIOS JURÍDICOS BANCÁRIOS. AÇÃO DE INDENIZAÇÃO POR DANOS MATERIAIS. RESSARCIMENTO DE VALORES. TRANSAÇÃO BANCÁRIA REALIZADA DE FORMA FRAUDULENTA POR TERCEIROS. INTERNET BANKING. RESPONSABILIDADE DO BANCO. SUMULA 479 DO STJ. SENTENÇA MANTIDA. As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias. Súmula 479 do STJ. Art. 14 do CDC. Para
12

responsabilização do prestador de serviços a existência de culpa ou dolo, exige-se apenas a conduta ilícita e a existência de dano, bem como nexo de causalidade entre eles. Caso. Autora que foi vítima de estelionato praticado por terceiro. Empréstimo autorizado pela instituição financeira. Nesse ponto, desimporta que a fraude tenha se perpetrado através dos canais de atendimento via internet (internet banking), porquanto a parte autora negou ter sido a autora dos saques, e o banco não se desincumbiu do ônus de demonstrar a regularidade das transações impugnadas pelo cliente. NEGARAM PROVIMENTO AO APELO. UNÂNIME.

Entre outros exemplos de golpes como os já citados ?phishing?, ?vishing? e ?smishing? que buscam a obtenção de vantagem ilícita frente as vítimas, muitas vezes fazendo uso de um terceiro como ponte para alçar seu objetivo fraudulento, ocorre que, como mencionado, mesmo esse terceiro não tendo o dolo na prática do crime deve garantir a segurança e impermeabilidade do seu sistema para que isso não ocorra, contando com a obrigação de assegurar os direitos do consumidor e usuário. Este é o entendimento das jurisprudências pátrias:
RECURSO INOMINADO. AÇÃO DECLARATÓRIA DE INEXISTÊNCIA DE DÉBITO C/C INDENIZAÇÃO POR DANOS MORAIS. PRELIMINAR DE VIOLAÇÃO AO PRINCÍPIO DA DIALETICDADE. INOCORRÊNCIA. BANCÁRIO. TRANSFERÊNCIA DE VALORES REALIZADA POR TERCEIRO. FRAUDE EVIDENCIADA. CULPA DA VÍTIMA NÃO CONFIGURADA. INSTITUIÇÃO FINANCEIRA QUE NÃO APRESENTOU PROVAS ACERCA DA SEGURANÇA, AUTENTICAÇÃO OU IDENTIFICAÇÃO DA OPERAÇÃO. FALHA NA PRESTAÇÃO DO SERVIÇO CONFIGURADA. RESPONSABILIDADE OBJETIVA DO BANCO. APLICAÇÃO DA SÚMULA 479 DO STJ. RESTITUIÇÃO DEVIDA. AUSÊNCIA DE SOLUÇÃO ADMINISTRATIVA. DANO MORAL CONFIGURADO NO CASO CONCRETO. QUANTUM ARBITRADO EM R$ 2.000,00 (DOIS MIL REAIS) QUE COMPORTA MAJORAÇÃO PARA R$ 3.000,00 (TRÊS MIL REAIS). OBSERVÂNCIA AOS PRINCÍPIOS DA PROPORCIONALIDADE E RAZOABILIDADE. SENTENÇA PARCIALMENTE REFORMADA. Recurso da autora conhecido e provido.Recurso do réu conhecido e desprovido. (TJPR - 1ª Turma Recursal - 0003317-67.2020.8.16.0136 - Pitanga - Rel.: JUIZ DE DIREITO DA TURMA RECURSAL DOS JUIZADOS ESPECIAIS NESTARIO DA SILVA QUEIROZ - J. 23.05.2022)
(TJ-PR - RI: 00033176720208160136 Pitanga 0003317-67.2020.8.16.0136 (Acórdão), Relator: Nestario da Silva Queiroz, Data de Julgamento: 23/05/2022, 1ª Turma Recursal, Data de Publicação: 23/05/2022)

Ressalta-se que o estelionato na sua modalidade digital é considerado crime de ação penal pública incondicionada, ou seja, a responsabilidade para conduzir o procedimento é do Ministério Público, independente de manifestação de vontade da vítima, a natureza dessa ação ressalva a relevância de tratar esse delito de forma mais eficaz, independente da vontade da vítima de ver o autor do crime responsabilizado, com o fito de preservar a ordem social e diminuir o índice de novos casos.
13

Nesse sentido, cumpre destacar que mesmo a responsabilidade do crime ser direta em relação ao Autor, também pode abranger mais partes do processo dependendo da especificada do caso. A jurisprudência entende que a responsabilidade não é apenas do Estado, mas também da empresa, entidade ou qualquer terceiro que tenha a obrigação de tornar o ambiente digital seguro para o

usuário.

3.1 CONCEPÇÃO DAS NORMAS JURÍDICAS ATUALIZADAS E FORMAS DE PUNIÇÃO DO CRIME DO ESTELIONATO DIGITAL.

Como já explicitado, um grande fator que desencadeou o aumento da efetivação do crime em questão foi a pandemia, de modo que, com o advento do Covid-19, foi necessário que a população se protegesse em suas casas para corroborar com o distanciamento social e assim evitar a proliferação do vírus, ocorre que em contrapartida a isso foi destaque a aproximação online dos usuários que culminou em oportunidade para os criminosos inovarem suas artimanhas, contando com a suposta sensação de anonimato.
O crime de estelionato digital, no sistema jurídico atual do Brasil, é apreciado no âmbito do Direito Penal, o qual pressupõe responsabilização para esse tipo de ato, que era equiparado ao crime de estelionato, previsto no artigo 171 do Código Penal.
A Lei 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann, entrou em vigor como uma tentativa inicial de tipificar a conduta dos crimes na modalidade virtual para proteção dos dados pessoais da população em face aos criminosos virtuais, ocorre que com o passar dos anos se mostrou necessária a inclusão de novas medidas frente a progressão da criminalidade no país, em específico os crimes virtuais.
Para combater essa crescente negativa no âmbito jurídico nacional entrou em vigor a lei 14.155/21, de 27 de maio de 2021, que incluiu e modificou alguns parágrafos no supramencionado dispositivo legal, alterando algumas regras para julgar o crime.

Art. 1º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar com as seguintes alterações:
?Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
14

§ 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.
§ 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso:
I ? 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;
II ? Aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável. Pena ? reclusão, de 1 (um) a 4 (quatro) anos, e multa.

§ 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. Pena ? reclusão, de 2 (dois) a 5 (cinco) anos, e multa.

Dentre as alterações, foram incluídos os § § 2º-A e 2º-B, que tratam de fraude eletrônica, sendo o § 2º-A qualificadora para o crime de estelionato que não é praticado na modalidade presencial, ou seja, quando a frade é cometida com uso de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de reses sociais ou qualquer outro meio fraudulento análogo.

Fraude eletrônica
§ 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.
§ 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.
Estelionato contra idoso ou vulnerável
§ 4º A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso.
Art. 2º O art. 70 do Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), passa a vigorar acrescido do seguinte § 4º:
§ 4º Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção.? (NR).

Nesse sentido, observa-se que foram elencados os crimes específicos mediante fraude eletrônica objetivando tornar mais rigorosa a lei, ainda tentando acompanhar o avanço da criminalidade. Frisa-se que a Lei 14.155/21 deu ênfase também ao aumento da pena para esse crime na modalidade virtual, com pena de reclusão de 4 a 8 anos e o aumento de 1/3 ao dobro da pena acaso o crime seja praticado contra idoso ou vulnerável, com expectativa para prejudicar a prática delituosa.
15

Cabe destacar também a alteração quanto a competência para apuração do estelionato por fraude mediante cheque ou transferência bancária, o código de

processo penal previa que a competência era do local do banco sacado, o que muitas vezes dificultava a apuração do crime, até pela localização da vítima que nem sempre residia no mesmo local do banco sacado, competência esta alterada para o domicílio da vítima pela Lei 14.155/21.
Por fim, a execução da lei e a responsabilização dos golpistas submete-se a conduta das autoridades capazes, para investigar, processar e julgar os casos de estelionato digital, como a polícia e o poder judiciário.

4 O HISTÓRICO DA PRÁTICA DO ESTELIONATO DIGITAL E OS REFLEXOS DA LEI 14.155 FRENTE A VULNERABILIDADE DA VÍTIMA.

Como já demonstrado, o estelionato digital foi uma modalidade que cresceu esporadicamente com o advento da internet e o constante avanço da tecnologia, mas também teve um de seus marcos recentemente, em 2020, com crescimento exponencial pela pandemia da covid 19 que possibilitou mais ?vítimas? online.
Relativizando em números, o país registrou um aumento ainda mais expressivo que o estelionato comum quando em sua modalidade virtual, com direta relação a pandemia, em 2021 houve 120.470 (cento e cinto mil, quatrocentos e setenta) casos registrados, já em 2022 foram registrados 200.322 (duzentos mil, trezentos e vinte e dois) casos, um aumento de 66,2% (sessenta e seis virgula dois por cento) de acordo com os dados do Fórum Brasileiro de Segurança Pública (FBSP).
Foram registrados em 2021 115 (cento e quinze) estelionatos a cada 100 (cem) mil habitantes no país, já no ano seguinte foram registrados 189,9 (cento e oitenta e nove virgula nove), um aumento de 65,1% (sessenta e cinco vírgula um porcento), ainda de acordo com a FBSP o estado que detém o recorde de casos registrados de estelionato em sua modalidade digital é Santa Catarina, com 64.230 (sessenta e quatro mil, duzentos e trinta) registros em 2022 o que representa 32% (trinta e dois porcento) dos casos do país, ressalvando que Bahia, Ceará, Rio de Janeiro, Rio Grande do Norte, Rio Grande do Sul e São Paulo não tinham ou não disponibilizaram dados.
Cabe destacar que, além de Santa Catarina, tiveram relevantes aumentos Minas Gerais que passou de 25.574 (vinte e cinco mil, quinhentos e setenta e quatro)
16

casos em 2021 para 35.749 (trinta e cinco mil, setecentos e quarenta e nove) em 2022, um aumento de 49,4% (quarenta e nove vírgula quatro porcento), Distrito Federal que passou de 10.049 (dez mil e quarenta e nove) casos em 2021 para 15.580 (quinze mil, quinhentos e oitenta) em 2022, registrando um aumento de 55% (cinquenta e cinco porcento), e o Espírito Santo que passou de 10.545 (dez mil, quinhentos e quarenta e cinco) casos em 2021 para 15.277 (quinze mil, duzentos e setenta e sete) casos em 2022, o que resultou em um aumento de 44,8% (quarenta e quatro vírgula oito por cento).
Dentre todos esses dados disponibilizados pela FBSP cabe destacar por fim os Estados que mais sofreram variações em seus índices, quais sejam Roraima que

passou de 59 (cinquenta e nove) casos em 2021 para absurdos 759 (setecentos e cinquenta e nove) em 2022 acarretando um aumento de 1.186% (mil, cento e oitenta e seis por cento) e Goiás com um aumento de 1.041% (mil e quarenta e um porcento), passando de 128 (cento e vinte e oito) casos em 2021 para 1.461 (mil, quatrocentos e sessenta e um) casos em 2022.
Ainda sobre o marco recente que corroborou com a prática do referido delito é reiterado pelo Fórum Brasileiro de Segurança Pública (FBSP) que:

A digitalização das finanças, de serviço e do comércio, especialmente impulsionada durante o período pandêmico, contribui com a formação de um ambiente propício ao desenvolvimento de modalidades criminais que exploram vulnerabilidade nestes segmentos. (FBSP 2022, p. 6).

Conforme já citado, a modalidade de estelionato digital foi inserida ao Código Penal em meados de 2021 pela Lei nº 14.155/21 que também especificou o estelionato praticado na modalidade digital, por meio cibernético. Essa lei trouxe novidades legislativas que no geral foram positivas com relação a vulnerabilidade da vítima.
Destarte podemos citar que invadir dispositivo informático de uso alheio, ressalvando que conectado ou não a internet, com o fim de obter vantagem ilícita terá pena de reclusão de 4 (quatro) a 8 (oito) anos e multa, com suas devidas especificações, demonstrando assim a preocupação do legislador com as vítimas que infelizmente só estavam crescendo no país e isso refletiu no agravamento da pena que antigamente era disposta no crime de invasão de dispositivo informático, criando uma resistência ao criminoso na medida em que vê o crime como algo mais grave, mediante nova pena mais severa.
17

Ainda quanto aos reflexos dessa lei frente a vulnerabilidade da vítima podem-se listar os agravantes trazidos em sua redação quanto ao furto, com pena de reclusão de 4 a 8 anos, para o crime nessa modalidade realizado com o uso de dispositivos eletrônicos, conectados ou não a internet, por meio de uso de sistemas invasores ou violação de senha, além do agravamento se praticado contra idosos ou vulnerável com consequente aumento de pena de 1/3 ao dobro, ainda na hipótese de ser praticado por servidor fora do território nacional aumenta a pena de 1/3 (um terço) a 2/3 (dois terços).
Quanto ao estelionato também tornou-se agravante o furto qualificado no âmbito cibernético, com igual pena de reclusão de 4 (quatro) a 8 (oito) anos, além de possível multa e pode ter pena aumentada de 1/3 (um terço) a 2/3 (dois terços) acaso seja praticada por servidor fora do território nacional e acaso praticada contra idoso ou vulnerável poderá ter a pena aumentada de 1/3 (um terço) ao dobro.
Por fim, no que tange a invasão de aparelhos para obtenção de dados, a lei passou de detenção de 3 (três) meses a 1 (um) ano para reclusão de 1 (um) a 4 (quatro) anos. Ainda na hipótese de resultar em obtenção de informações sigilosos

pode ser majorada de reclusão de 2 (dois) a 5 (cinco) anos e multa, com agravante de 1/3 (um terço) a 2/3 (dois terços) caso ocorra prejuízo econômico decorrente da invasão.
Assim, as novidades legislativas trazidas pela lei confortam brasileiros que podem ser vítimas de criminosos fora do território nacional, o que é plenamente possível pelo advento da internet e também a população mais velha que, em suma maioria, não tem familiaridade com as ferramentas e linguagens online, não tendo manejo e trato com os meios digitais o que por muitas vezes os torna os principiais focos dos criminosos pela ?facilidade? e ?inocência? desses usuários em específico, assim como os vulneráveis.
Portanto, resta claro que o legislador buscou efetivamente ampliar a guarda dos direitos, de modo a, buscar uma equidade entre diversos grupos de pessoas/possíveis vítimas, resultando em maior segurança, de modo que passa a observar significativas mudanças objetificando proteger os direitos do usuário e penalizando de forma mais grave os criminosos.

5 CONCLUSÃO.

18

O presente artigo, por meio da análise de dados estatísticos, legislação e julgados, buscou tecer uma análise crítica da disciplina normativa do estelionato digital, suas formas de conduta e as possíveis consequências sociais.
Demonstrando que a sociedade está cada vez mais conectada e as redes sociais têm uma função muito importante nessa interação, ocorre que o aumento desenfreado de pessoas conectadas à internet propiciou um ambiente para prática de crimes e com diversas possibilidades de artimanhas dos criminosos, que enxergam a internet como ?terra sem lei?, para obtenção da vantagem ilícita virtualmente, caracterizando o estelionato digital.
Dentre as diversas artimanhas utilizadas pelos estelionatários destacarm-se o ?phishing?, utilizada para enganar os usuários e conseguir informações privadas, ?vishing? popularmente conhecido por ?phishing por voz? quando o ato é realizado por ligações ou envio de áudios com o mesmo intuito de ludibriar a vítima, mas para divulgar dados pessoais e ?smishing? modalidade em que a vítima é provocada a acessar link que corrompe seu aparelho, além de outros golpes como investimentos fraudulentos, promessas de retornos financeiros utopicamente elevados e esquema de pirâmides, esses golpistas beneficiam-se da leiguice de suas vítimas no âmbito de investimento financeiro com falsas promessas de enriquecimento acelerado para enganá-las.
Assim, restou demonstrado que os golpistas tem o mesmo fito, qual seja a obtenção da vantagem ilícita fazendo uso do ambiente cibernético, enquadrando-os no âmbito de estelionatários digitais.
Nesta senda, ainda não existia um enquadramento específico para conter o avanço do referido ilícito que muitas vezes poderia ser caracterizado como tentativa

de extorsão ou crimes análogos o que obrigou o poder legislativo a se atualizar. Para ?frear? o avanço do crime foi introduzida a Lei 12.737/2012, popularmente conhecida por ?Lei Carolina Dieckmann?, que surgiu após um incidente em que a atriz teve seu aparelho pessoal invadido e com isso o vazamento de fotos íntimas na rede.
A introdução da Lei ?Carolina Dieckmann? mostrou-se muito importante por iniciar a caminhada rumo a tipificada do crime de estelionato em sua modalidade digital, ocorre que a tecnologia seguiu se modernizando trazendo novas oportunidades para inovação dos criminosos que vivem as sombras da internet. Com o estabelecimento de modalidades de transferência eletrônica como ?TED? e ?PIX? 19

tornou-se cada vez mais comum o embate entre as autoridades e os golpistas, já demonstrando a necessidade de nova atualização da legislação atinente ao tema.
Quanto a responsabilidade do crime no âmbito jurídico restou pacificado pelas jurisprudências pátrias que torna-se direta em relação ao Autor, sendo aferida pelo Estado que tem o dever de tutelar a convivência no âmbito cibernético. Cumpre destacar que nem sempre a responsabilidade é exclusiva do Autor, podendo recair de forma subjetiva ou objetiva para um terceiro da relação que deveria zelar pela segurança dos dados pessoais do usuário, tais como bancos, tomadores de serviço...
O marco de crescimento registrado no crime de estelionato na sua modalidade virtual foi durante a pandemia de covid 19, época em que foi necessário a reclusão da população em casa o que gerou aumento exponencial de usuários online na rede e, em paralelo, oportunidade para os criminosos inovarem suas artimanhas.
Para combater essa crescente negativa no âmbito jurídico nacional entrou em vigor a lei 14.155/21, de 27 de maio de 2021 trazendo enrijecimento das penas e tipificação de novos crimes, como estelionato contra idoso ou vulnerável e fraude eletrônica, intentando ainda em penas mais rigorosas que podem ser alongadas a depender do caso e alteração de competência para estelionato por fraude mediante cheque ou transferência bancária, submetendo a execução da lei e responsabilização dos golpistas a conduta das autoridades capazes.
O que se conclui é que, com o passar dos anos as leis e medidas tomadas se tornam ultrapassadas vide o ?aperfeiçoamento? dos criminosos, portanto, com o fito do controle do Estado se tornar uma manutenção mais célere se mostrou necessário inserção de um sistema de inovação e renovação legislativa.
Ora, restou comprovado que o âmbito jurídico sempre buscou acompanhar a inovação criminosa trazendo atualizações a legislação para coibir a progressão desses ataques criminosos, mas igualmente restou comprovado que apenas acompanhar não está mais sendo o suficiente, tornando tendência o adiantamento aos movimentos da marginalidade com sucessivo progresso de imersão tecnológica das autoridades para se adiantar ao crime com a devida manutenção das leis de forma mais célere objetivando deter o claro avanço da criminalidade hodierna.

REFERÊNCIAS

20

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez.

BRASIL, DECRETO-LEI NO 2.848, DE 7 DE DEZEMBRO DE 1940. Código Penal. Rio de Janeiro, 7 de dezembro de 1940; 119º da Independência e 52º da República. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 08/06/2023.

BRASIL. LEI Nº 14.155, DE 27 DE MAIO DE 2021. Lei de Invasão a Dispositivo Informático [Internet]. Disponível em: https://www.in.gov.br/en/web/dou/-/lei-n-14.155-de-27-de-maio-de-2021-322698993. Acesso em: 24 nov. 2023

BRASIL. LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012. Lei de Invasão a Dispositivo Informático [Internet]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em:
24 nov. 2023.

BRASIL. LEI Nº 14.155, DE 27 DE MAIO DE 2021. Lei de Invasão a Dispositivo Informático [Internet]. Disponível em: https://www.in.gov.br/en/web/dou/-/lei-nº 14.155-de-27-de-maio-de-2021-322698993. Acesso em: 13 dez. 2023.

BRASIL. Tribunal de Justiça do Paraná. TJ-PR - Recurso Inominado XXXXX-67.2020.8.16.0136 PR. Relator Nestario da Silva Queiroz. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-pr/1511018743. Acesso em: 25 nov. 2023

BRASIL. Tribunal de Justiça do Rio Grande do Sul. TJ-RS - Apelação Cível XXXXX-22.2020.8.21.7000 RS. Relator Giovanni Conti. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-rs/932015329. Acesso em: 25 nov. 2023

BRITO, Auriney. Direito penal informático. São Paulo: Saraiva, 2013, p.189.

CAMPOS, Pedro Franco de [et al.]. Direito penal aplicado: parte geral e parte especial do Código Penal. - 6ª. Ed. ? São Paulo: Saraiva, 2016.

CASSANTI, Moisés de Oliveira. Crimes virtuais, vítimas reais. 1ª ed. Rio de Janeiro: Brasport, 2014, p.6.

CHAVES, Fábio Barbosa; TEIXEIRA, Filipe Silva. Os crimes de fraude e estelionato cibernético e a proteção do consumidor no e-commerce. 2020. Disponível em: <https://conteudojuridico.com.br>. Acesso em: 12/06/2023.

COELHO, Yuri Carneiro. Curso de Direito Penal Didático. vol. único, 2ª ed. ? São Paulo: Atlas, 2015.

CÔRREA, Gustavo Testa. Aspectos jurídicos da internet. 5. ed. rev. e atual. São Paulo, Saraiva, 2010.

CUNHA, Rogério Sanches. Manual de direito penal: parte especial (arts. 121 ao 361). 11. ed. rev., ampl. e atual. Salvador: JusPODIVM, 2019.
21

CUNHA, Rogério Sanches. Lei 14.155/21 e os crimes de fraude digital - primeiras impressões e reflexos no CP e no CPP. Meu Site Jurídico (JusPodivm), 2021. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2021/05/28/lei-14-15521-e-os-crimes-de-fraude-digital-primeiras-impressoes-e-reflexos-no-cp-e-no-cpp/. Acesso em: 13 dez. 2023.

FBSP. Fórum Brasileiro de Segurança Pública. Os crimes patrimoniais no Brasil: entre novas e velhas dinâmicas. Anuário Brasileiro de Segurança Pública, 2022. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2022/07/07-anuario-2022-os-crimes-patrimoniais-no-brasil-entre-novas-e-velhas-dinamicas.pdf. Acesso em 24 nov. 2023.

GENNARINI, Juliana. Revista de Direito Penal e Processo Penal, ISSN 2674-6093, v. 2, n. 2, jul./dez. 2020.

GONÇALVES, Victor Eduardo Rios. Direito penal esquematizado: parte especial do Código Penal. - 8. ed. ? São Paulo: Saraiva Educação, 2018.
GRECO, Rogério. Curso de Direito Penal: parte especial. v. III. 7. ed. Rio de Janeiro: Ed. Impetus, 2010.

GOUSSINSKY, Eugenio. Crimes digitais têm forte alta em vários estados; saiba como prevenir. Portal R7, 2021. Disponível em: https://noticias.r7.com/tecnologia-e-ciencia/crimes-digitais-tem-forte-alta-em-varios-estados-saiba-como-prevenir-05052021. Acesso em: 12 dez. 2023.

GRECO, Rogério. Curso de Direito Penal: parte especial. v. III. 7. ed. Rio de Janeiro: Ed. Impetus, 2010, p. 228.

HUNGRIA, Nelson. Comentários ao Código Penal ? Vol. IX. Rio de Janeiro: Forense, 1958.

MIRABETE, Júlio Fabbrini e FABBRINI, Renato N./ Manual de direito penal: parte especial: arts. 121 a 234-B do CP ? volume 2, 36° edição, São Paulo, Atlas, 2021.

ESTELIONATO DIGITAL: UMA ANÁLISE CRÍTICA DA DISCIPLINA NORMATIVA, SUAS FORMAS DE CONDUTA E AS POSSÍVEIS CONSEQUÊNCIAS SOCIAIS

Rafael Lemos Garcia de Oliveira1
Ricardo Simões Xavier dos Santos2

Resumo
O presente artigo discorre sobre a figura do estelionato digital, fazendo uma análise crítica da disciplina normativa, suas formas de conduta e as possíveis consequências sociais. É notório que a atual legislação do país tem avançado, conforme mencionado, na forma que tipifica os crimes que ocorrem em meios virtuais, todavia as sanções ainda são moderadas e as normas devem avançar no sentido de impedir a prática dos crimes virtuais. Para que seja viável a hipótese narrada, o Estado tem o dever de incrementar métodos novos de apuração e averiguação e aprimorar os recursos tecnológicos e digitais que estão à disposição das autoridades responsáveis. Nesse sentido, é necessário compreender o que é o estelionato digital, suas características, maneiras de prevenção e formas em que pode aparecer no dia a dia dos usuários da rede, compactuando com a legislação penal e o cabimento de penalização para os criminosos que praticam esse crime. Por fim, conclui-se que a legislação penal brasileira vem evoluindo, mas para que alcance um nível suficiente de eficácia no combate a esse crime é necessário compreender o que é o estelionato digital, suas características, maneiras de prevenção e formas em que pode aparecer no dia a dia dos usuários da rede, compactuando com a legislação penal e o cabimento de penalização para os criminosos que praticam esse crime.

PALAVRAS-CHAVE: Internet. Crime Cibernético. Estelionato Digital. Código Penal.

1 Graduando em bacharelado em direito pela UCSAL. E-mail: rafaell.oliveira@ucsal.edu.br
2 Doutor em Políticas Sociais e Cidadania pela Universidade Católica do Salvador ? UCSal. E-mail:

ricardo.santos@pro.ucsal.br
2

ABSTRACT: This article discusses the figure of digital fraud, making a critical analysis of the normative discipline, its forms of conduct and the possible social consequences. It is notable that the country's current legislation has advanced, as mentioned, in the way it typifies crimes that occur in virtual media, however sanctions are still moderate and standards must advance in order to prevent the practice of virtual crimes. In order for the narrated hypothesis to be viable, the State has the duty to increase new methods of investigation and investigation and improve the technological and digital resources that are available to the responsible authorities. In this sense, it is necessary to understand what digital fraud is, its characteristics, methods of prevention and ways in which it can appear in the daily lives of network users, in agreement with criminal legislation and the appropriateness of penalizing criminals who practice this crime. Finally, it is concluded that Brazilian criminal legislation has been evolving, but in order to achieve a sufficient level of effectiveness in combating this crime, it is necessary to understand what digital fraud is, its characteristics, methods of prevention and forms in which it can appear. in the daily lives of network users, complying with criminal legislation and the appropriateness of penalizing criminals who commit this crime.

KEYWORDS: Internet. Cybercrime. Digital Fraud. Penal Code.

SUMÁRIO: 1 INTRODUÇÃO. 2 CONDUTA DO ESTELIONATO DIGITAL: CONCEITOS PRÉVIOS, DISCUSSÕES INICIAIS E FORMAS APRESENTADAS. 2.1 Análise acerca das eventuais consequências sociais advindas da conduta do estelionato digital 3 A RESPONSABILIZAÇÃO DO CRIME DE ESTELIONATO DIGITAL NO ÂMBITO JURÍDICO 3.1 Concepção das normas jurídicas atualizadas e formas de punição do crime do estelionato digital 4 O HISTÓRICO DA PRÁTICA DO ESTELIONATO DIGITAL E OS REFLEXOS DA LEI 14.155 FRENTE A VULNERABILIDADE DA VÍTIMA 5 CONCLUSÃO 6 REFERÊNCIAS

1 INTRODUÇÃO

No âmbito penalista são diversos os crimes que têm como objetivo a obtenção de lucros financeiros da vítima, o referido trabalho tem como objetivo abordar o estelionato digital fazendo uma análise crítica da disciplina normativa, apresentando suas formas de conduta e relacionando a suas possíveis consequências sociais.
3

Há uma previsão legal do Código Penal em garantir que todos os cidadãos lesados por práticas de golpes, em que são utilizados artifícios ou qualquer meio fraudulento, podem ingressar no juízo criminal a fim de prosseguirem com a punição penal e com o ressarcimento dos prejuízos.
Para breve introito, o estelionato é 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.
Dentre os crimes mais comuns no Brasil e no mundo pode-se destacar o estelionato, além do meio físico os criminosos procuram pela navegação na rede com o fito de obtenção de dados e informações das pessoas que tem perfil para serem suas possíveis vítimas, pondo em prática das mais diversas maneiras tais como ligações, mensagens, falsificação de identidade, haja vista que todos os dias, a população vive a internet, cadastrando senhas, trocando mensagens, adentrando redes sociais, fazendo negócios pela internet...
Nesse sentido, acompanhando o aumento dos usuários das redes a realização de crimes online cresceu consideravelmente, obviamente relacionado a simplicidade de manejo dos meios virtuais e pela dificuldade de identificação dos criminosos para posterior punição, haja vista ausência de legislações específicas e supressão das identidades.
A realização de golpes e fraudes cometendo ilícitos para obter vantagem sob outras pessoas é prática recorrente e por muitas vezes impune no Brasil, com o estelionato digital não é diferente.
Em sua esfera digital ele se configura quando o criminoso submete o aparelho da vítima e sincroniza-o a demais sistemas de informação ou, em outra hipótese, quando a vítima é posta em uma conjuntura de sensibilidade para obtenção de vantagem ilícita. Na atualidade é mais comum do que se imagina conhecer alguém que tenha passado por essa situação e caído nesse golpe, desde ligações de números sem chamador ou desconhecidos a e-mails/mensagens com ofertas incríveis.
Outro ponto importante que contribuiu para esse aumento, além da facilidade no manejo dos meios virtuais foi o advento da pandemia do Covid-19, as práticas desses crimes se multiplicaram, haja vista que, relevante porcentagem da população tanto brasileira quanto mundial, se viu obrigada a passar mais tempo em casa, o que, em consequência, ampliou o número de pessoas online, acessando a rede. Neste liame, os criminosos têm agido cada vez mais e feito várias vítimas no mundo virtual.
4

Para que o crime possa ser classificado como estelionato digital é imprescindível que a entrega das informações pela vítima seja de forma voluntária, haja vista que a obtenção dos dados se deu por outros meios, o crime pode ter outra classificação, tal como ?furto mediante fraude eletrônica?.
Dentre as principais vítimas desse crime tão comum na atualidade estão as pessoas desatentas e que não tomam total atenção para se esquivar dos estelionatários, seguindo as hipóteses de compra e venda pela internet não verificando a fonte, se é de confiança etc., links enviados de números aleatórios possibilitando o acesso do criminoso a rede da vítima entre outros...
A despeito da clara regulação e evolução da internet e redes sociais, os conselhos e observações para a premeditação dos crimes digitais em geral continua sendo de cuidado e cautela com os dados pessoais e sua divulgação, ainda com o remetente e usuários/links que adentra. É necessário que sempre pense que tudo que

identifique quem você é ou que busque saber informações que só você teria acesso são o alerta inicial para entender se não se está diante de uma possível tentativa de estelionato digital.
É notório que a atual legislação do país tem avançado, conforme mencionado, na forma que tipifica os crimes que ocorrem em meios virtuais, todavia as sanções ainda são moderadas e as normas devem avançar no sentido de impedir a prática dos crimes virtuais. Para que seja viável a hipótese narrada, o Estado tem o dever de incrementar métodos novos de apuração e averiguação e aprimorar os recursos tecnológicos e digitais que estão à disposição das autoridades responsáveis.
Nesse sentido, é necessário compreender o que é o estelionato digital, suas características, maneiras de prevenção e formas em que pode aparecer no dia a dia dos usuários da rede, compactuando com a legislação penal e o cabimento de penalização para os criminosos que praticam esse crime.
Assim, as perguntas que ficam são quais as formas de conduta do estelionato digital e seus impactos na sociedade, além do questionamento acerca das normas brasileiras, nosso sistema jurídico atual contempla qual espécie de responsabilização para o crime de estelionato digital, alinhado a isso, como o Estado Democrático Brasileiro pode melhorar para combater o aumento desse crime.
No presente artigo, seguindo após a introdução para o capítulo ?2? onde serão apresentadas as condutas do estelionato digital, seus conceitos prévios e formas apresentadas, a diferença entre o estelionato e outros crimes contra o patrimônio e
5

sua forma de proliferação pela rede mediante sites falsos, mensagens e e-mails. O capítulo ?2? contém ainda um subtópico ?2.1? onde serão analisadas as consequências sociais advindas da conduta do estelionato digital, desde a inovação dos criminosos partindo para o meio digital até os ?traumas? das vítimas e sua repercussão na sociedade.
Já no capítulo ?3? será amplamente explicada a quem deve ser dirigida a responsabilidade pelo crime do estelionato digital, no âmbito jurídico, já que o crime na grande maioria das vezes tem por conclusão a ?fuga? do criminoso pelo meio cibernético. Ainda no capítulo ?3? serão exploradas, mediante subtópico ?3.1?, as normas jurídicas atualizadas e formas de punição do crime tendo relação direta com a ampla possibilidade de escape do criminoso.
Por fim, em capítulo ?4?, será demonstrado o histórico da prática do estelionato digital, sua evolução paralela ao avanço da tecnologia na sociedade e os reflexos da Lei 14.155, instituída em 2021 especialmente para tornar mais grave a pena de estelionato cometido de forma eletrônica pela internet, frente ainda a vulnerabilidade da vítima. Seguidos da conclusão e as referências bibliográficas.
De certo, cumpre-se destacar que a pesquisa em questão, valeu-se do método da revisão bibliográfica de trabalhos científicos atualizados das áreas penal e constitucional, frente às questões sociais, publicadas em periódicos nacionais e internacionais, qualificados como publicações de A1, assim como B1. Além de importantes nomes do cenário retrato, ao passo que se cita Rogério Greco e Fabio

Barbosa Chavez, bem como análise jurisprudencial e legislativa da lei 14.155.
Compreende-se então, que a escolha metodológica se justifica de base teórica, fundada em estudos atualizados sobre o estelionato digital, suas formas de conduta e as consequências sociais.
O foco da pesquisa bibliográfica foi de apresentar informações e dados específicos sobre a evolução dos crimes digitais, exibindo o progresso do direito penal frente os crimes digitais, através da análise filosófica e de referenciais teóricos de artigos, códigos e outros trabalhos sobre a mesma questão jurídica. Assim, o método empregado é de leitura e análise de material doutrinário especializado já existente sobre o tema de Direito Penal, tal como de jurisprudência, dados, legislação e artigos científicos.

6

2 CONDUTA DO ESTELIONATO DIGITAL: CONCEITOS PRÉVIOS, DISCUSSÕES INICIAIS E FORMAS APRESENTADAS.

O termo estelionato está disposta no Art. 171 do Código Penal como:

Art. 171. Obter, para si ou para outrem, vantagem ilícita em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: pena ? Reclusão, de 1 (um) a 5 (cinco) anos, de multa.

Trata-se de crime contra o patrimônio onde a legislação penal visa proteger a inviolabilidade patrimonial orientada pela prática de atos que visam enganar a vítima e beneficiar o agente (CUNHA, 2019, p. 345).
Assim, pode-se inferir que a diferença entre o estelionato e os diversos crimes contra o patrimônio, ou seja, crimes que tenham por objetivo atentar contra o patrimônio de uma pessoa ou organização, é que no estelionato não é utilizada a força para obtenção de ?vantagem?. É sabido, portanto, que essa atitude é conhecida há muitos anos, de modo que Greco cita que:

Desde que surgiram as relações sociais, o homem se vale da fraude para dissimular seus verdadeiros sentimentos e intenções para, de alguma forma, ocultar ou falsear a verdade, a fim de obter vantagens que, em tese, lhe seriam indevidas (GRECO, 2019, p. 228).

Ressalta-se que o crime existe apenas na modalidade dolosa, sem previsão na forma culposa.
A respeito da expressão ?vantagem ilícita?, Fernando Capez (2020) ensina que, esta, trata-se do objeto material do crime e, caso o agente esteja agindo em razão de uma vantagem devida, a conduta é tipificada como exercício arbitrário das próprias razões, delito previsto no art. 345, do Código Penal.
De acordo com o que se retira do artigo 171, do supramencionado dispositivo

legal, o estelionato pode ser cometido mediante artificio, ardil ou qualquer outro meio fraudulento. Em relação ao termo ?artificio?, o doutrinador Júlio Fabbrini Mirabete ensina o seguinte:

?o artifício existe quando o agente se utilizar de um aparato que modifica, ao menos aparentemente, o aspecto material da coisa, figurando entre esses meios o documento falso ou outra falsificação qualquer, o disfarce, a modificação por aparelhos mecânicos ou elétricos, filmes, efeitos de luz etc.? (MIRABETE, 2021, pag. 325).

Em sua modalidade digital o estelionato ocorre através de sites falsos, mensagens e até e-mail, sendo prioritariamente focado no âmbito virtual. É bastante
7

normal que o consumidor busque virtualmente os mesmos bens desejados fisicamente, mas com a comodidade de não se deslocar e em grande maioria dos casos a acessibilidade com preços menores, levando a promessa da oferta muitas vezes a encantar o consumidor que não percebe a fraude.
Dentre as formas de conduta do referido crime podem ser listadas as mais comuns sendo: vendas falsas em sua maioria quando os estelionatários oferecem serviços ou produtos inexistentes em redes sociais e/ou sites e links de comércio eletrônico; ?phishing?, uma artimanha utilizada pelos criminosos para enganar os usuários e conseguir informações privadas, tais como senhas, detalhes de cartões de crédito, comumente realizado por meio do envio de mensagens eletrônicas se passando por instituições de confiança, pode ser realizado por sites e por redes sociais também, mas sempre com o intuito de prejudicar e obter vantagem, ?vishing? popularmente conhecido por ?phishing por voz? quando o ato é realizado por ligações ou envio de áudios com o mesmo intuito de ludibriar a vítima, mas para divulgar dados pessoais, ?smishing? realizada também por mensagem, mas nessa modalidade a vítima é provocada a acessar link que corrompe seu aparelho, e por último os golpes de investimentos fraudulentos que podem acontecer de diversas maneiras, tais como promessas de retornos financeiros utopicamente elevados e esquema de pirâmides, esses golpistas beneficiam-se da leiguice de suas vítimas no âmbito de investimento financeiro com falsas promessas de enriquecimento acelerado para enganá-las.
No Art. 171 do Código Penal, o estelionato possui a pena de reclusão de 1 a 5 anos e multa. Diante disso, o crime admite suspensão condicional no processo de acordo com o art. 89, § 1ª, da Lei dos Juizados Especiais - Lei n. 9099/95:

Art. 89. Nos crimes em que a pena mínima cominada for igual ou inferior a um ano, abrangidas ou não por esta Lei, o Ministério Público, ao oferecer a denúncia, poderá propor a suspensão do processo, por dois a quatro anos, desde que o acusado não esteja sendo processado ou não tenha sido condenado por outro crime, presentes os demais requisitos que autorizariam a suspensão condicional da pena (art. 77 do Código Penal).

Conforme dito, o crime de estelionato digital, no sistema jurídico atual do Brasil, é apreciado no âmbito do Direito Penal o qual pressupõe responsabilização penal para esse tipo de ato, o qual era equiparado ao crime de estelionato, previsto no artigo 171 do Código Penal, ocorre que ainda no caminhar para a especificação do crime de estelionato na modalidade digital foi introduzida a Lei 12.737/2012, ou como é popularmente conhecida a ?Lei Carolina Dieckmann?, que surgiu após um incidente 8

em que a atriz teve seu aparelho pessoal invadido e com isso o vazamento de fotos íntimas na rede, mediante ainda tentativa de extorsão.
Na época em questão os criminosos seriam apenas denunciados pelo crime de tentativa de extorsão, haja vista ausência de legislação específica quanto aos crimes digitais, assim vários projetos de lei foram analisados para tentar tipificar condutas para crimes semelhantes ao sofrido pela atriz e findada essa fase foi sancionada a Lei 12.737/2012 que entrou em vigor em 02 de abril de 2013.
A lei visava combater o vazamento de informações pessoais dos usuários das redes, zelando pela proteção da privacidade dos mesmos, ainda acrescentou ao Código Penal, mais especificamente no Decreto-Lei 2848, os artigos 154-A e 154-B.

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

A lei se demonstrou efetiva a época da sanção sendo citada como um marco legislativo por muitos autores, desde que entrou em vigor a invasão de computadores, celulares, tablets...no geral dispositivos informáticos alheios passou a ser crime.
Cabe destacar que execução da lei e a responsabilização dos golpistas submete-se a conduta das autoridades capazes, para investigar, processar e julgar os casos de estelionato digital, como a polícia e o Poder Judiciário.

2.1 ANÁLISE ACERCA DAS EVENTUAIS CONSEQUÊNCIAS SOCIAIS ADVINDAS DA CONDUTA DO ESTELIONATO DIGITAL.

A sociedade está cada vez mais conectada e as redes sociais têm uma função muito importante nessa interação, vez que o ser humano sempre precisou de convívio

social. Assim, tais ferramentas estão presentes na vida de muitos brasileiros e esse ambiente digital, como já evidenciado, tornou-se, também, um meio para a prática de crimes, seja pela facilidade de acesso e/ou pelo grande número de usuários.
9

Na atualidade existe uma grande facilidade na obtenção de produtos, sendo de maneira virtual, de modo que não existe mais a necessidade do consumidor se deslocar até o fornecedor para adquirir o produto, nesta feita, é notório que a compra virtual vem amadurecendo cada vez mais, o que consequentemente ocasiona um aumento dos crimes cibernéticos. Nesse contexto, Chaves e Teixeira destacam que:

Com a investigação correta é possível localizar e punir os criminosos que causaram prejuízo a essa nova espécie de consumidores. Todavia, no mesmo ritmo que a internet evolui, os fraudadores também se renovam com novas modalidades de golpes, alguns tão específicos que são até difíceis de definir qual a punição correta a ser aplicada (CHAVES e TEIXEIRA, 2019, p. 119).

Conforme já citado a inovação dos criminosos acompanha em paralelo o avanço da tecnologia pela sociedade, de modo que muitos usuários têm a sensação de que a internet é ?terra sem lei? fomentando sua ?liberdade tecnológica? em pequenos delitos, tais como injúria, difamação... Ao passo em que não imaginam ter a sua responsabilidade realmente comprovada, agindo por trás da tela do celular ou computador.
Perpassando por isso os criminosos buscam a obtenção de vantagem ilícita e veem na internet uma oportunidade recheada de opções, possuídos pela sensação de impunidade e munidos das mais diversas artimanhas para concluir seu objetivo. Cumpre ressaltar que sociedade caminha para um futuro mais tecnológico e os criminosos ?surfam nessa onda?.
A cada dia que passa resta mais rudimentar os métodos de pagamento por cédulas ou moedas, a trajetória da população tem destino eletrônico, de modo que é fato notório o quão comum se tornaram os sistemas de pagamento eletrônico, estando já alguns mais rudimentares como a transferência ?TED?.
A popularização dos sistemas de pagamento eletrônico, a exemplo do ?pix?, propicia diariamente um combate necessário entre as autoridades e os golpistas. Já é rotina na sociedade a divulgação de novos meios de golpes cibernéticos com o fito de alertar os usuários a se precaverem mais, infelizmente nem sempre todo cuidado é tomado e as consequências podem ser desastrosas para os consumidores da rede.
O prejuízo causado a essa nova espécie de consumidores afeta tanto de forma direta as vítimas quanto a sociedade, de maneira geral. Dentre as consequências sociais advindas dessa conduta resta mister destacar o impacto financeiro nas vítimas, de forma direta, que podem encarar perdas financeiras o que acarreta
10

problemas emocionais e instabilidade, perda de confiança no meio digital para compras que também gera impacto na maneira como as pessoas conduzem negócios online.
Além do consumidor direto, as instituições financeiras também sofrem em muitos casos ressarcindo o valor perdido por seus clientes lesados, arcando com o custo de fraude e também no investimento em segurança virtual, mesmo ainda tendo um receio a implantação dos pagamentos digitais buscando ao máximo reforçar sua segurança desde confirmação por ?face id? quanto senhas regularmente trocadas e ?tokens digitais?, sempre tentando confirmar que é realmente o usuário da conta quem realmente está fazendo a operação e não um terceiro. Frisa-se que essas consequências sociais acarretam, num todo, impacto na economia.
Felizmente, não são somente os consumidores que passam pelo processo de consequências negativas, mas também os fraudadores. Mesmo diante da crescente a qual ocorre o ?fenômeno? do estelionato digital, os criminosos não restam imunes a responsabilização pelo seu crime. Conforme será demonstrado no presente artigo, a legislação do país delimita o crime e suas consequências, assim como as penalidades que podem levar os fraudadores a condenação pelas atividades ilícitas.
Nesse sentido, o avanço da tecnologia com o passar dos tempos corroborou indiretamente para que os criminosos inovassem seus meios ilícitos para obtenção de vantagens, causando diversos impactos na sociedade que não teriam como ser positivos, sendo alguns dos principais o prejuízo financeiro as vítimas; perda de confiança na segurança online e transações digitais, além do choque nos sistemas judiciais, de segurança e nas bases digitais o que consequentemente requer mecanismos e investimentos relevantes de atribuição das empresas e do judiciário.
Sendo assim, infere-se que ainda existe certa dificuldade para identificação dos golpistas o que, alternativamente, tem relação com a legislação brasileira que tem avançado na tipificação dos crimes cibernéticos, todavia as sanções ainda são moderadas e as normas devem acompanhar no sentido de bridar a prática desses crimes na modalidade virtual.

3 A RESPONSABILIZAÇÃO DO CRIME DE ESTELIONATO DIGITAL NO ÂMBITO JURÍDICO.

11

É claro que a internet e toda a esfera digital não foi inserida na sociedade com o intuito ou sequer resguarda em relação a possibilidade do advento de crimes em paralelo a isso, mas como toda imprevisão, a criminalidade evoluiu em conjunto deixando cada vez mais vulnerável a segurança dos usuários na rede, como amplamente demonstrado no presente trabalho, os golpes digitais se aperfeiçoam com o passar dos anos, com ênfase para o estelionato que conta hoje com diversos tipos de obtenção de vantagem ilícita na sua modalidade digital.
A internet tornou-se essencial na rotina da população, interligando usuários e pessoas conectadas a rede, assim, como bem destacou Uchoa de Brito:

(...) O problema da internet passou a ser identificado quando a tecnologia incrementou e complicou as relações sociais consideradas, até então, pacíficas e controladas, possibilitando algumas experiências socialmente desagradáveis e indesejadas, como a sua utilização para a prática de crimes, e a criação de novos contatos que colocam em risco bens que ainda não tiveram sua relevância reconhecida pelo Direito. (BRITO, 2013, p. 9).

Assim, a prática do estelionato na modalidade virtual cresceu ao longo dos anos, sempre com a tentativa em paralelo do Direito Penal de acompanhar para poder punir em cerceamento legislativo, com projetos de lei, inovações e acréscimos a legislações já vigentes.
Quanto a responsabilização do crime em questão torna-se direta em relação ao Autor, sendo aferida pelo Estado, mesmo em sua modalidade digital, haja vista que tem o encargo de combater, controlar e reprimir tais práticas tanto no mundo ?real? quanto no ambiente digital, além de ser responsável por tutelar a convivência e atuação neste âmbito cibernético.
Além da responsabilização direta quanto ao autor do delito, muitas vezes a responsabilidade também recai de forma subjetiva ou objetiva para um terceiro da relação que deveria zelar pela segurança dos dados pessoais do usuário, grandes exemplos são os de vazamento de dados bancários online após invasão por hackers, recaindo responsabilidade também para os bancos que deveriam proteger o consumidor.

APELAÇÃO CÍVEL. NEGÓCIOS JURÍDICOS BANCÁRIOS. AÇÃO DE INDENIZAÇÃO POR DANOS MATERIAIS. RESSARCIMENTO DE VALORES. TRANSAÇÃO BANCÁRIA REALIZADA DE FORMA FRAUDULENTA POR TERCEIROS. INTERNET BANKING. RESPONSABILIDADE DO BANCO. SUMULA 479 DO STJ. SENTENÇA MANTIDA. As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias. Súmula 479 do STJ. Art. 14 do CDC. Para
12

responsabilização do prestador de serviços a existência de culpa ou dolo, exige-se apenas a conduta ilícita e a existência de dano, bem como nexo de causalidade entre eles. Caso. Autora que foi vítima de estelionato praticado por terceiro. Empréstimo autorizado pela instituição financeira. Nesse ponto, desimporta que a fraude tenha se perpetrado através dos canais de atendimento via internet (internet banking), porquanto a parte autora negou ter sido a autora dos saques, e o banco não se desincumbiu do ônus de demonstrar a regularidade das transações impugnadas pelo cliente. NEGARAM PROVIMENTO AO APELO. UNÂNIME.

Entre outros exemplos de golpes como os já citados ?phishing?, ?vishing? e ?smishing? que buscam a obtenção de vantagem ilícita frente as vítimas, muitas vezes fazendo uso de um terceiro como ponte para alçar seu objetivo fraudulento, ocorre que, como mencionado, mesmo esse terceiro não tendo o dolo na prática do crime deve garantir a segurança e impermeabilidade do seu sistema para que isso não ocorra, contando com a obrigação de assegurar os direitos do consumidor e usuário. Este é o entendimento das jurisprudências pátrias:
RECURSO INOMINADO. AÇÃO DECLARATÓRIA DE INEXISTÊNCIA DE DÉBITO C/C INDENIZAÇÃO POR DANOS MORAIS. PRELIMINAR DE VIOLAÇÃO AO PRINCÍPIO DA DIALETICDADE. INOCORRÊNCIA. BANCÁRIO. TRANSFERÊNCIA DE VALORES REALIZADA POR TERCEIRO. FRAUDE EVIDENCIADA. CULPA DA VÍTIMA NÃO CONFIGURADA. INSTITUIÇÃO FINANCEIRA QUE NÃO APRESENTOU PROVAS ACERCA DA SEGURANÇA, AUTENTICAÇÃO OU IDENTIFICAÇÃO DA OPERAÇÃO. FALHA NA PRESTAÇÃO DO SERVIÇO CONFIGURADA. RESPONSABILIDADE OBJETIVA DO BANCO. APLICAÇÃO DA SÚMULA 479 DO STJ. RESTITUIÇÃO DEVIDA. AUSÊNCIA DE SOLUÇÃO ADMINISTRATIVA. DANO MORAL CONFIGURADO NO CASO CONCRETO. QUANTUM ARBITRADO EM R$ 2.000,00 (DOIS MIL REAIS) QUE COMPORTA MAJORAÇÃO PARA R$ 3.000,00 (TRÊS MIL REAIS). OBSERVÂNCIA AOS PRINCÍPIOS DA PROPORCIONALIDADE E RAZOABILIDADE. SENTENÇA PARCIALMENTE REFORMADA. Recurso da autora conhecido e provido.Recurso do réu conhecido e desprovido. (TJPR - 1ª Turma Recursal - 0003317-67.2020.8.16.0136 - Pitanga - Rel.: JUIZ DE DIREITO DA TURMA RECURSAL DOS JUIZADOS ESPECIAIS NESTARIO DA SILVA QUEIROZ - J. 23.05.2022)
(TJ-PR - RI: 00033176720208160136 Pitanga 0003317-67.2020.8.16.0136 (Acórdão), Relator: Nestario da Silva Queiroz, Data de Julgamento: 23/05/2022, 1ª Turma Recursal, Data de Publicação: 23/05/2022)

Ressalta-se que o estelionato na sua modalidade digital é considerado crime de ação penal pública incondicionada, ou seja, a responsabilidade para conduzir o procedimento é do Ministério Público, independente de manifestação de vontade da vítima, a natureza dessa ação ressalva a relevância de tratar esse delito de forma mais eficaz, independente da vontade da vítima de ver o autor do crime responsabilizado, com o fito de preservar a ordem social e diminuir o índice de novos casos.
13

Nesse sentido, cumpre destacar que mesmo a responsabilidade do crime ser direta em relação ao Autor, também pode abranger mais partes do processo dependendo da especificada do caso. A jurisprudência entende que a responsabilidade não é apenas do Estado, mas também da empresa, entidade ou qualquer terceiro que tenha a obrigação de tornar o ambiente digital seguro para o

usuário.

3.1 CONCEPÇÃO DAS NORMAS JURÍDICAS ATUALIZADAS E FORMAS DE PUNIÇÃO DO CRIME DO ESTELIONATO DIGITAL.

Como já explicitado, um grande fator que desencadeou o aumento da efetivação do crime em questão foi a pandemia, de modo que, com o advento do Covid-19, foi necessário que a população se protegesse em suas casas para corroborar com o distanciamento social e assim evitar a proliferação do vírus, ocorre que em contrapartida a isso foi destaque a aproximação online dos usuários que culminou em oportunidade para os criminosos inovarem suas artimanhas, contando com a suposta sensação de anonimato.
O crime de estelionato digital, no sistema jurídico atual do Brasil, é apreciado no âmbito do Direito Penal, o qual pressupõe responsabilização para esse tipo de ato, que era equiparado ao crime de estelionato, previsto no artigo 171 do Código Penal.
A Lei 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann, entrou em vigor como uma tentativa inicial de tipificar a conduta dos crimes na modalidade virtual para proteção dos dados pessoais da população em face aos criminosos virtuais, ocorre que com o passar dos anos se mostrou necessária a inclusão de novas medidas frente a progressão da criminalidade no país, em específico os crimes virtuais.
Para combater essa crescente negativa no âmbito jurídico nacional entrou em vigor a lei 14.155/21, de 27 de maio de 2021, que incluiu e modificou alguns parágrafos no supramencionado dispositivo legal, alterando algumas regras para julgar o crime.

Art. 1º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar com as seguintes alterações:
?Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
14

§ 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.
§ 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso:
I ? 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;
II ? Aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável. Pena ? reclusão, de 1 (um) a 4 (quatro) anos, e multa.

§ 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. Pena ? reclusão, de 2 (dois) a 5 (cinco) anos, e multa.

Dentre as alterações, foram incluídos os § § 2º-A e 2º-B, que tratam de fraude eletrônica, sendo o § 2º-A qualificadora para o crime de estelionato que não é praticado na modalidade presencial, ou seja, quando a frade é cometida com uso de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de reses sociais ou qualquer outro meio fraudulento análogo.

Fraude eletrônica
§ 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.
§ 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.
Estelionato contra idoso ou vulnerável
§ 4º A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso.
Art. 2º O art. 70 do Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), passa a vigorar acrescido do seguinte § 4º:
§ 4º Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção.? (NR).

Nesse sentido, observa-se que foram elencados os crimes específicos mediante fraude eletrônica objetivando tornar mais rigorosa a lei, ainda tentando acompanhar o avanço da criminalidade. Frisa-se que a Lei 14.155/21 deu ênfase também ao aumento da pena para esse crime na modalidade virtual, com pena de reclusão de 4 a 8 anos e o aumento de 1/3 ao dobro da pena acaso o crime seja praticado contra idoso ou vulnerável, com expectativa para prejudicar a prática delituosa.
15

Cabe destacar também a alteração quanto a competência para apuração do estelionato por fraude mediante cheque ou transferência bancária, o código de

processo penal previa que a competência era do local do banco sacado, o que muitas vezes dificultava a apuração do crime, até pela localização da vítima que nem sempre residia no mesmo local do banco sacado, competência esta alterada para o domicílio da vítima pela Lei 14.155/21.
Por fim, a execução da lei e a responsabilização dos golpistas submete-se a conduta das autoridades capazes, para investigar, processar e julgar os casos de estelionato digital, como a polícia e o poder judiciário.

4 O HISTÓRICO DA PRÁTICA DO ESTELIONATO DIGITAL E OS REFLEXOS DA LEI 14.155 FRENTE A VULNERABILIDADE DA VÍTIMA.

Como já demonstrado, o estelionato digital foi uma modalidade que cresceu esporadicamente com o advento da internet e o constante avanço da tecnologia, mas também teve um de seus marcos recentemente, em 2020, com crescimento exponencial pela pandemia da covid 19 que possibilitou mais ?vítimas? online.
Relativizando em números, o país registrou um aumento ainda mais expressivo que o estelionato comum quando em sua modalidade virtual, com direta relação a pandemia, em 2021 houve 120.470 (cento e cinto mil, quatrocentos e setenta) casos registrados, já em 2022 foram registrados 200.322 (duzentos mil, trezentos e vinte e dois) casos, um aumento de 66,2% (sessenta e seis virgula dois por cento) de acordo com os dados do Fórum Brasileiro de Segurança Pública (FBSP).
Foram registrados em 2021 115 (cento e quinze) estelionatos a cada 100 (cem) mil habitantes no país, já no ano seguinte foram registrados 189,9 (cento e oitenta e nove virgula nove), um aumento de 65,1% (sessenta e cinco vírgula um porcento), ainda de acordo com a FBSP o estado que detém o recorde de casos registrados de estelionato em sua modalidade digital é Santa Catarina, com 64.230 (sessenta e quatro mil, duzentos e trinta) registros em 2022 o que representa 32% (trinta e dois porcento) dos casos do país, ressalvando que Bahia, Ceará, Rio de Janeiro, Rio Grande do Norte, Rio Grande do Sul e São Paulo não tinham ou não disponibilizaram dados.
Cabe destacar que, além de Santa Catarina, tiveram relevantes aumentos Minas Gerais que passou de 25.574 (vinte e cinco mil, quinhentos e setenta e quatro)
16

casos em 2021 para 35.749 (trinta e cinco mil, setecentos e quarenta e nove) em 2022, um aumento de 49,4% (quarenta e nove vírgula quatro porcento), Distrito Federal que passou de 10.049 (dez mil e quarenta e nove) casos em 2021 para 15.580 (quinze mil, quinhentos e oitenta) em 2022, registrando um aumento de 55% (cinquenta e cinco porcento), e o Espírito Santo que passou de 10.545 (dez mil, quinhentos e quarenta e cinco) casos em 2021 para 15.277 (quinze mil, duzentos e setenta e sete) casos em 2022, o que resultou em um aumento de 44,8% (quarenta e quatro vírgula oito por cento).
Dentre todos esses dados disponibilizados pela FBSP cabe destacar por fim os Estados que mais sofreram variações em seus índices, quais sejam Roraima que

passou de 59 (cinquenta e nove) casos em 2021 para absurdos 759 (setecentos e cinquenta e nove) em 2022 acarretando um aumento de 1.186% (mil, cento e oitenta e seis por cento) e Goiás com um aumento de 1.041% (mil e quarenta e um porcento), passando de 128 (cento e vinte e oito) casos em 2021 para 1.461 (mil, quatrocentos e sessenta e um) casos em 2022.
Ainda sobre o marco recente que corroborou com a prática do referido delito é reiterado pelo Fórum Brasileiro de Segurança Pública (FBSP) que:

A digitalização das finanças, de serviço e do comércio, especialmente impulsionada durante o período pandêmico, contribui com a formação de um ambiente propício ao desenvolvimento de modalidades criminais que exploram vulnerabilidade nestes segmentos. (FBSP 2022, p. 6).

Conforme já citado, a modalidade de estelionato digital foi inserida ao Código Penal em meados de 2021 pela Lei nº 14.155/21 que também especificou o estelionato praticado na modalidade digital, por meio cibernético. Essa lei trouxe novidades legislativas que no geral foram positivas com relação a vulnerabilidade da vítima.
Destarte podemos citar que invadir dispositivo informático de uso alheio, ressalvando que conectado ou não a internet, com o fim de obter vantagem ilícita terá pena de reclusão de 4 (quatro) a 8 (oito) anos e multa, com suas devidas especificações, demonstrando assim a preocupação do legislador com as vítimas que infelizmente só estavam crescendo no país e isso refletiu no agravamento da pena que antigamente era disposta no crime de invasão de dispositivo informático, criando uma resistência ao criminoso na medida em que vê o crime como algo mais grave, mediante nova pena mais severa.
17

Ainda quanto aos reflexos dessa lei frente a vulnerabilidade da vítima podem-se listar os agravantes trazidos em sua redação quanto ao furto, com pena de reclusão de 4 a 8 anos, para o crime nessa modalidade realizado com o uso de dispositivos eletrônicos, conectados ou não a internet, por meio de uso de sistemas invasores ou violação de senha, além do agravamento se praticado contra idosos ou vulnerável com consequente aumento de pena de 1/3 ao dobro, ainda na hipótese de ser praticado por servidor fora do território nacional aumenta a pena de 1/3 (um terço) a 2/3 (dois terços).
Quanto ao estelionato também tornou-se agravante o furto qualificado no âmbito cibernético, com igual pena de reclusão de 4 (quatro) a 8 (oito) anos, além de possível multa e pode ter pena aumentada de 1/3 (um terço) a 2/3 (dois terços) acaso seja praticada por servidor fora do território nacional e acaso praticada contra idoso ou vulnerável poderá ter a pena aumentada de 1/3 (um terço) ao dobro.
Por fim, no que tange a invasão de aparelhos para obtenção de dados, a lei passou de detenção de 3 (três) meses a 1 (um) ano para reclusão de 1 (um) a 4 (quatro) anos. Ainda na hipótese de resultar em obtenção de informações sigilosos

pode ser majorada de reclusão de 2 (dois) a 5 (cinco) anos e multa, com agravante de 1/3 (um terço) a 2/3 (dois terços) caso ocorra prejuízo econômico decorrente da invasão.
Assim, as novidades legislativas trazidas pela lei confortam brasileiros que podem ser vítimas de criminosos fora do território nacional, o que é plenamente possível pelo advento da internet e também a população mais velha que, em suma maioria, não tem familiaridade com as ferramentas e linguagens online, não tendo manejo e trato com os meios digitais o que por muitas vezes os torna os principiais focos dos criminosos pela ?facilidade? e ?inocência? desses usuários em específico, assim como os vulneráveis.
Portanto, resta claro que o legislador buscou efetivamente ampliar a guarda dos direitos, de modo a, buscar uma equidade entre diversos grupos de pessoas/possíveis vítimas, resultando em maior segurança, de modo que passa a observar significativas mudanças objetificando proteger os direitos do usuário e penalizando de forma mais grave os criminosos.

5 CONCLUSÃO.

18

O presente artigo, por meio da análise de dados estatísticos, legislação e julgados, buscou tecer uma análise crítica da disciplina normativa do estelionato digital, suas formas de conduta e as possíveis consequências sociais.
Demonstrando que a sociedade está cada vez mais conectada e as redes sociais têm uma função muito importante nessa interação, ocorre que o aumento desenfreado de pessoas conectadas à internet propiciou um ambiente para prática de crimes e com diversas possibilidades de artimanhas dos criminosos, que enxergam a internet como ?terra sem lei?, para obtenção da vantagem ilícita virtualmente, caracterizando o estelionato digital.
Dentre as diversas artimanhas utilizadas pelos estelionatários destacarm-se o ?phishing?, utilizada para enganar os usuários e conseguir informações privadas, ?vishing? popularmente conhecido por ?phishing por voz? quando o ato é realizado por ligações ou envio de áudios com o mesmo intuito de ludibriar a vítima, mas para divulgar dados pessoais e ?smishing? modalidade em que a vítima é provocada a acessar link que corrompe seu aparelho, além de outros golpes como investimentos fraudulentos, promessas de retornos financeiros utopicamente elevados e esquema de pirâmides, esses golpistas beneficiam-se da leiguice de suas vítimas no âmbito de investimento financeiro com falsas promessas de enriquecimento acelerado para enganá-las.
Assim, restou demonstrado que os golpistas tem o mesmo fito, qual seja a obtenção da vantagem ilícita fazendo uso do ambiente cibernético, enquadrando-os no âmbito de estelionatários digitais.
Nesta senda, ainda não existia um enquadramento específico para conter o avanço do referido ilícito que muitas vezes poderia ser caracterizado como tentativa

de extorsão ou crimes análogos o que obrigou o poder legislativo a se atualizar. Para ?frear? o avanço do crime foi introduzida a Lei 12.737/2012, popularmente conhecida por ?Lei Carolina Dieckmann?, que surgiu após um incidente em que a atriz teve seu aparelho pessoal invadido e com isso o vazamento de fotos íntimas na rede.
A introdução da Lei ?Carolina Dieckmann? mostrou-se muito importante por iniciar a caminhada rumo a tipificada do crime de estelionato em sua modalidade digital, ocorre que a tecnologia seguiu se modernizando trazendo novas oportunidades para inovação dos criminosos que vivem as sombras da internet. Com o estabelecimento de modalidades de transferência eletrônica como ?TED? e ?PIX? 19

tornou-se cada vez mais comum o embate entre as autoridades e os golpistas, já demonstrando a necessidade de nova atualização da legislação atinente ao tema.
Quanto a responsabilidade do crime no âmbito jurídico restou pacificado pelas jurisprudências pátrias que torna-se direta em relação ao Autor, sendo aferida pelo Estado que tem o dever de tutelar a convivência no âmbito cibernético. Cumpre destacar que nem sempre a responsabilidade é exclusiva do Autor, podendo recair de forma subjetiva ou objetiva para um terceiro da relação que deveria zelar pela segurança dos dados pessoais do usuário, tais como bancos, tomadores de serviço...
O marco de crescimento registrado no crime de estelionato na sua modalidade virtual foi durante a pandemia de covid 19, época em que foi necessário a reclusão da população em casa o que gerou aumento exponencial de usuários online na rede e, em paralelo, oportunidade para os criminosos inovarem suas artimanhas.
Para combater essa crescente negativa no âmbito jurídico nacional entrou em vigor a lei 14.155/21, de 27 de maio de 2021 trazendo enrijecimento das penas e tipificação de novos crimes, como estelionato contra idoso ou vulnerável e fraude eletrônica, intentando ainda em penas mais rigorosas que podem ser alongadas a depender do caso e alteração de competência para estelionato por fraude mediante cheque ou transferência bancária, submetendo a execução da lei e responsabilização dos golpistas a conduta das autoridades capazes.
O que se conclui é que, com o passar dos anos as leis e medidas tomadas se tornam ultrapassadas vide o ?aperfeiçoamento? dos criminosos, portanto, com o fito do controle do Estado se tornar uma manutenção mais célere se mostrou necessário inserção de um sistema de inovação e renovação legislativa.
Ora, restou comprovado que o âmbito jurídico sempre buscou acompanhar a inovação criminosa trazendo atualizações a legislação para coibir a progressão desses ataques criminosos, mas igualmente restou comprovado que apenas acompanhar não está mais sendo o suficiente, tornando tendência o adiantamento aos movimentos da marginalidade com sucessivo progresso de imersão tecnológica das autoridades para se adiantar ao crime com a devida manutenção das leis de forma mais célere objetivando deter o claro avanço da criminalidade hodierna.

REFERÊNCIAS

20

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez.

BRASIL, DECRETO-LEI NO 2.848, DE 7 DE DEZEMBRO DE 1940. Código Penal. Rio de Janeiro, 7 de dezembro de 1940; 119º da Independência e 52º da República. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 08/06/2023.

BRASIL. LEI Nº 14.155, DE 27 DE MAIO DE 2021. Lei de Invasão a Dispositivo Informático [Internet]. Disponível em: https://www.in.gov.br/en/web/dou/-/lei-n-14.155-de-27-de-maio-de-2021-322698993. Acesso em: 24 nov. 2023

BRASIL. LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012. Lei de Invasão a Dispositivo Informático [Internet]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em:
24 nov. 2023.

BRASIL. LEI Nº 14.155, DE 27 DE MAIO DE 2021. Lei de Invasão a Dispositivo Informático [Internet]. Disponível em: https://www.in.gov.br/en/web/dou/-/lei-nº 14.155-de-27-de-maio-de-2021-322698993. Acesso em: 13 dez. 2023.

BRASIL. Tribunal de Justiça do Paraná. TJ-PR - Recurso Inominado XXXXX-67.2020.8.16.0136 PR. Relator Nestario da Silva Queiroz. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-pr/1511018743. Acesso em: 25 nov. 2023

BRASIL. Tribunal de Justiça do Rio Grande do Sul. TJ-RS - Apelação Cível XXXXX-22.2020.8.21.7000 RS. Relator Giovanni Conti. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-rs/932015329. Acesso em: 25 nov. 2023

BRITO, Auriney. Direito penal informático. São Paulo: Saraiva, 2013, p.189.

CAMPOS, Pedro Franco de [et al.]. Direito penal aplicado: parte geral e parte especial do Código Penal. - 6ª. Ed. ? São Paulo: Saraiva, 2016.

CASSANTI, Moisés de Oliveira. Crimes virtuais, vítimas reais. 1ª ed. Rio de Janeiro: Brasport, 2014, p.6.

CHAVES, Fábio Barbosa; TEIXEIRA, Filipe Silva. Os crimes de fraude e estelionato cibernético e a proteção do consumidor no e-commerce. 2020. Disponível em: <https://conteudojuridico.com.br>. Acesso em: 12/06/2023.

COELHO, Yuri Carneiro. Curso de Direito Penal Didático. vol. único, 2ª ed. ? São Paulo: Atlas, 2015.

CÔRREA, Gustavo Testa. Aspectos jurídicos da internet. 5. ed. rev. e atual. São Paulo, Saraiva, 2010.

CUNHA, Rogério Sanches. Manual de direito penal: parte especial (arts. 121 ao 361). 11. ed. rev., ampl. e atual. Salvador: JusPODIVM, 2019.
21

CUNHA, Rogério Sanches. Lei 14.155/21 e os crimes de fraude digital - primeiras impressões e reflexos no CP e no CPP. Meu Site Jurídico (JusPodivm), 2021. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2021/05/28/lei-14-15521-e-os-crimes-de-fraude-digital-primeiras-impressoes-e-reflexos-no-cp-e-no-cpp/. Acesso em: 13 dez. 2023.

FBSP. Fórum Brasileiro de Segurança Pública. Os crimes patrimoniais no Brasil: entre novas e velhas dinâmicas. Anuário Brasileiro de Segurança Pública, 2022. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2022/07/07-anuario-2022-os-crimes-patrimoniais-no-brasil-entre-novas-e-velhas-dinamicas.pdf. Acesso em 24 nov. 2023.

GENNARINI, Juliana. Revista de Direito Penal e Processo Penal, ISSN 2674-6093, v. 2, n. 2, jul./dez. 2020.

GONÇALVES, Victor Eduardo Rios. Direito penal esquematizado: parte especial do Código Penal. - 8. ed. ? São Paulo: Saraiva Educação, 2018.
GRECO, Rogério. Curso de Direito Penal: parte especial. v. III. 7. ed. Rio de Janeiro: Ed. Impetus, 2010.

GOUSSINSKY, Eugenio. Crimes digitais têm forte alta em vários estados; saiba como prevenir. Portal R7, 2021. Disponível em: https://noticias.r7.com/tecnologia-e-ciencia/crimes-digitais-tem-forte-alta-em-varios-estados-saiba-como-prevenir-05052021. Acesso em: 12 dez. 2023.

GRECO, Rogério. Curso de Direito Penal: parte especial. v. III. 7. ed. Rio de Janeiro: Ed. Impetus, 2010, p. 228.

HUNGRIA, Nelson. Comentários ao Código Penal ? Vol. IX. Rio de Janeiro: Forense, 1958.

MIRABETE, Júlio Fabbrini e FABBRINI, Renato N./ Manual de direito penal: parte especial: arts. 121 a 234-B do CP ? volume 2, 36° edição, São Paulo, Atlas, 2021.

ESTELIONATO DIGITAL: UMA ANÁLISE CRÍTICA DA DISCIPLINA NORMATIVA, SUAS FORMAS DE CONDUTA E AS POSSÍVEIS CONSEQUÊNCIAS SOCIAIS

Rafael Lemos Garcia de Oliveira1
Ricardo Simões Xavier dos Santos2

Resumo
O presente artigo discorre sobre a figura do estelionato digital, fazendo uma análise crítica da disciplina normativa, suas formas de conduta e as possíveis consequências sociais. É notório que a atual legislação do país tem avançado, conforme mencionado, na forma que tipifica os crimes que ocorrem em meios virtuais, todavia as sanções ainda são moderadas e as normas devem avançar no sentido de impedir a prática dos crimes virtuais. Para que seja viável a hipótese narrada, o Estado tem o dever de incrementar métodos novos de apuração e averiguação e aprimorar os recursos tecnológicos e digitais que estão à disposição das autoridades responsáveis. Nesse sentido, é necessário compreender o que é o estelionato digital, suas características, maneiras de prevenção e formas em que pode aparecer no dia a dia dos usuários da rede, compactuando com a legislação penal e o cabimento de penalização para os criminosos que praticam esse crime. Por fim, conclui-se que a legislação penal brasileira vem evoluindo, mas para que alcance um nível suficiente de eficácia no combate a esse crime é necessário compreender o que é o estelionato digital, suas características, maneiras de prevenção e formas em que pode aparecer no dia a dia dos usuários da rede, compactuando com a legislação penal e o cabimento de penalização para os criminosos que praticam esse crime.

PALAVRAS-CHAVE: Internet. Crime Cibernético. Estelionato Digital. Código Penal.

1 Graduando em bacharelado em direito pela UCSAL. E-mail: rafaell.oliveira@ucsal.edu.br

2 Doutor em Políticas Sociais e Cidadania pela Universidade Católica do Salvador ? UCSal. E-mail: ricardo.santos@pro.ucsal.br
2

ABSTRACT: This article discusses the figure of digital fraud, making a critical analysis of the normative discipline, its forms of conduct and the possible social consequences. It is notable that the country's current legislation has advanced, as mentioned, in the way it typifies crimes that occur in virtual media, however sanctions are still moderate and standards must advance in order to prevent the practice of virtual crimes. In order for the narrated hypothesis to be viable, the State has the duty to increase new methods of investigation and investigation and improve the technological and digital resources that are available to the responsible authorities. In this sense, it is necessary to understand what digital fraud is, its characteristics, methods of prevention and ways in which it can appear in the daily lives of network users, in agreement with criminal legislation and the appropriateness of penalizing criminals who practice this crime. Finally, it is concluded that Brazilian criminal legislation has been evolving, but in order to achieve a sufficient level of effectiveness in combating this crime, it is necessary to understand what digital fraud is, its characteristics, methods of prevention and forms in which it can appear. in the daily lives of network users, complying with criminal legislation and the appropriateness of penalizing criminals who commit this crime.

KEYWORDS: Internet. Cybercrime. Digital Fraud. Penal Code.

SUMÁRIO: 1 INTRODUÇÃO. 2 CONDUTA DO ESTELIONATO DIGITAL: CONCEITOS PRÉVIOS, DISCUSSÕES INICIAIS E FORMAS APRESENTADAS. 2.1 Análise acerca das eventuais consequências sociais advindas da conduta do estelionato digital 3 A RESPONSABILIZAÇÃO DO CRIME DE ESTELIONATO DIGITAL NO ÂMBITO JURÍDICO 3.1 Concepção das normas jurídicas atualizadas e formas de punição do crime do estelionato digital 4 O HISTÓRICO DA PRÁTICA DO ESTELIONATO DIGITAL E OS REFLEXOS DA LEI 14.155 FRENTE A VULNERABILIDADE DA VÍTIMA 5 CONCLUSÃO 6 REFERÊNCIAS

1 INTRODUÇÃO

No âmbito penalista são diversos os crimes que têm como objetivo a obtenção de lucros financeiros da vítima, o referido trabalho tem como objetivo abordar o estelionato digital fazendo uma análise crítica da disciplina normativa, apresentando suas formas de conduta e relacionando a suas possíveis consequências sociais.
3

Há uma previsão legal do Código Penal em garantir que todos os cidadãos lesados por práticas de golpes, em que são utilizados artifícios ou qualquer meio fraudulento, podem ingressar no juízo criminal a fim de prosseguirem com a punição penal e com o ressarcimento dos prejuízos.

Para breve introito, o estelionato é 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.
Dentre os crimes mais comuns no Brasil e no mundo pode-se destacar o estelionato, além do meio físico os criminosos procuram pela navegação na rede com o fito de obtenção de dados e informações das pessoas que tem perfil para serem suas possíveis vítimas, pondo em prática das mais diversas maneiras tais como ligações, mensagens, falsificação de identidade, haja vista que todos os dias, a população vive a internet, cadastrando senhas, trocando mensagens, adentrando redes sociais, fazendo negócios pela internet...
Nesse sentido, acompanhando o aumento dos usuários das redes a realização de crimes online cresceu consideravelmente, obviamente relacionado a simplicidade de manejo dos meios virtuais e pela dificuldade de identificação dos criminosos para posterior punição, haja vista ausência de legislações específicas e supressão das identidades.
A realização de golpes e fraudes cometendo ilícitos para obter vantagem sob outras pessoas é prática recorrente e por muitas vezes impune no Brasil, com o estelionato digital não é diferente.
Em sua esfera digital ele se configura quando o criminoso submete o aparelho da vítima e sincroniza-o a demais sistemas de informação ou, em outra hipótese, quando a vítima é posta em uma conjuntura de sensibilidade para obtenção de vantagem ilícita. Na atualidade é mais comum do que se imagina conhecer alguém que tenha passado por essa situação e caído nesse golpe, desde ligações de números sem chamador ou desconhecidos a e-mails/mensagens com ofertas incríveis.
Outro ponto importante que contribuiu para esse aumento, além da facilidade no manejo dos meios virtuais foi o advento da pandemia do Covid-19, as práticas desses crimes se multiplicaram, haja vista que, relevante porcentagem da população tanto brasileira quanto mundial, se viu obrigada a passar mais tempo em casa, o que, em consequência, ampliou o número de pessoas online, acessando a rede. Neste liame, os criminosos têm agido cada vez mais e feito várias vítimas no mundo virtual.
4

Para que o crime possa ser classificado como estelionato digital é imprescindível que a entrega das informações pela vítima seja de forma voluntária, haja vista que a obtenção dos dados se deu por outros meios, o crime pode ter outra classificação, tal como ?furto mediante fraude eletrônica?.
Dentre as principais vítimas desse crime tão comum na atualidade estão as pessoas desatentas e que não tomam total atenção para se esquivar dos estelionatários, seguindo as hipóteses de compra e venda pela internet não verificando a fonte, se é de confiança etc., links enviados de números aleatórios possibilitando o acesso do criminoso a rede da vítima entre outros...
A despeito da clara regulação e evolução da internet e redes sociais, os conselhos e observações para a premeditação dos crimes digitais em geral continua sendo de cuidado e cautela com os dados pessoais e sua divulgação, ainda com o

remetente e usuários/links que adentra. É necessário que sempre pense que tudo que identifique quem você é ou que busque saber informações que só você teria acesso são o alerta inicial para entender se não se está diante de uma possível tentativa de estelionato digital.
É notório que a atual legislação do país tem avançado, conforme mencionado, na forma que tipifica os crimes que ocorrem em meios virtuais, todavia as sanções ainda são moderadas e as normas devem avançar no sentido de impedir a prática dos crimes virtuais. Para que seja viável a hipótese narrada, o Estado tem o dever de incrementar métodos novos de apuração e averiguação e aprimorar os recursos tecnológicos e digitais que estão à disposição das autoridades responsáveis.
Nesse sentido, é necessário compreender o que é o estelionato digital, suas características, maneiras de prevenção e formas em que pode aparecer no dia a dia dos usuários da rede, compactuando com a legislação penal e o cabimento de penalização para os criminosos que praticam esse crime.
Assim, as perguntas que ficam são quais as formas de conduta do estelionato digital e seus impactos na sociedade, além do questionamento acerca das normas brasileiras, nosso sistema jurídico atual contempla qual espécie de responsabilização para o crime de estelionato digital, alinhado a isso, como o Estado Democrático Brasileiro pode melhorar para combater o aumento desse crime.
No presente artigo, seguindo após a introdução para o capítulo ?2? onde serão apresentadas as condutas do estelionato digital, seus conceitos prévios e formas apresentadas, a diferença entre o estelionato e outros crimes contra o patrimônio e
5

sua forma de proliferação pela rede mediante sites falsos, mensagens e e-mails. O capítulo ?2? contém ainda um subtópico ?2.1? onde serão analisadas as consequências sociais advindas da conduta do estelionato digital, desde a inovação dos criminosos partindo para o meio digital até os ?traumas? das vítimas e sua repercussão na sociedade.
Já no capítulo ?3? será amplamente explicada a quem deve ser dirigida a responsabilidade pelo crime do estelionato digital, no âmbito jurídico, já que o crime na grande maioria das vezes tem por conclusão a ?fuga? do criminoso pelo meio cibernético. Ainda no capítulo ?3? serão exploradas, mediante subtópico ?3.1?, as normas jurídicas atualizadas e formas de punição do crime tendo relação direta com a ampla possibilidade de escape do criminoso.
Por fim, em capítulo ?4?, será demonstrado o histórico da prática do estelionato digital, sua evolução paralela ao avanço da tecnologia na sociedade e os reflexos da Lei 14.155, instituída em 2021 especialmente para tornar mais grave a pena de estelionato cometido de forma eletrônica pela internet, frente ainda a vulnerabilidade da vítima. Seguidos da conclusão e as referências bibliográficas.
De certo, cumpre-se destacar que a pesquisa em questão, valeu-se do método da revisão bibliográfica de trabalhos científicos atualizados das áreas penal e constitucional, frente às questões sociais, publicadas em periódicos nacionais e internacionais, qualificados como publicações de A1, assim como B1. Além de

importantes nomes do cenário retrato, ao passo que se cita Rogério Greco e Fabio Barbosa Chavez, bem como análise jurisprudencial e legislativa da lei 14.155.
Compreende-se então, que a escolha metodológica se justifica de base teórica, fundada em estudos atualizados sobre o estelionato digital, suas formas de conduta e as consequências sociais.
O foco da pesquisa bibliográfica foi de apresentar informações e dados específicos sobre a evolução dos crimes digitais, exibindo o progresso do direito penal frente os crimes digitais, através da análise filosófica e de referenciais teóricos de artigos, códigos e outros trabalhos sobre a mesma questão jurídica. Assim, o método empregado é de leitura e análise de material doutrinário especializado já existente sobre o tema de Direito Penal, tal como de jurisprudência, dados, legislação e artigos científicos.

6

2 CONDUTA DO ESTELIONATO DIGITAL: CONCEITOS PRÉVIOS, DISCUSSÕES INICIAIS E FORMAS APRESENTADAS.

O termo estelionato está disposta no Art. 171 do Código Penal como:

Art. 171. Obter, para si ou para outrem, vantagem ilícita em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: pena ? Reclusão, de 1 (um) a 5 (cinco) anos, de multa.

Trata-se de crime contra o patrimônio onde a legislação penal visa proteger a inviolabilidade patrimonial orientada pela prática de atos que visam enganar a vítima e beneficiar o agente (CUNHA, 2019, p. 345).
Assim, pode-se inferir que a diferença entre o estelionato e os diversos crimes contra o patrimônio, ou seja, crimes que tenham por objetivo atentar contra o patrimônio de uma pessoa ou organização, é que no estelionato não é utilizada a força para obtenção de ?vantagem?. É sabido, portanto, que essa atitude é conhecida há muitos anos, de modo que Greco cita que:

Desde que surgiram as relações sociais, o homem se vale da fraude para dissimular seus verdadeiros sentimentos e intenções para, de alguma forma, ocultar ou falsear a verdade, a fim de obter vantagens que, em tese, lhe seriam indevidas (GRECO, 2019, p. 228).

Ressalta-se que o crime existe apenas na modalidade dolosa, sem previsão na forma culposa.
A respeito da expressão ?vantagem ilícita?, Fernando Capez (2020) ensina que, esta, trata-se do objeto material do crime e, caso o agente esteja agindo em razão de uma vantagem devida, a conduta é tipificada como exercício arbitrário das próprias razões, delito previsto no art. 345, do Código Penal.

De acordo com o que se retira do artigo 171, do supramencionado dispositivo legal, o estelionato pode ser cometido mediante artificio, ardil ou qualquer outro meio fraudulento. Em relação ao termo ?artificio?, o doutrinador Júlio Fabbrini Mirabete ensina o seguinte:

?o artifício existe quando o agente se utilizar de um aparato que modifica, ao menos aparentemente, o aspecto material da coisa, figurando entre esses meios o documento falso ou outra falsificação qualquer, o disfarce, a modificação por aparelhos mecânicos ou elétricos, filmes, efeitos de luz etc.? (MIRABETE, 2021, pag. 325).

Em sua modalidade digital o estelionato ocorre através de sites falsos, mensagens e até e-mail, sendo prioritariamente focado no âmbito virtual. É bastante
7

normal que o consumidor busque virtualmente os mesmos bens desejados fisicamente, mas com a comodidade de não se deslocar e em grande maioria dos casos a acessibilidade com preços menores, levando a promessa da oferta muitas vezes a encantar o consumidor que não percebe a fraude.
Dentre as formas de conduta do referido crime podem ser listadas as mais comuns sendo: vendas falsas em sua maioria quando os estelionatários oferecem serviços ou produtos inexistentes em redes sociais e/ou sites e links de comércio eletrônico; ?phishing?, uma artimanha utilizada pelos criminosos para enganar os usuários e conseguir informações privadas, tais como senhas, detalhes de cartões de crédito, comumente realizado por meio do envio de mensagens eletrônicas se passando por instituições de confiança, pode ser realizado por sites e por redes sociais também, mas sempre com o intuito de prejudicar e obter vantagem, ?vishing? popularmente conhecido por ?phishing por voz? quando o ato é realizado por ligações ou envio de áudios com o mesmo intuito de ludibriar a vítima, mas para divulgar dados pessoais, ?smishing? realizada também por mensagem, mas nessa modalidade a vítima é provocada a acessar link que corrompe seu aparelho, e por último os golpes de investimentos fraudulentos que podem acontecer de diversas maneiras, tais como promessas de retornos financeiros utopicamente elevados e esquema de pirâmides, esses golpistas beneficiam-se da leiguice de suas vítimas no âmbito de investimento financeiro com falsas promessas de enriquecimento acelerado para enganá-las.
No Art. 171 do Código Penal, o estelionato possui a pena de reclusão de 1 a 5 anos e multa. Diante disso, o crime admite suspensão condicional no processo de acordo com o art. 89, § 1ª, da Lei dos Juizados Especiais - Lei n. 9099/95:

Art. 89. Nos crimes em que a pena mínima cominada for igual ou inferior a um ano, abrangidas ou não por esta Lei, o Ministério Público, ao oferecer a denúncia, poderá propor a suspensão do processo, por dois a quatro anos, desde que o acusado não esteja sendo processado ou não tenha sido condenado por outro crime, presentes os demais requisitos que autorizariam

a suspensão condicional da pena (art. 77 do Código Penal).

Conforme dito, o crime de estelionato digital, no sistema jurídico atual do Brasil, é apreciado no âmbito do Direito Penal o qual pressupõe responsabilização penal para esse tipo de ato, o qual era equiparado ao crime de estelionato, previsto no artigo 171 do Código Penal, ocorre que ainda no caminhar para a especificação do crime de estelionato na modalidade digital foi introduzida a Lei 12.737/2012, ou como é popularmente conhecida a ?Lei Carolina Dieckmann?, que surgiu após um incidente 8

em que a atriz teve seu aparelho pessoal invadido e com isso o vazamento de fotos íntimas na rede, mediante ainda tentativa de extorsão.
Na época em questão os criminosos seriam apenas denunciados pelo crime de tentativa de extorsão, haja vista ausência de legislação específica quanto aos crimes digitais, assim vários projetos de lei foram analisados para tentar tipificar condutas para crimes semelhantes ao sofrido pela atriz e findada essa fase foi sancionada a Lei 12.737/2012 que entrou em vigor em 02 de abril de 2013.
A lei visava combater o vazamento de informações pessoais dos usuários das redes, zelando pela proteção da privacidade dos mesmos, ainda acrescentou ao Código Penal, mais especificamente no Decreto-Lei 2848, os artigos 154-A e 154-B.

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

A lei se demonstrou efetiva a época da sanção sendo citada como um marco legislativo por muitos autores, desde que entrou em vigor a invasão de computadores, celulares, tablets...no geral dispositivos informáticos alheios passou a ser crime.
Cabe destacar que execução da lei e a responsabilização dos golpistas submete-se a conduta das autoridades capazes, para investigar, processar e julgar os casos de estelionato digital, como a polícia e o Poder Judiciário.

2.1 ANÁLISE ACERCA DAS EVENTUAIS CONSEQUÊNCIAS SOCIAIS ADVINDAS DA CONDUTA DO ESTELIONATO DIGITAL.

A sociedade está cada vez mais conectada e as redes sociais têm uma função

muito importante nessa interação, vez que o ser humano sempre precisou de convívio social. Assim, tais ferramentas estão presentes na vida de muitos brasileiros e esse ambiente digital, como já evidenciado, tornou-se, também, um meio para a prática de crimes, seja pela facilidade de acesso e/ou pelo grande número de usuários.
9

Na atualidade existe uma grande facilidade na obtenção de produtos, sendo de maneira virtual, de modo que não existe mais a necessidade do consumidor se deslocar até o fornecedor para adquirir o produto, nesta feita, é notório que a compra virtual vem amadurecendo cada vez mais, o que consequentemente ocasiona um aumento dos crimes cibernéticos. Nesse contexto, Chaves e Teixeira destacam que:

Com a investigação correta é possível localizar e punir os criminosos que causaram prejuízo a essa nova espécie de consumidores. Todavia, no mesmo ritmo que a internet evolui, os fraudadores também se renovam com novas modalidades de golpes, alguns tão específicos que são até difíceis de definir qual a punição correta a ser aplicada (CHAVES e TEIXEIRA, 2019, p. 119).

Conforme já citado a inovação dos criminosos acompanha em paralelo o avanço da tecnologia pela sociedade, de modo que muitos usuários têm a sensação de que a internet é ?terra sem lei? fomentando sua ?liberdade tecnológica? em pequenos delitos, tais como injúria, difamação... Ao passo em que não imaginam ter a sua responsabilidade realmente comprovada, agindo por trás da tela do celular ou computador.
Perpassando por isso os criminosos buscam a obtenção de vantagem ilícita e veem na internet uma oportunidade recheada de opções, possuídos pela sensação de impunidade e munidos das mais diversas artimanhas para concluir seu objetivo. Cumpre ressaltar que sociedade caminha para um futuro mais tecnológico e os criminosos ?surfam nessa onda?.
A cada dia que passa resta mais rudimentar os métodos de pagamento por cédulas ou moedas, a trajetória da população tem destino eletrônico, de modo que é fato notório o quão comum se tornaram os sistemas de pagamento eletrônico, estando já alguns mais rudimentares como a transferência ?TED?.
A popularização dos sistemas de pagamento eletrônico, a exemplo do ?pix?, propicia diariamente um combate necessário entre as autoridades e os golpistas. Já é rotina na sociedade a divulgação de novos meios de golpes cibernéticos com o fito de alertar os usuários a se precaverem mais, infelizmente nem sempre todo cuidado é tomado e as consequências podem ser desastrosas para os consumidores da rede.
O prejuízo causado a essa nova espécie de consumidores afeta tanto de forma direta as vítimas quanto a sociedade, de maneira geral. Dentre as consequências sociais advindas dessa conduta resta mister destacar o impacto financeiro nas vítimas, de forma direta, que podem encarar perdas financeiras o que acarreta
10

problemas emocionais e instabilidade, perda de confiança no meio digital para compras que também gera impacto na maneira como as pessoas conduzem negócios online.
Além do consumidor direto, as instituições financeiras também sofrem em muitos casos ressarcindo o valor perdido por seus clientes lesados, arcando com o custo de fraude e também no investimento em segurança virtual, mesmo ainda tendo um receio a implantação dos pagamentos digitais buscando ao máximo reforçar sua segurança desde confirmação por ?face id? quanto senhas regularmente trocadas e ?tokens digitais?, sempre tentando confirmar que é realmente o usuário da conta quem realmente está fazendo a operação e não um terceiro. Frisa-se que essas consequências sociais acarretam, num todo, impacto na economia.
Felizmente, não são somente os consumidores que passam pelo processo de consequências negativas, mas também os fraudadores. Mesmo diante da crescente a qual ocorre o ?fenômeno? do estelionato digital, os criminosos não restam imunes a responsabilização pelo seu crime. Conforme será demonstrado no presente artigo, a legislação do país delimita o crime e suas consequências, assim como as penalidades que podem levar os fraudadores a condenação pelas atividades ilícitas.
Nesse sentido, o avanço da tecnologia com o passar dos tempos corroborou indiretamente para que os criminosos inovassem seus meios ilícitos para obtenção de vantagens, causando diversos impactos na sociedade que não teriam como ser positivos, sendo alguns dos principais o prejuízo financeiro as vítimas; perda de confiança na segurança online e transações digitais, além do choque nos sistemas judiciais, de segurança e nas bases digitais o que consequentemente requer mecanismos e investimentos relevantes de atribuição das empresas e do judiciário.
Sendo assim, infere-se que ainda existe certa dificuldade para identificação dos golpistas o que, alternativamente, tem relação com a legislação brasileira que tem avançado na tipificação dos crimes cibernéticos, todavia as sanções ainda são moderadas e as normas devem acompanhar no sentido de bridar a prática desses crimes na modalidade virtual.

3 A RESPONSABILIZAÇÃO DO CRIME DE ESTELIONATO DIGITAL NO ÂMBITO JURÍDICO.

11

É claro que a internet e toda a esfera digital não foi inserida na sociedade com o intuito ou sequer resguarda em relação a possibilidade do advento de crimes em paralelo a isso, mas como toda imprevisão, a criminalidade evoluiu em conjunto deixando cada vez mais vulnerável a segurança dos usuários na rede, como amplamente demonstrado no presente trabalho, os golpes digitais se aperfeiçoam com o passar dos anos, com ênfase para o estelionato que conta hoje com diversos tipos de obtenção de vantagem ilícita na sua modalidade digital.
A internet tornou-se essencial na rotina da população, interligando usuários e

pessoas conectadas a rede, assim, como bem destacou Uchoa de Brito:

(...) O problema da internet passou a ser identificado quando a tecnologia incrementou e complicou as relações sociais consideradas, até então, pacíficas e controladas, possibilitando algumas experiências socialmente desagradáveis e indesejadas, como a sua utilização para a prática de crimes, e a criação de novos contatos que colocam em risco bens que ainda não tiveram sua relevância reconhecida pelo Direito. (BRITO, 2013, p. 9).

Assim, a prática do estelionato na modalidade virtual cresceu ao longo dos anos, sempre com a tentativa em paralelo do Direito Penal de acompanhar para poder punir em cerceamento legislativo, com projetos de lei, inovações e acréscimos a legislações já vigentes.
Quanto a responsabilização do crime em questão torna-se direta em relação ao Autor, sendo aferida pelo Estado, mesmo em sua modalidade digital, haja vista que tem o encargo de combater, controlar e reprimir tais práticas tanto no mundo ?real? quanto no ambiente digital, além de ser responsável por tutelar a convivência e atuação neste âmbito cibernético.
Além da responsabilização direta quanto ao autor do delito, muitas vezes a responsabilidade também recai de forma subjetiva ou objetiva para um terceiro da relação que deveria zelar pela segurança dos dados pessoais do usuário, grandes exemplos são os de vazamento de dados bancários online após invasão por hackers, recaindo responsabilidade também para os bancos que deveriam proteger o consumidor.

APELAÇÃO CÍVEL. NEGÓCIOS JURÍDICOS BANCÁRIOS. AÇÃO DE INDENIZAÇÃO POR DANOS MATERIAIS. RESSARCIMENTO DE VALORES. TRANSAÇÃO BANCÁRIA REALIZADA DE FORMA FRAUDULENTA POR TERCEIROS. INTERNET BANKING. RESPONSABILIDADE DO BANCO. SUMULA 479 DO STJ. SENTENÇA MANTIDA. As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias. Súmula 479 do STJ. Art. 14 do CDC. Para
12

responsabilização do prestador de serviços a existência de culpa ou dolo, exige-se apenas a conduta ilícita e a existência de dano, bem como nexo de causalidade entre eles. Caso. Autora que foi vítima de estelionato praticado por terceiro. Empréstimo autorizado pela instituição financeira. Nesse ponto, desimporta que a fraude tenha se perpetrado através dos canais de atendimento via internet (internet banking), porquanto a parte autora negou ter sido a autora dos saques, e o banco não se desincumbiu do ônus de demonstrar a regularidade das transações impugnadas pelo cliente. NEGARAM PROVIMENTO AO APELO. UNÂNIME.

Entre outros exemplos de golpes como os já citados ?phishing?, ?vishing? e ?smishing? que buscam a obtenção de vantagem ilícita frente as vítimas, muitas vezes fazendo uso de um terceiro como ponte para alçar seu objetivo fraudulento, ocorre que, como mencionado, mesmo esse terceiro não tendo o dolo na prática do crime deve garantir a segurança e impermeabilidade do seu sistema para que isso não ocorra, contando com a obrigação de assegurar os direitos do consumidor e usuário.
Este é o entendimento das jurisprudências pátrias:
RECURSO INOMINADO. AÇÃO DECLARATÓRIA DE INEXISTÊNCIA DE DÉBITO C/C INDENIZAÇÃO POR DANOS MORAIS. PRELIMINAR DE VIOLAÇÃO AO PRINCÍPIO DA DIALETICDADE. INOCORRÊNCIA. BANCÁRIO. TRANSFERÊNCIA DE VALORES REALIZADA POR TERCEIRO. FRAUDE EVIDENCIADA. CULPA DA VÍTIMA NÃO CONFIGURADA. INSTITUIÇÃO FINANCEIRA QUE NÃO APRESENTOU PROVAS ACERCA DA SEGURANÇA, AUTENTICAÇÃO OU IDENTIFICAÇÃO DA OPERAÇÃO. FALHA NA PRESTAÇÃO DO SERVIÇO CONFIGURADA. RESPONSABILIDADE OBJETIVA DO BANCO. APLICAÇÃO DA SÚMULA 479 DO STJ. RESTITUIÇÃO DEVIDA. AUSÊNCIA DE SOLUÇÃO ADMINISTRATIVA. DANO MORAL CONFIGURADO NO CASO CONCRETO. QUANTUM ARBITRADO EM R$ 2.000,00 (DOIS MIL REAIS) QUE COMPORTA MAJORAÇÃO PARA R$ 3.000,00 (TRÊS MIL REAIS). OBSERVÂNCIA AOS PRINCÍPIOS DA PROPORCIONALIDADE E RAZOABILIDADE. SENTENÇA PARCIALMENTE REFORMADA. Recurso da autora conhecido e provido.Recurso do réu conhecido e desprovido. (TJPR - 1ª Turma Recursal - 0003317-67.2020.8.16.0136 - Pitanga - Rel.: JUIZ DE DIREITO DA TURMA RECURSAL DOS JUIZADOS ESPECIAIS NESTARIO DA SILVA QUEIROZ - J. 23.05.2022)
(TJ-PR - RI: 00033176720208160136 Pitanga 0003317-67.2020.8.16.0136 (Acórdão), Relator: Nestario da Silva Queiroz, Data de Julgamento: 23/05/2022, 1ª Turma Recursal, Data de Publicação: 23/05/2022)

Ressalta-se que o estelionato na sua modalidade digital é considerado crime de ação penal pública incondicionada, ou seja, a responsabilidade para conduzir o procedimento é do Ministério Público, independente de manifestação de vontade da vítima, a natureza dessa ação ressalva a relevância de tratar esse delito de forma mais eficaz, independente da vontade da vítima de ver o autor do crime responsabilizado, com o fito de preservar a ordem social e diminuir o índice de novos casos.
13

Nesse sentido, cumpre destacar que mesmo a responsabilidade do crime ser direta em relação ao Autor, também pode abranger mais partes do processo dependendo da especificada do caso. A jurisprudência entende que a responsabilidade não é apenas do Estado, mas também da empresa, entidade ou

qualquer terceiro que tenha a obrigação de tornar o ambiente digital seguro para o usuário.

3.1 CONCEPÇÃO DAS NORMAS JURÍDICAS ATUALIZADAS E FORMAS DE PUNIÇÃO DO CRIME DO ESTELIONATO DIGITAL.

Como já explicitado, um grande fator que desencadeou o aumento da efetivação do crime em questão foi a pandemia, de modo que, com o advento do Covid-19, foi necessário que a população se protegesse em suas casas para corroborar com o distanciamento social e assim evitar a proliferação do vírus, ocorre que em contrapartida a isso foi destaque a aproximação online dos usuários que culminou em oportunidade para os criminosos inovarem suas artimanhas, contando com a suposta sensação de anonimato.
O crime de estelionato digital, no sistema jurídico atual do Brasil, é apreciado no âmbito do Direito Penal, o qual pressupõe responsabilização para esse tipo de ato, que era equiparado ao crime de estelionato, previsto no artigo 171 do Código Penal.
A Lei 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann, entrou em vigor como uma tentativa inicial de tipificar a conduta dos crimes na modalidade virtual para proteção dos dados pessoais da população em face aos criminosos virtuais, ocorre que com o passar dos anos se mostrou necessária a inclusão de novas medidas frente a progressão da criminalidade no país, em específico os crimes virtuais.
Para combater essa crescente negativa no âmbito jurídico nacional entrou em vigor a lei 14.155/21, de 27 de maio de 2021, que incluiu e modificou alguns parágrafos no supramencionado dispositivo legal, alterando algumas regras para julgar o crime.

Art. 1º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar com as seguintes alterações:
?Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
14

§ 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.
§ 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso:
I ? 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;
II ? Aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra

idoso ou vulnerável. Pena ? reclusão, de 1 (um) a 4 (quatro) anos, e multa.
§ 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. Pena ? reclusão, de 2 (dois) a 5 (cinco) anos, e multa.

Dentre as alterações, foram incluídos os § § 2º-A e 2º-B, que tratam de fraude eletrônica, sendo o § 2º-A qualificadora para o crime de estelionato que não é praticado na modalidade presencial, ou seja, quando a frade é cometida com uso de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de reses sociais ou qualquer outro meio fraudulento análogo.

Fraude eletrônica
§ 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.
§ 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.
Estelionato contra idoso ou vulnerável
§ 4º A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso.
Art. 2º O art. 70 do Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), passa a vigorar acrescido do seguinte § 4º:
§ 4º Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção.? (NR).

Nesse sentido, observa-se que foram elencados os crimes específicos mediante fraude eletrônica objetivando tornar mais rigorosa a lei, ainda tentando acompanhar o avanço da criminalidade. Frisa-se que a Lei 14.155/21 deu ênfase também ao aumento da pena para esse crime na modalidade virtual, com pena de reclusão de 4 a 8 anos e o aumento de 1/3 ao dobro da pena acaso o crime seja praticado contra idoso ou vulnerável, com expectativa para prejudicar a prática delituosa.
15

Cabe destacar também a alteração quanto a competência para apuração do

estelionato por fraude mediante cheque ou transferência bancária, o código de processo penal previa que a competência era do local do banco sacado, o que muitas vezes dificultava a apuração do crime, até pela localização da vítima que nem sempre residia no mesmo local do banco sacado, competência esta alterada para o domicílio da vítima pela Lei 14.155/21.
Por fim, a execução da lei e a responsabilização dos golpistas submete-se a conduta das autoridades capazes, para investigar, processar e julgar os casos de estelionato digital, como a polícia e o poder judiciário.

4 O HISTÓRICO DA PRÁTICA DO ESTELIONATO DIGITAL E OS REFLEXOS DA LEI 14.155 FRENTE A VULNERABILIDADE DA VÍTIMA.

Como já demonstrado, o estelionato digital foi uma modalidade que cresceu esporadicamente com o advento da internet e o constante avanço da tecnologia, mas também teve um de seus marcos recentemente, em 2020, com crescimento exponencial pela pandemia da covid 19 que possibilitou mais ?vítimas? online.
Relativizando em números, o país registrou um aumento ainda mais expressivo que o estelionato comum quando em sua modalidade virtual, com direta relação a pandemia, em 2021 houve 120.470 (cento e cinto mil, quatrocentos e setenta) casos registrados, já em 2022 foram registrados 200.322 (duzentos mil, trezentos e vinte e dois) casos, um aumento de 66,2% (sessenta e seis virgula dois por cento) de acordo com os dados do Fórum Brasileiro de Segurança Pública (FBSP).
Foram registrados em 2021 115 (cento e quinze) estelionatos a cada 100 (cem) mil habitantes no país, já no ano seguinte foram registrados 189,9 (cento e oitenta e nove virgula nove), um aumento de 65,1% (sessenta e cinco vírgula um porcento), ainda de acordo com a FBSP o estado que detém o recorde de casos registrados de estelionato em sua modalidade digital é Santa Catarina, com 64.230 (sessenta e quatro mil, duzentos e trinta) registros em 2022 o que representa 32% (trinta e dois porcento) dos casos do país, ressalvando que Bahia, Ceará, Rio de Janeiro, Rio Grande do Norte, Rio Grande do Sul e São Paulo não tinham ou não disponibilizaram dados.
Cabe destacar que, além de Santa Catarina, tiveram relevantes aumentos Minas Gerais que passou de 25.574 (vinte e cinco mil, quinhentos e setenta e quatro)
16

casos em 2021 para 35.749 (trinta e cinco mil, setecentos e quarenta e nove) em 2022, um aumento de 49,4% (quarenta e nove vírgula quatro porcento), Distrito Federal que passou de 10.049 (dez mil e quarenta e nove) casos em 2021 para 15.580 (quinze mil, quinhentos e oitenta) em 2022, registrando um aumento de 55% (cinquenta e cinco porcento), e o Espírito Santo que passou de 10.545 (dez mil, quinhentos e quarenta e cinco) casos em 2021 para 15.277 (quinze mil, duzentos e setenta e sete) casos em 2022, o que resultou em um aumento de 44,8% (quarenta e quatro vírgula oito por cento).
Dentre todos esses dados disponibilizados pela FBSP cabe destacar por fim os

Estados que mais sofreram variações em seus índices, quais sejam Roraima que passou de 59 (cinquenta e nove) casos em 2021 para absurdos 759 (setecentos e cinquenta e nove) em 2022 acarretando um aumento de 1.186% (mil, cento e oitenta e seis por cento) e Goiás com um aumento de 1.041% (mil e quarenta e um porcento), passando de 128 (cento e vinte e oito) casos em 2021 para 1.461 (mil, quatrocentos e sessenta e um) casos em 2022.
Ainda sobre o marco recente que corroborou com a prática do referido delito é reiterado pelo Fórum Brasileiro de Segurança Pública (FBSP) que:

A digitalização das finanças, de serviço e do comércio, especialmente impulsionada durante o período pandêmico, contribui com a formação de um ambiente propício ao desenvolvimento de modalidades criminais que exploram vulnerabilidade nestes segmentos. (FBSP 2022, p. 6).

Conforme já citado, a modalidade de estelionato digital foi inserida ao Código Penal em meados de 2021 pela Lei nº 14.155/21 que também especificou o estelionato praticado na modalidade digital, por meio cibernético. Essa lei trouxe novidades legislativas que no geral foram positivas com relação a vulnerabilidade da vítima.
Destarte podemos citar que invadir dispositivo informático de uso alheio, ressalvando que conectado ou não a internet, com o fim de obter vantagem ilícita terá pena de reclusão de 4 (quatro) a 8 (oito) anos e multa, com suas devidas especificações, demonstrando assim a preocupação do legislador com as vítimas que infelizmente só estavam crescendo no país e isso refletiu no agravamento da pena que antigamente era disposta no crime de invasão de dispositivo informático, criando uma resistência ao criminoso na medida em que vê o crime como algo mais grave, mediante nova pena mais severa.
17

Ainda quanto aos reflexos dessa lei frente a vulnerabilidade da vítima podem-se listar os agravantes trazidos em sua redação quanto ao furto, com pena de reclusão de 4 a 8 anos, para o crime nessa modalidade realizado com o uso de dispositivos eletrônicos, conectados ou não a internet, por meio de uso de sistemas invasores ou violação de senha, além do agravamento se praticado contra idosos ou vulnerável com consequente aumento de pena de 1/3 ao dobro, ainda na hipótese de ser praticado por servidor fora do território nacional aumenta a pena de 1/3 (um terço) a 2/3 (dois terços).
Quanto ao estelionato também tornou-se agravante o furto qualificado no âmbito cibernético, com igual pena de reclusão de 4 (quatro) a 8 (oito) anos, além de possível multa e pode ter pena aumentada de 1/3 (um terço) a 2/3 (dois terços) acaso seja praticada por servidor fora do território nacional e acaso praticada contra idoso ou vulnerável poderá ter a pena aumentada de 1/3 (um terço) ao dobro.
Por fim, no que tange a invasão de aparelhos para obtenção de dados, a lei passou de detenção de 3 (três) meses a 1 (um) ano para reclusão de 1 (um) a 4

(quatro) anos. Ainda na hipótese de resultar em obtenção de informações sigilosos pode ser majorada de reclusão de 2 (dois) a 5 (cinco) anos e multa, com agravante de 1/3 (um terço) a 2/3 (dois terços) caso ocorra prejuízo econômico decorrente da invasão.
Assim, as novidades legislativas trazidas pela lei confortam brasileiros que podem ser vítimas de criminosos fora do território nacional, o que é plenamente possível pelo advento da internet e também a população mais velha que, em suma maioria, não tem familiaridade com as ferramentas e linguagens online, não tendo manejo e trato com os meios digitais o que por muitas vezes os torna os principiais focos dos criminosos pela ?facilidade? e ?inocência? desses usuários em específico, assim como os vulneráveis.
Portanto, resta claro que o legislador buscou efetivamente ampliar a guarda dos direitos, de modo a, buscar uma equidade entre diversos grupos de pessoas/possíveis vítimas, resultando em maior segurança, de modo que passa a observar significativas mudanças objetificando proteger os direitos do usuário e penalizando de forma mais grave os criminosos.

5 CONCLUSÃO.

18

O presente artigo, por meio da análise de dados estatísticos, legislação e julgados, buscou tecer uma análise crítica da disciplina normativa do estelionato digital, suas formas de conduta e as possíveis consequências sociais.
Demonstrando que a sociedade está cada vez mais conectada e as redes sociais têm uma função muito importante nessa interação, ocorre que o aumento desenfreado de pessoas conectadas à internet propiciou um ambiente para prática de crimes e com diversas possibilidades de artimanhas dos criminosos, que enxergam a internet como ?terra sem lei?, para obtenção da vantagem ilícita virtualmente, caracterizando o estelionato digital.
Dentre as diversas artimanhas utilizadas pelos estelionatários destacarm-se o ?phishing?, utilizada para enganar os usuários e conseguir informações privadas, ?vishing? popularmente conhecido por ?phishing por voz? quando o ato é realizado por ligações ou envio de áudios com o mesmo intuito de ludibriar a vítima, mas para divulgar dados pessoais e ?smishing? modalidade em que a vítima é provocada a acessar link que corrompe seu aparelho, além de outros golpes como investimentos fraudulentos, promessas de retornos financeiros utopicamente elevados e esquema de pirâmides, esses golpistas beneficiam-se da leiguice de suas vítimas no âmbito de investimento financeiro com falsas promessas de enriquecimento acelerado para enganá-las.
Assim, restou demonstrado que os golpistas tem o mesmo fito, qual seja a obtenção da vantagem ilícita fazendo uso do ambiente cibernético, enquadrando-os no âmbito de estelionatários digitais.
Nesta senda, ainda não existia um enquadramento específico para conter o

avanço do referido ilícito que muitas vezes poderia ser caracterizado como tentativa de extorsão ou crimes análogos o que obrigou o poder legislativo a se atualizar. Para ?frear? o avanço do crime foi introduzida a Lei 12.737/2012, popularmente conhecida por ?Lei Carolina Dieckmann?, que surgiu após um incidente em que a atriz teve seu aparelho pessoal invadido e com isso o vazamento de fotos íntimas na rede.
A introdução da Lei ?Carolina Dieckmann? mostrou-se muito importante por iniciar a caminhada rumo a tipificada do crime de estelionato em sua modalidade digital, ocorre que a tecnologia seguiu se modernizando trazendo novas oportunidades para inovação dos criminosos que vivem as sombras da internet. Com o estabelecimento de modalidades de transferência eletrônica como ?TED? e ?PIX?
19

tornou-se cada vez mais comum o embate entre as autoridades e os golpistas, já demonstrando a necessidade de nova atualização da legislação atinente ao tema.
Quanto a responsabilidade do crime no âmbito jurídico restou pacificado pelas jurisprudências pátrias que torna-se direta em relação ao Autor, sendo aferida pelo Estado que tem o dever de tutelar a convivência no âmbito cibernético. Cumpre destacar que nem sempre a responsabilidade é exclusiva do Autor, podendo recair de forma subjetiva ou objetiva para um terceiro da relação que deveria zelar pela segurança dos dados pessoais do usuário, tais como bancos, tomadores de serviço...
O marco de crescimento registrado no crime de estelionato na sua modalidade virtual foi durante a pandemia de covid 19, época em que foi necessário a reclusão da população em casa o que gerou aumento exponencial de usuários online na rede e, em paralelo, oportunidade para os criminosos inovarem suas artimanhas.
Para combater essa crescente negativa no âmbito jurídico nacional entrou em vigor a lei 14.155/21, de 27 de maio de 2021 trazendo enrijecimento das penas e tipificação de novos crimes, como estelionato contra idoso ou vulnerável e fraude eletrônica, intentando ainda em penas mais rigorosas que podem ser alongadas a depender do caso e alteração de competência para estelionato por fraude mediante cheque ou transferência bancária, submetendo a execução da lei e responsabilização dos golpistas a conduta das autoridades capazes.
O que se conclui é que, com o passar dos anos as leis e medidas tomadas se tornam ultrapassadas vide o ?aperfeiçoamento? dos criminosos, portanto, com o fito do controle do Estado se tornar uma manutenção mais célere se mostrou necessário inserção de um sistema de inovação e renovação legislativa.
Ora, restou comprovado que o âmbito jurídico sempre buscou acompanhar a inovação criminosa trazendo atualizações a legislação para coibir a progressão desses ataques criminosos, mas igualmente restou comprovado que apenas acompanhar não está mais sendo o suficiente, tornando tendência o adiantamento aos movimentos da marginalidade com sucessivo progresso de imersão tecnológica das autoridades para se adiantar ao crime com a devida manutenção das leis de forma mais célere objetivando deter o claro avanço da criminalidade hodierna.

REFERÊNCIAS

20

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez.

BRASIL, DECRETO-LEI NO 2.848, DE 7 DE DEZEMBRO DE 1940. Código Penal. Rio de Janeiro, 7 de dezembro de 1940; 119º da Independência e 52º da República. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 08/06/2023.

BRASIL. LEI Nº 14.155, DE 27 DE MAIO DE 2021. Lei de Invasão a Dispositivo Informático [Internet]. Disponível em: https://www.in.gov.br/en/web/dou/-/lei-n-14.155-de-27-de-maio-de-2021-322698993. Acesso em: 24 nov. 2023

BRASIL. LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012. Lei de Invasão a Dispositivo Informático [Internet]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em:
24 nov. 2023.

BRASIL. LEI Nº 14.155, DE 27 DE MAIO DE 2021. Lei de Invasão a Dispositivo Informático [Internet]. Disponível em: https://www.in.gov.br/en/web/dou/-/lei-nº 14.155-de-27-de-maio-de-2021-322698993. Acesso em: 13 dez. 2023.

BRASIL. Tribunal de Justiça do Paraná. TJ-PR - Recurso Inominado XXXXX-67.2020.8.16.0136 PR. Relator Nestario da Silva Queiroz. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-pr/1511018743. Acesso em: 25 nov. 2023

BRASIL. Tribunal de Justiça do Rio Grande do Sul. TJ-RS - Apelação Cível XXXXX-22.2020.8.21.7000 RS. Relator Giovanni Conti. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-rs/932015329. Acesso em: 25 nov. 2023

BRITO, Auriney. Direito penal informático. São Paulo: Saraiva, 2013, p.189.

CAMPOS, Pedro Franco de [et al.]. Direito penal aplicado: parte geral e parte especial do Código Penal. - 6ª. Ed. ? São Paulo: Saraiva, 2016.

CASSANTI, Moisés de Oliveira. Crimes virtuais, vítimas reais. 1ª ed. Rio de Janeiro: Brasport, 2014, p.6.

CHAVES, Fábio Barbosa; TEIXEIRA, Filipe Silva. Os crimes de fraude e estelionato cibernético e a proteção do consumidor no e-commerce. 2020. Disponível em: <https://conteudojuridico.com.br>. Acesso em: 12/06/2023.

COELHO, Yuri Carneiro. Curso de Direito Penal Didático. vol. único, 2ª ed. ? São Paulo: Atlas, 2015.

CÔRREA, Gustavo Testa. Aspectos jurídicos da internet. 5. ed. rev. e atual. São Paulo, Saraiva, 2010.

CUNHA, Rogério Sanches. Manual de direito penal: parte especial (arts. 121 ao 361). 11. ed. rev., ampl. e atual. Salvador: JusPODIVM, 2019.
21

CUNHA, Rogério Sanches. Lei 14.155/21 e os crimes de fraude digital - primeiras impressões e reflexos no CP e no CPP. Meu Site Jurídico (JusPodivm), 2021. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2021/05/28/lei-14-15521-e-os-crimes-de-fraude-digital-primeiras-impressoes-e-reflexos-no-cp-e-no-cpp/. Acesso em: 13 dez. 2023.

FBSP. Fórum Brasileiro de Segurança Pública. Os crimes patrimoniais no Brasil: entre novas e velhas dinâmicas. Anuário Brasileiro de Segurança Pública, 2022. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2022/07/07-anuario-2022-os-crimes-patrimoniais-no-brasil-entre-novas-e-velhas-dinamicas.pdf. Acesso em 24 nov. 2023.

GENNARINI, Juliana. Revista de Direito Penal e Processo Penal, ISSN 2674-6093, v. 2, n. 2, jul./dez. 2020.

GONÇALVES, Victor Eduardo Rios. Direito penal esquematizado: parte especial do Código Penal. - 8. ed. ? São Paulo: Saraiva Educação, 2018.
GRECO, Rogério. Curso de Direito Penal: parte especial. v. III. 7. ed. Rio de Janeiro: Ed. Impetus, 2010.

GOUSSINSKY, Eugenio. Crimes digitais têm forte alta em vários estados; saiba como prevenir. Portal R7, 2021. Disponível em: https://noticias.r7.com/tecnologia-e-ciencia/crimes-digitais-tem-forte-alta-em-varios-estados-saiba-como-prevenir-05052021. Acesso em: 12 dez. 2023.

GRECO, Rogério. Curso de Direito Penal: parte especial. v. III. 7. ed. Rio de Janeiro: Ed. Impetus, 2010, p. 228.

HUNGRIA, Nelson. Comentários ao Código Penal ? Vol. IX. Rio de Janeiro: Forense, 1958.

MIRABETE, Júlio Fabbrini e FABBRINI, Renato N./ Manual de direito penal: parte

especial: arts. 121 a 234-B do CP ? volume 2, 36° edição, São Paulo, Atlas, 2021.

ESTELIONATO DIGITAL: UMA ANÁLISE CRÍTICA DA DISCIPLINA NORMATIVA, SUAS FORMAS DE CONDUTA E AS POSSÍVEIS CONSEQUÊNCIAS SOCIAIS

Rafael Lemos Garcia de Oliveira1
Ricardo Simões Xavier dos Santos2

Resumo
O presente artigo discorre sobre a figura do estelionato digital, fazendo uma análise crítica da disciplina normativa, suas formas de conduta e as possíveis consequências sociais. É notório que a atual legislação do país tem avançado, conforme mencionado, na forma que tipifica os crimes que ocorrem em meios virtuais, todavia as sanções ainda são moderadas e as normas devem avançar no sentido de impedir a prática dos crimes virtuais. Para que seja viável a hipótese narrada, o Estado tem o dever de incrementar métodos novos de apuração e averiguação e aprimorar os recursos tecnológicos e digitais que estão à disposição das autoridades responsáveis. Nesse sentido, é necessário compreender o que é o estelionato digital, suas características, maneiras de prevenção e formas em que pode aparecer no dia a dia dos usuários da rede, compactuando com a legislação penal e o cabimento de penalização para os criminosos que praticam esse crime. Por fim, conclui-se que a legislação penal brasileira vem evoluindo, mas para que alcance um nível suficiente de eficácia no combate a esse crime é necessário compreender o que é o estelionato digital, suas características, maneiras de prevenção e formas em que pode aparecer no dia a dia dos usuários da rede, compactuando com a legislação penal e o cabimento de penalização para os criminosos que praticam esse crime.

PALAVRAS-CHAVE: Internet. Crime Cibernético. Estelionato Digital. Código Penal.

1 Graduando em bacharelado em direito pela UCSAL. E-mail: rafaell.oliveira@ucsal.edu.br
2 Doutor em Políticas Sociais e Cidadania pela Universidade Católica do Salvador ? UCSal. E-mail:

ricardo.santos@pro.ucsal.br
2

ABSTRACT: This article discusses the figure of digital fraud, making a critical analysis of the normative discipline, its forms of conduct and the possible social consequences. It is notable that the country's current legislation has advanced, as mentioned, in the way it typifies crimes that occur in virtual media, however sanctions are still moderate and standards must advance in order to prevent the practice of virtual crimes. In order for the narrated hypothesis to be viable, the State has the duty to increase new methods of investigation and investigation and improve the technological and digital resources that are available to the responsible authorities. In this sense, it is necessary to understand what digital fraud is, its characteristics, methods of prevention and ways in which it can appear in the daily lives of network users, in agreement with criminal legislation and the appropriateness of penalizing criminals who practice this crime. Finally, it is concluded that Brazilian criminal legislation has been evolving, but in order to achieve a sufficient level of effectiveness in combating this crime, it is necessary to understand what digital fraud is, its characteristics, methods of prevention and forms in which it can appear. in the daily lives of network users, complying with criminal legislation and the appropriateness of penalizing criminals who commit this crime.

KEYWORDS: Internet. Cybercrime. Digital Fraud. Penal Code.

SUMÁRIO: 1 INTRODUÇÃO. 2 CONDUTA DO ESTELIONATO DIGITAL: CONCEITOS PRÉVIOS, DISCUSSÕES INICIAIS E FORMAS APRESENTADAS. 2.1 Análise acerca das eventuais consequências sociais advindas da conduta do estelionato digital 3 A RESPONSABILIZAÇÃO DO CRIME DE ESTELIONATO DIGITAL NO ÂMBITO JURÍDICO 3.1 Concepção das normas jurídicas atualizadas e formas de punição do crime do estelionato digital 4 O HISTÓRICO DA PRÁTICA DO ESTELIONATO DIGITAL E OS REFLEXOS DA LEI 14.155 FRENTE A VULNERABILIDADE DA VÍTIMA 5 CONCLUSÃO 6 REFERÊNCIAS

1 INTRODUÇÃO

No âmbito penalista são diversos os crimes que têm como objetivo a obtenção de lucros financeiros da vítima, o referido trabalho tem como objetivo abordar o estelionato digital fazendo uma análise crítica da disciplina normativa, apresentando suas formas de conduta e relacionando a suas possíveis consequências sociais.
3

Há uma previsão legal do Código Penal em garantir que todos os cidadãos lesados por práticas de golpes, em que são utilizados artifícios ou qualquer meio fraudulento, podem ingressar no juízo criminal a fim de prosseguirem com a punição penal e com o ressarcimento dos prejuízos.
Para breve introito, o estelionato é 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.
Dentre os crimes mais comuns no Brasil e no mundo pode-se destacar o estelionato, além do meio físico os criminosos procuram pela navegação na rede com o fito de obtenção de dados e informações das pessoas que tem perfil para serem suas possíveis vítimas, pondo em prática das mais diversas maneiras tais como ligações, mensagens, falsificação de identidade, haja vista que todos os dias, a população vive a internet, cadastrando senhas, trocando mensagens, adentrando redes sociais, fazendo negócios pela internet...
Nesse sentido, acompanhando o aumento dos usuários das redes a realização de crimes online cresceu consideravelmente, obviamente relacionado a simplicidade de manejo dos meios virtuais e pela dificuldade de identificação dos criminosos para posterior punição, haja vista ausência de legislações específicas e supressão das identidades.
A realização de golpes e fraudes cometendo ilícitos para obter vantagem sob outras pessoas é prática recorrente e por muitas vezes impune no Brasil, com o estelionato digital não é diferente.
Em sua esfera digital ele se configura quando o criminoso submete o aparelho da vítima e sincroniza-o a demais sistemas de informação ou, em outra hipótese, quando a vítima é posta em uma conjuntura de sensibilidade para obtenção de vantagem ilícita. Na atualidade é mais comum do que se imagina conhecer alguém que tenha passado por essa situação e caído nesse golpe, desde ligações de números sem chamador ou desconhecidos a e-mails/mensagens com ofertas incríveis.
Outro ponto importante que contribuiu para esse aumento, além da facilidade no manejo dos meios virtuais foi o advento da pandemia do Covid-19, as práticas desses crimes se multiplicaram, haja vista que, relevante porcentagem da população tanto brasileira quanto mundial, se viu obrigada a passar mais tempo em casa, o que, em consequência, ampliou o número de pessoas online, acessando a rede. Neste liame, os criminosos têm agido cada vez mais e feito várias vítimas no mundo virtual.
4

Para que o crime possa ser classificado como estelionato digital é imprescindível que a entrega das informações pela vítima seja de forma voluntária, haja vista que a obtenção dos dados se deu por outros meios, o crime pode ter outra classificação, tal como ?furto mediante fraude eletrônica?.
Dentre as principais vítimas desse crime tão comum na atualidade estão as pessoas desatentas e que não tomam total atenção para se esquivar dos estelionatários, seguindo as hipóteses de compra e venda pela internet não verificando a fonte, se é de confiança etc., links enviados de números aleatórios possibilitando o acesso do criminoso a rede da vítima entre outros...
A despeito da clara regulação e evolução da internet e redes sociais, os conselhos e observações para a premeditação dos crimes digitais em geral continua sendo de cuidado e cautela com os dados pessoais e sua divulgação, ainda com o remetente e usuários/links que adentra. É necessário que sempre pense que tudo que

identifique quem você é ou que busque saber informações que só você teria acesso são o alerta inicial para entender se não se está diante de uma possível tentativa de estelionato digital.
É notório que a atual legislação do país tem avançado, conforme mencionado, na forma que tipifica os crimes que ocorrem em meios virtuais, todavia as sanções ainda são moderadas e as normas devem avançar no sentido de impedir a prática dos crimes virtuais. Para que seja viável a hipótese narrada, o Estado tem o dever de incrementar métodos novos de apuração e averiguação e aprimorar os recursos tecnológicos e digitais que estão à disposição das autoridades responsáveis.
Nesse sentido, é necessário compreender o que é o estelionato digital, suas características, maneiras de prevenção e formas em que pode aparecer no dia a dia dos usuários da rede, compactuando com a legislação penal e o cabimento de penalização para os criminosos que praticam esse crime.
Assim, as perguntas que ficam são quais as formas de conduta do estelionato digital e seus impactos na sociedade, além do questionamento acerca das normas brasileiras, nosso sistema jurídico atual contempla qual espécie de responsabilização para o crime de estelionato digital, alinhado a isso, como o Estado Democrático Brasileiro pode melhorar para combater o aumento desse crime.
No presente artigo, seguindo após a introdução para o capítulo ?2? onde serão apresentadas as condutas do estelionato digital, seus conceitos prévios e formas apresentadas, a diferença entre o estelionato e outros crimes contra o patrimônio e
5

sua forma de proliferação pela rede mediante sites falsos, mensagens e e-mails. O capítulo ?2? contém ainda um subtópico ?2.1? onde serão analisadas as consequências sociais advindas da conduta do estelionato digital, desde a inovação dos criminosos partindo para o meio digital até os ?traumas? das vítimas e sua repercussão na sociedade.
Já no capítulo ?3? será amplamente explicada a quem deve ser dirigida a responsabilidade pelo crime do estelionato digital, no âmbito jurídico, já que o crime na grande maioria das vezes tem por conclusão a ?fuga? do criminoso pelo meio cibernético. Ainda no capítulo ?3? serão exploradas, mediante subtópico ?3.1?, as normas jurídicas atualizadas e formas de punição do crime tendo relação direta com a ampla possibilidade de escape do criminoso.
Por fim, em capítulo ?4?, será demonstrado o histórico da prática do estelionato digital, sua evolução paralela ao avanço da tecnologia na sociedade e os reflexos da Lei 14.155, instituída em 2021 especialmente para tornar mais grave a pena de estelionato cometido de forma eletrônica pela internet, frente ainda a vulnerabilidade da vítima. Seguidos da conclusão e as referências bibliográficas.
De certo, cumpre-se destacar que a pesquisa em questão, valeu-se do método da revisão bibliográfica de trabalhos científicos atualizados das áreas penal e constitucional, frente às questões sociais, publicadas em periódicos nacionais e internacionais, qualificados como publicações de A1, assim como B1. Além de importantes nomes do cenário retrato, ao passo que se cita Rogério Greco e Fabio

Barbosa Chavez, bem como análise jurisprudencial e legislativa da lei 14.155.
Compreende-se então, que a escolha metodológica se justifica de base teórica, fundada em estudos atualizados sobre o estelionato digital, suas formas de conduta e as consequências sociais.
O foco da pesquisa bibliográfica foi de apresentar informações e dados específicos sobre a evolução dos crimes digitais, exibindo o progresso do direito penal frente os crimes digitais, através da análise filosófica e de referenciais teóricos de artigos, códigos e outros trabalhos sobre a mesma questão jurídica. Assim, o método empregado é de leitura e análise de material doutrinário especializado já existente sobre o tema de Direito Penal, tal como de jurisprudência, dados, legislação e artigos científicos.

6

2 CONDUTA DO ESTELIONATO DIGITAL: CONCEITOS PRÉVIOS, DISCUSSÕES INICIAIS E FORMAS APRESENTADAS.

O termo estelionato está disposta no Art. 171 do Código Penal como:

Art. 171. Obter, para si ou para outrem, vantagem ilícita em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: pena ? Reclusão, de 1 (um) a 5 (cinco) anos, de multa.

Trata-se de crime contra o patrimônio onde a legislação penal visa proteger a inviolabilidade patrimonial orientada pela prática de atos que visam enganar a vítima e beneficiar o agente (CUNHA, 2019, p. 345).
Assim, pode-se inferir que a diferença entre o estelionato e os diversos crimes contra o patrimônio, ou seja, crimes que tenham por objetivo atentar contra o patrimônio de uma pessoa ou organização, é que no estelionato não é utilizada a força para obtenção de ?vantagem?. É sabido, portanto, que essa atitude é conhecida há muitos anos, de modo que Greco cita que:

Desde que surgiram as relações sociais, o homem se vale da fraude para dissimular seus verdadeiros sentimentos e intenções para, de alguma forma, ocultar ou falsear a verdade, a fim de obter vantagens que, em tese, lhe seriam indevidas (GRECO, 2019, p. 228).

Ressalta-se que o crime existe apenas na modalidade dolosa, sem previsão na forma culposa.
A respeito da expressão ?vantagem ilícita?, Fernando Capez (2020) ensina que, esta, trata-se do objeto material do crime e, caso o agente esteja agindo em razão de uma vantagem devida, a conduta é tipificada como exercício arbitrário das próprias razões, delito previsto no art. 345, do Código Penal.
De acordo com o que se retira do artigo 171, do supramencionado dispositivo

legal, o estelionato pode ser cometido mediante artificio, ardil ou qualquer outro meio fraudulento. Em relação ao termo ?artificio?, o doutrinador Júlio Fabbrini Mirabete ensina o seguinte:

?o artifício existe quando o agente se utilizar de um aparato que modifica, ao menos aparentemente, o aspecto material da coisa, figurando entre esses meios o documento falso ou outra falsificação qualquer, o disfarce, a modificação por aparelhos mecânicos ou elétricos, filmes, efeitos de luz etc.? (MIRABETE, 2021, pag. 325).

Em sua modalidade digital o estelionato ocorre através de sites falsos, mensagens e até e-mail, sendo prioritariamente focado no âmbito virtual. É bastante
7

normal que o consumidor busque virtualmente os mesmos bens desejados fisicamente, mas com a comodidade de não se deslocar e em grande maioria dos casos a acessibilidade com preços menores, levando a promessa da oferta muitas vezes a encantar o consumidor que não percebe a fraude.
Dentre as formas de conduta do referido crime podem ser listadas as mais comuns sendo: vendas falsas em sua maioria quando os estelionatários oferecem serviços ou produtos inexistentes em redes sociais e/ou sites e links de comércio eletrônico; ?phishing?, uma artimanha utilizada pelos criminosos para enganar os usuários e conseguir informações privadas, tais como senhas, detalhes de cartões de crédito, comumente realizado por meio do envio de mensagens eletrônicas se passando por instituições de confiança, pode ser realizado por sites e por redes sociais também, mas sempre com o intuito de prejudicar e obter vantagem, ?vishing? popularmente conhecido por ?phishing por voz? quando o ato é realizado por ligações ou envio de áudios com o mesmo intuito de ludibriar a vítima, mas para divulgar dados pessoais, ?smishing? realizada também por mensagem, mas nessa modalidade a vítima é provocada a acessar link que corrompe seu aparelho, e por último os golpes de investimentos fraudulentos que podem acontecer de diversas maneiras, tais como promessas de retornos financeiros utopicamente elevados e esquema de pirâmides, esses golpistas beneficiam-se da leiguice de suas vítimas no âmbito de investimento financeiro com falsas promessas de enriquecimento acelerado para enganá-las.
No Art. 171 do Código Penal, o estelionato possui a pena de reclusão de 1 a 5 anos e multa. Diante disso, o crime admite suspensão condicional no processo de acordo com o art. 89, § 1ª, da Lei dos Juizados Especiais - Lei n. 9099/95:

Art. 89. Nos crimes em que a pena mínima cominada for igual ou inferior a um ano, abrangidas ou não por esta Lei, o Ministério Público, ao oferecer a denúncia, poderá propor a suspensão do processo, por dois a quatro anos, desde que o acusado não esteja sendo processado ou não tenha sido condenado por outro crime, presentes os demais requisitos que autorizariam a suspensão condicional da pena (art. 77 do Código Penal).

Conforme dito, o crime de estelionato digital, no sistema jurídico atual do Brasil, é apreciado no âmbito do Direito Penal o qual pressupõe responsabilização penal para esse tipo de ato, o qual era equiparado ao crime de estelionato, previsto no artigo 171 do Código Penal, ocorre que ainda no caminhar para a especificação do crime de estelionato na modalidade digital foi introduzida a Lei 12.737/2012, ou como é popularmente conhecida a ?Lei Carolina Dieckmann?, que surgiu após um incidente 8

em que a atriz teve seu aparelho pessoal invadido e com isso o vazamento de fotos íntimas na rede, mediante ainda tentativa de extorsão.
Na época em questão os criminosos seriam apenas denunciados pelo crime de tentativa de extorsão, haja vista ausência de legislação específica quanto aos crimes digitais, assim vários projetos de lei foram analisados para tentar tipificar condutas para crimes semelhantes ao sofrido pela atriz e findada essa fase foi sancionada a Lei 12.737/2012 que entrou em vigor em 02 de abril de 2013.
A lei visava combater o vazamento de informações pessoais dos usuários das redes, zelando pela proteção da privacidade dos mesmos, ainda acrescentou ao Código Penal, mais especificamente no Decreto-Lei 2848, os artigos 154-A e 154-B.

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

A lei se demonstrou efetiva a época da sanção sendo citada como um marco legislativo por muitos autores, desde que entrou em vigor a invasão de computadores, celulares, tablets...no geral dispositivos informáticos alheios passou a ser crime.
Cabe destacar que execução da lei e a responsabilização dos golpistas submete-se a conduta das autoridades capazes, para investigar, processar e julgar os casos de estelionato digital, como a polícia e o Poder Judiciário.

2.1 ANÁLISE ACERCA DAS EVENTUAIS CONSEQUÊNCIAS SOCIAIS ADVINDAS DA CONDUTA DO ESTELIONATO DIGITAL.

A sociedade está cada vez mais conectada e as redes sociais têm uma função muito importante nessa interação, vez que o ser humano sempre precisou de convívio

social. Assim, tais ferramentas estão presentes na vida de muitos brasileiros e esse ambiente digital, como já evidenciado, tornou-se, também, um meio para a prática de crimes, seja pela facilidade de acesso e/ou pelo grande número de usuários.
9

Na atualidade existe uma grande facilidade na obtenção de produtos, sendo de maneira virtual, de modo que não existe mais a necessidade do consumidor se deslocar até o fornecedor para adquirir o produto, nesta feita, é notório que a compra virtual vem amadurecendo cada vez mais, o que consequentemente ocasiona um aumento dos crimes cibernéticos. Nesse contexto, Chaves e Teixeira destacam que:

Com a investigação correta é possível localizar e punir os criminosos que causaram prejuízo a essa nova espécie de consumidores. Todavia, no mesmo ritmo que a internet evolui, os fraudadores também se renovam com novas modalidades de golpes, alguns tão específicos que são até difíceis de definir qual a punição correta a ser aplicada (CHAVES e TEIXEIRA, 2019, p. 119).

Conforme já citado a inovação dos criminosos acompanha em paralelo o avanço da tecnologia pela sociedade, de modo que muitos usuários têm a sensação de que a internet é ?terra sem lei? fomentando sua ?liberdade tecnológica? em pequenos delitos, tais como injúria, difamação... Ao passo em que não imaginam ter a sua responsabilidade realmente comprovada, agindo por trás da tela do celular ou computador.
Perpassando por isso os criminosos buscam a obtenção de vantagem ilícita e veem na internet uma oportunidade recheada de opções, possuídos pela sensação de impunidade e munidos das mais diversas artimanhas para concluir seu objetivo. Cumpre ressaltar que sociedade caminha para um futuro mais tecnológico e os criminosos ?surfam nessa onda?.
A cada dia que passa resta mais rudimentar os métodos de pagamento por cédulas ou moedas, a trajetória da população tem destino eletrônico, de modo que é fato notório o quão comum se tornaram os sistemas de pagamento eletrônico, estando já alguns mais rudimentares como a transferência ?TED?.
A popularização dos sistemas de pagamento eletrônico, a exemplo do ?pix?, propicia diariamente um combate necessário entre as autoridades e os golpistas. Já é rotina na sociedade a divulgação de novos meios de golpes cibernéticos com o fito de alertar os usuários a se precaverem mais, infelizmente nem sempre todo cuidado é tomado e as consequências podem ser desastrosas para os consumidores da rede.
O prejuízo causado a essa nova espécie de consumidores afeta tanto de forma direta as vítimas quanto a sociedade, de maneira geral. Dentre as consequências sociais advindas dessa conduta resta mister destacar o impacto financeiro nas vítimas, de forma direta, que podem encarar perdas financeiras o que acarreta
10

problemas emocionais e instabilidade, perda de confiança no meio digital para compras que também gera impacto na maneira como as pessoas conduzem negócios online.
Além do consumidor direto, as instituições financeiras também sofrem em muitos casos ressarcindo o valor perdido por seus clientes lesados, arcando com o custo de fraude e também no investimento em segurança virtual, mesmo ainda tendo um receio a implantação dos pagamentos digitais buscando ao máximo reforçar sua segurança desde confirmação por ?face id? quanto senhas regularmente trocadas e ?tokens digitais?, sempre tentando confirmar que é realmente o usuário da conta quem realmente está fazendo a operação e não um terceiro. Frisa-se que essas consequências sociais acarretam, num todo, impacto na economia.
Felizmente, não são somente os consumidores que passam pelo processo de consequências negativas, mas também os fraudadores. Mesmo diante da crescente a qual ocorre o ?fenômeno? do estelionato digital, os criminosos não restam imunes a responsabilização pelo seu crime. Conforme será demonstrado no presente artigo, a legislação do país delimita o crime e suas consequências, assim como as penalidades que podem levar os fraudadores a condenação pelas atividades ilícitas.
Nesse sentido, o avanço da tecnologia com o passar dos tempos corroborou indiretamente para que os criminosos inovassem seus meios ilícitos para obtenção de vantagens, causando diversos impactos na sociedade que não teriam como ser positivos, sendo alguns dos principais o prejuízo financeiro as vítimas; perda de confiança na segurança online e transações digitais, além do choque nos sistemas judiciais, de segurança e nas bases digitais o que consequentemente requer mecanismos e investimentos relevantes de atribuição das empresas e do judiciário.
Sendo assim, infere-se que ainda existe certa dificuldade para identificação dos golpistas o que, alternativamente, tem relação com a legislação brasileira que tem avançado na tipificação dos crimes cibernéticos, todavia as sanções ainda são moderadas e as normas devem acompanhar no sentido de bridar a prática desses crimes na modalidade virtual.

3 A RESPONSABILIZAÇÃO DO CRIME DE ESTELIONATO DIGITAL NO ÂMBITO JURÍDICO.

11

É claro que a internet e toda a esfera digital não foi inserida na sociedade com o intuito ou sequer resguarda em relação a possibilidade do advento de crimes em paralelo a isso, mas como toda imprevisão, a criminalidade evoluiu em conjunto deixando cada vez mais vulnerável a segurança dos usuários na rede, como amplamente demonstrado no presente trabalho, os golpes digitais se aperfeiçoam com o passar dos anos, com ênfase para o estelionato que conta hoje com diversos tipos de obtenção de vantagem ilícita na sua modalidade digital.
A internet tornou-se essencial na rotina da população, interligando usuários e pessoas conectadas a rede, assim, como bem destacou Uchoa de Brito:

(...) O problema da internet passou a ser identificado quando a tecnologia incrementou e complicou as relações sociais consideradas, até então, pacíficas e controladas, possibilitando algumas experiências socialmente desagradáveis e indesejadas, como a sua utilização para a prática de crimes, e a criação de novos contatos que colocam em risco bens que ainda não tiveram sua relevância reconhecida pelo Direito. (BRITO, 2013, p. 9).

Assim, a prática do estelionato na modalidade virtual cresceu ao longo dos anos, sempre com a tentativa em paralelo do Direito Penal de acompanhar para poder punir em cerceamento legislativo, com projetos de lei, inovações e acréscimos a legislações já vigentes.
Quanto a responsabilização do crime em questão torna-se direta em relação ao Autor, sendo aferida pelo Estado, mesmo em sua modalidade digital, haja vista que tem o encargo de combater, controlar e reprimir tais práticas tanto no mundo ?real? quanto no ambiente digital, além de ser responsável por tutelar a convivência e atuação neste âmbito cibernético.
Além da responsabilização direta quanto ao autor do delito, muitas vezes a responsabilidade também recai de forma subjetiva ou objetiva para um terceiro da relação que deveria zelar pela segurança dos dados pessoais do usuário, grandes exemplos são os de vazamento de dados bancários online após invasão por hackers, recaindo responsabilidade também para os bancos que deveriam proteger o consumidor.

APELAÇÃO CÍVEL. NEGÓCIOS JURÍDICOS BANCÁRIOS. AÇÃO DE INDENIZAÇÃO POR DANOS MATERIAIS. RESSARCIMENTO DE VALORES. TRANSAÇÃO BANCÁRIA REALIZADA DE FORMA FRAUDULENTA POR TERCEIROS. INTERNET BANKING. RESPONSABILIDADE DO BANCO. SUMULA 479 DO STJ. SENTENÇA MANTIDA. As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias. Súmula 479 do STJ. Art. 14 do CDC. Para
12

responsabilização do prestador de serviços a existência de culpa ou dolo, exige-se apenas a conduta ilícita e a existência de dano, bem como nexo de causalidade entre eles. Caso. Autora que foi vítima de estelionato praticado por terceiro. Empréstimo autorizado pela instituição financeira. Nesse ponto, desimporta que a fraude tenha se perpetrado através dos canais de atendimento via internet (internet banking), porquanto a parte autora negou ter sido a autora dos saques, e o banco não se desincumbiu do ônus de demonstrar a regularidade das transações impugnadas pelo cliente. NEGARAM PROVIMENTO AO APELO. UNÂNIME.

Entre outros exemplos de golpes como os já citados ?phishing?, ?vishing? e ?smishing? que buscam a obtenção de vantagem ilícita frente as vítimas, muitas vezes fazendo uso de um terceiro como ponte para alçar seu objetivo fraudulento, ocorre que, como mencionado, mesmo esse terceiro não tendo o dolo na prática do crime deve garantir a segurança e impermeabilidade do seu sistema para que isso não ocorra, contando com a obrigação de assegurar os direitos do consumidor e usuário. Este é o entendimento das jurisprudências pátrias:
RECURSO INOMINADO. AÇÃO DECLARATÓRIA DE INEXISTÊNCIA DE DÉBITO C/C INDENIZAÇÃO POR DANOS MORAIS. PRELIMINAR DE VIOLAÇÃO AO PRINCÍPIO DA DIALETICDADE. INOCORRÊNCIA. BANCÁRIO. TRANSFERÊNCIA DE VALORES REALIZADA POR TERCEIRO. FRAUDE EVIDENCIADA. CULPA DA VÍTIMA NÃO CONFIGURADA. INSTITUIÇÃO FINANCEIRA QUE NÃO APRESENTOU PROVAS ACERCA DA SEGURANÇA, AUTENTICAÇÃO OU IDENTIFICAÇÃO DA OPERAÇÃO. FALHA NA PRESTAÇÃO DO SERVIÇO CONFIGURADA. RESPONSABILIDADE OBJETIVA DO BANCO. APLICAÇÃO DA SÚMULA 479 DO STJ. RESTITUIÇÃO DEVIDA. AUSÊNCIA DE SOLUÇÃO ADMINISTRATIVA. DANO MORAL CONFIGURADO NO CASO CONCRETO. QUANTUM ARBITRADO EM R$ 2.000,00 (DOIS MIL REAIS) QUE COMPORTA MAJORAÇÃO PARA R$ 3.000,00 (TRÊS MIL REAIS). OBSERVÂNCIA AOS PRINCÍPIOS DA PROPORCIONALIDADE E RAZOABILIDADE. SENTENÇA PARCIALMENTE REFORMADA. Recurso da autora conhecido e provido.Recurso do réu conhecido e desprovido. (TJPR - 1ª Turma Recursal - 0003317-67.2020.8.16.0136 - Pitanga - Rel.: JUIZ DE DIREITO DA TURMA RECURSAL DOS JUIZADOS ESPECIAIS NESTARIO DA SILVA QUEIROZ - J. 23.05.2022)
(TJ-PR - RI: 00033176720208160136 Pitanga 0003317-67.2020.8.16.0136 (Acórdão), Relator: Nestario da Silva Queiroz, Data de Julgamento: 23/05/2022, 1ª Turma Recursal, Data de Publicação: 23/05/2022)

Ressalta-se que o estelionato na sua modalidade digital é considerado crime de ação penal pública incondicionada, ou seja, a responsabilidade para conduzir o procedimento é do Ministério Público, independente de manifestação de vontade da vítima, a natureza dessa ação ressalva a relevância de tratar esse delito de forma mais eficaz, independente da vontade da vítima de ver o autor do crime responsabilizado, com o fito de preservar a ordem social e diminuir o índice de novos casos.
13

Nesse sentido, cumpre destacar que mesmo a responsabilidade do crime ser direta em relação ao Autor, também pode abranger mais partes do processo dependendo da especificada do caso. A jurisprudência entende que a responsabilidade não é apenas do Estado, mas também da empresa, entidade ou qualquer terceiro que tenha a obrigação de tornar o ambiente digital seguro para o

usuário.

3.1 CONCEPÇÃO DAS NORMAS JURÍDICAS ATUALIZADAS E FORMAS DE PUNIÇÃO DO CRIME DO ESTELIONATO DIGITAL.

Como já explicitado, um grande fator que desencadeou o aumento da efetivação do crime em questão foi a pandemia, de modo que, com o advento do Covid-19, foi necessário que a população se protegesse em suas casas para corroborar com o distanciamento social e assim evitar a proliferação do vírus, ocorre que em contrapartida a isso foi destaque a aproximação online dos usuários que culminou em oportunidade para os criminosos inovarem suas artimanhas, contando com a suposta sensação de anonimato.
O crime de estelionato digital, no sistema jurídico atual do Brasil, é apreciado no âmbito do Direito Penal, o qual pressupõe responsabilização para esse tipo de ato, que era equiparado ao crime de estelionato, previsto no artigo 171 do Código Penal.
A Lei 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann, entrou em vigor como uma tentativa inicial de tipificar a conduta dos crimes na modalidade virtual para proteção dos dados pessoais da população em face aos criminosos virtuais, ocorre que com o passar dos anos se mostrou necessária a inclusão de novas medidas frente a progressão da criminalidade no país, em específico os crimes virtuais.
Para combater essa crescente negativa no âmbito jurídico nacional entrou em vigor a lei 14.155/21, de 27 de maio de 2021, que incluiu e modificou alguns parágrafos no supramencionado dispositivo legal, alterando algumas regras para julgar o crime.

Art. 1º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar com as seguintes alterações:
?Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
14

§ 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.
§ 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso:
I ? 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;
II ? Aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável. Pena ? reclusão, de 1 (um) a 4 (quatro) anos, e multa.

§ 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. Pena ? reclusão, de 2 (dois) a 5 (cinco) anos, e multa.

Dentre as alterações, foram incluídos os § § 2º-A e 2º-B, que tratam de fraude eletrônica, sendo o § 2º-A qualificadora para o crime de estelionato que não é praticado na modalidade presencial, ou seja, quando a frade é cometida com uso de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de reses sociais ou qualquer outro meio fraudulento análogo.

Fraude eletrônica
§ 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.
§ 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.
Estelionato contra idoso ou vulnerável
§ 4º A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso.
Art. 2º O art. 70 do Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), passa a vigorar acrescido do seguinte § 4º:
§ 4º Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção.? (NR).

Nesse sentido, observa-se que foram elencados os crimes específicos mediante fraude eletrônica objetivando tornar mais rigorosa a lei, ainda tentando acompanhar o avanço da criminalidade. Frisa-se que a Lei 14.155/21 deu ênfase também ao aumento da pena para esse crime na modalidade virtual, com pena de reclusão de 4 a 8 anos e o aumento de 1/3 ao dobro da pena acaso o crime seja praticado contra idoso ou vulnerável, com expectativa para prejudicar a prática delituosa.
15

Cabe destacar também a alteração quanto a competência para apuração do estelionato por fraude mediante cheque ou transferência bancária, o código de

processo penal previa que a competência era do local do banco sacado, o que muitas vezes dificultava a apuração do crime, até pela localização da vítima que nem sempre residia no mesmo local do banco sacado, competência esta alterada para o domicílio da vítima pela Lei 14.155/21.
Por fim, a execução da lei e a responsabilização dos golpistas submete-se a conduta das autoridades capazes, para investigar, processar e julgar os casos de estelionato digital, como a polícia e o poder judiciário.

4 O HISTÓRICO DA PRÁTICA DO ESTELIONATO DIGITAL E OS REFLEXOS DA LEI 14.155 FRENTE A VULNERABILIDADE DA VÍTIMA.

Como já demonstrado, o estelionato digital foi uma modalidade que cresceu esporadicamente com o advento da internet e o constante avanço da tecnologia, mas também teve um de seus marcos recentemente, em 2020, com crescimento exponencial pela pandemia da covid 19 que possibilitou mais ?vítimas? online.
Relativizando em números, o país registrou um aumento ainda mais expressivo que o estelionato comum quando em sua modalidade virtual, com direta relação a pandemia, em 2021 houve 120.470 (cento e cinto mil, quatrocentos e setenta) casos registrados, já em 2022 foram registrados 200.322 (duzentos mil, trezentos e vinte e dois) casos, um aumento de 66,2% (sessenta e seis virgula dois por cento) de acordo com os dados do Fórum Brasileiro de Segurança Pública (FBSP).
Foram registrados em 2021 115 (cento e quinze) estelionatos a cada 100 (cem) mil habitantes no país, já no ano seguinte foram registrados 189,9 (cento e oitenta e nove virgula nove), um aumento de 65,1% (sessenta e cinco vírgula um porcento), ainda de acordo com a FBSP o estado que detém o recorde de casos registrados de estelionato em sua modalidade digital é Santa Catarina, com 64.230 (sessenta e quatro mil, duzentos e trinta) registros em 2022 o que representa 32% (trinta e dois porcento) dos casos do país, ressalvando que Bahia, Ceará, Rio de Janeiro, Rio Grande do Norte, Rio Grande do Sul e São Paulo não tinham ou não disponibilizaram dados.
Cabe destacar que, além de Santa Catarina, tiveram relevantes aumentos Minas Gerais que passou de 25.574 (vinte e cinco mil, quinhentos e setenta e quatro)
16

casos em 2021 para 35.749 (trinta e cinco mil, setecentos e quarenta e nove) em 2022, um aumento de 49,4% (quarenta e nove vírgula quatro porcento), Distrito Federal que passou de 10.049 (dez mil e quarenta e nove) casos em 2021 para 15.580 (quinze mil, quinhentos e oitenta) em 2022, registrando um aumento de 55% (cinquenta e cinco porcento), e o Espírito Santo que passou de 10.545 (dez mil, quinhentos e quarenta e cinco) casos em 2021 para 15.277 (quinze mil, duzentos e setenta e sete) casos em 2022, o que resultou em um aumento de 44,8% (quarenta e quatro vírgula oito por cento).
Dentre todos esses dados disponibilizados pela FBSP cabe destacar por fim os Estados que mais sofreram variações em seus índices, quais sejam Roraima que

passou de 59 (cinquenta e nove) casos em 2021 para absurdos 759 (setecentos e cinquenta e nove) em 2022 acarretando um aumento de 1.186% (mil, cento e oitenta e seis por cento) e Goiás com um aumento de 1.041% (mil e quarenta e um porcento), passando de 128 (cento e vinte e oito) casos em 2021 para 1.461 (mil, quatrocentos e sessenta e um) casos em 2022.
Ainda sobre o marco recente que corroborou com a prática do referido delito é reiterado pelo Fórum Brasileiro de Segurança Pública (FBSP) que:

A digitalização das finanças, de serviço e do comércio, especialmente impulsionada durante o período pandêmico, contribui com a formação de um ambiente propício ao desenvolvimento de modalidades criminais que exploram vulnerabilidade nestes segmentos. (FBSP 2022, p. 6).

Conforme já citado, a modalidade de estelionato digital foi inserida ao Código Penal em meados de 2021 pela Lei nº 14.155/21 que também especificou o estelionato praticado na modalidade digital, por meio cibernético. Essa lei trouxe novidades legislativas que no geral foram positivas com relação a vulnerabilidade da vítima.
Destarte podemos citar que invadir dispositivo informático de uso alheio, ressalvando que conectado ou não a internet, com o fim de obter vantagem ilícita terá pena de reclusão de 4 (quatro) a 8 (oito) anos e multa, com suas devidas especificações, demonstrando assim a preocupação do legislador com as vítimas que infelizmente só estavam crescendo no país e isso refletiu no agravamento da pena que antigamente era disposta no crime de invasão de dispositivo informático, criando uma resistência ao criminoso na medida em que vê o crime como algo mais grave, mediante nova pena mais severa.
17

Ainda quanto aos reflexos dessa lei frente a vulnerabilidade da vítima podem-se listar os agravantes trazidos em sua redação quanto ao furto, com pena de reclusão de 4 a 8 anos, para o crime nessa modalidade realizado com o uso de dispositivos eletrônicos, conectados ou não a internet, por meio de uso de sistemas invasores ou violação de senha, além do agravamento se praticado contra idosos ou vulnerável com consequente aumento de pena de 1/3 ao dobro, ainda na hipótese de ser praticado por servidor fora do território nacional aumenta a pena de 1/3 (um terço) a 2/3 (dois terços).
Quanto ao estelionato também tornou-se agravante o furto qualificado no âmbito cibernético, com igual pena de reclusão de 4 (quatro) a 8 (oito) anos, além de possível multa e pode ter pena aumentada de 1/3 (um terço) a 2/3 (dois terços) acaso seja praticada por servidor fora do território nacional e acaso praticada contra idoso ou vulnerável poderá ter a pena aumentada de 1/3 (um terço) ao dobro.
Por fim, no que tange a invasão de aparelhos para obtenção de dados, a lei passou de detenção de 3 (três) meses a 1 (um) ano para reclusão de 1 (um) a 4 (quatro) anos. Ainda na hipótese de resultar em obtenção de informações sigilosos

pode ser majorada de reclusão de 2 (dois) a 5 (cinco) anos e multa, com agravante de 1/3 (um terço) a 2/3 (dois terços) caso ocorra prejuízo econômico decorrente da invasão.
Assim, as novidades legislativas trazidas pela lei confortam brasileiros que podem ser vítimas de criminosos fora do território nacional, o que é plenamente possível pelo advento da internet e também a população mais velha que, em suma maioria, não tem familiaridade com as ferramentas e linguagens online, não tendo manejo e trato com os meios digitais o que por muitas vezes os torna os principiais focos dos criminosos pela ?facilidade? e ?inocência? desses usuários em específico, assim como os vulneráveis.
Portanto, resta claro que o legislador buscou efetivamente ampliar a guarda dos direitos, de modo a, buscar uma equidade entre diversos grupos de pessoas/possíveis vítimas, resultando em maior segurança, de modo que passa a observar significativas mudanças objetificando proteger os direitos do usuário e penalizando de forma mais grave os criminosos.

5 CONCLUSÃO.

18

O presente artigo, por meio da análise de dados estatísticos, legislação e julgados, buscou tecer uma análise crítica da disciplina normativa do estelionato digital, suas formas de conduta e as possíveis consequências sociais.
Demonstrando que a sociedade está cada vez mais conectada e as redes sociais têm uma função muito importante nessa interação, ocorre que o aumento desenfreado de pessoas conectadas à internet propiciou um ambiente para prática de crimes e com diversas possibilidades de artimanhas dos criminosos, que enxergam a internet como ?terra sem lei?, para obtenção da vantagem ilícita virtualmente, caracterizando o estelionato digital.
Dentre as diversas artimanhas utilizadas pelos estelionatários destacarm-se o ?phishing?, utilizada para enganar os usuários e conseguir informações privadas, ?vishing? popularmente conhecido por ?phishing por voz? quando o ato é realizado por ligações ou envio de áudios com o mesmo intuito de ludibriar a vítima, mas para divulgar dados pessoais e ?smishing? modalidade em que a vítima é provocada a acessar link que corrompe seu aparelho, além de outros golpes como investimentos fraudulentos, promessas de retornos financeiros utopicamente elevados e esquema de pirâmides, esses golpistas beneficiam-se da leiguice de suas vítimas no âmbito de investimento financeiro com falsas promessas de enriquecimento acelerado para enganá-las.
Assim, restou demonstrado que os golpistas tem o mesmo fito, qual seja a obtenção da vantagem ilícita fazendo uso do ambiente cibernético, enquadrando-os no âmbito de estelionatários digitais.
Nesta senda, ainda não existia um enquadramento específico para conter o avanço do referido ilícito que muitas vezes poderia ser caracterizado como tentativa

de extorsão ou crimes análogos o que obrigou o poder legislativo a se atualizar. Para ?frear? o avanço do crime foi introduzida a Lei 12.737/2012, popularmente conhecida por ?Lei Carolina Dieckmann?, que surgiu após um incidente em que a atriz teve seu aparelho pessoal invadido e com isso o vazamento de fotos íntimas na rede.
A introdução da Lei ?Carolina Dieckmann? mostrou-se muito importante por iniciar a caminhada rumo a tipificada do crime de estelionato em sua modalidade digital, ocorre que a tecnologia seguiu se modernizando trazendo novas oportunidades para inovação dos criminosos que vivem as sombras da internet. Com o estabelecimento de modalidades de transferência eletrônica como ?TED? e ?PIX? 19

tornou-se cada vez mais comum o embate entre as autoridades e os golpistas, já demonstrando a necessidade de nova atualização da legislação atinente ao tema.
Quanto a responsabilidade do crime no âmbito jurídico restou pacificado pelas jurisprudências pátrias que torna-se direta em relação ao Autor, sendo aferida pelo Estado que tem o dever de tutelar a convivência no âmbito cibernético. Cumpre destacar que nem sempre a responsabilidade é exclusiva do Autor, podendo recair de forma subjetiva ou objetiva para um terceiro da relação que deveria zelar pela segurança dos dados pessoais do usuário, tais como bancos, tomadores de serviço...
O marco de crescimento registrado no crime de estelionato na sua modalidade virtual foi durante a pandemia de covid 19, época em que foi necessário a reclusão da população em casa o que gerou aumento exponencial de usuários online na rede e, em paralelo, oportunidade para os criminosos inovarem suas artimanhas.
Para combater essa crescente negativa no âmbito jurídico nacional entrou em vigor a lei 14.155/21, de 27 de maio de 2021 trazendo enrijecimento das penas e tipificação de novos crimes, como estelionato contra idoso ou vulnerável e fraude eletrônica, intentando ainda em penas mais rigorosas que podem ser alongadas a depender do caso e alteração de competência para estelionato por fraude mediante cheque ou transferência bancária, submetendo a execução da lei e responsabilização dos golpistas a conduta das autoridades capazes.
O que se conclui é que, com o passar dos anos as leis e medidas tomadas se tornam ultrapassadas vide o ?aperfeiçoamento? dos criminosos, portanto, com o fito do controle do Estado se tornar uma manutenção mais célere se mostrou necessário inserção de um sistema de inovação e renovação legislativa.
Ora, restou comprovado que o âmbito jurídico sempre buscou acompanhar a inovação criminosa trazendo atualizações a legislação para coibir a progressão desses ataques criminosos, mas igualmente restou comprovado que apenas acompanhar não está mais sendo o suficiente, tornando tendência o adiantamento aos movimentos da marginalidade com sucessivo progresso de imersão tecnológica das autoridades para se adiantar ao crime com a devida manutenção das leis de forma mais célere objetivando deter o claro avanço da criminalidade hodierna.

REFERÊNCIAS

20

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez.

BRASIL, DECRETO-LEI NO 2.848, DE 7 DE DEZEMBRO DE 1940. Código Penal. Rio de Janeiro, 7 de dezembro de 1940; 119º da Independência e 52º da República. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 08/06/2023.

BRASIL. LEI Nº 14.155, DE 27 DE MAIO DE 2021. Lei de Invasão a Dispositivo Informático [Internet]. Disponível em: https://www.in.gov.br/en/web/dou/-/lei-n-14.155-de-27-de-maio-de-2021-322698993. Acesso em: 24 nov. 2023

BRASIL. LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012. Lei de Invasão a Dispositivo Informático [Internet]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em:
24 nov. 2023.

BRASIL. LEI Nº 14.155, DE 27 DE MAIO DE 2021. Lei de Invasão a Dispositivo Informático [Internet]. Disponível em: https://www.in.gov.br/en/web/dou/-/lei-nº 14.155-de-27-de-maio-de-2021-322698993. Acesso em: 13 dez. 2023.

BRASIL. Tribunal de Justiça do Paraná. TJ-PR - Recurso Inominado XXXXX-67.2020.8.16.0136 PR. Relator Nestario da Silva Queiroz. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-pr/1511018743. Acesso em: 25 nov. 2023

BRASIL. Tribunal de Justiça do Rio Grande do Sul. TJ-RS - Apelação Cível XXXXX-22.2020.8.21.7000 RS. Relator Giovanni Conti. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-rs/932015329. Acesso em: 25 nov. 2023

BRITO, Auriney. Direito penal informático. São Paulo: Saraiva, 2013, p.189.

CAMPOS, Pedro Franco de [et al.]. Direito penal aplicado: parte geral e parte especial do Código Penal. - 6ª. Ed. ? São Paulo: Saraiva, 2016.

CASSANTI, Moisés de Oliveira. Crimes virtuais, vítimas reais. 1ª ed. Rio de Janeiro: Brasport, 2014, p.6.

CHAVES, Fábio Barbosa; TEIXEIRA, Filipe Silva. Os crimes de fraude e estelionato cibernético e a proteção do consumidor no e-commerce. 2020. Disponível em: <https://conteudojuridico.com.br>. Acesso em: 12/06/2023.

COELHO, Yuri Carneiro. Curso de Direito Penal Didático. vol. único, 2ª ed. ? São Paulo: Atlas, 2015.

CÔRREA, Gustavo Testa. Aspectos jurídicos da internet. 5. ed. rev. e atual. São Paulo, Saraiva, 2010.

CUNHA, Rogério Sanches. Manual de direito penal: parte especial (arts. 121 ao 361). 11. ed. rev., ampl. e atual. Salvador: JusPODIVM, 2019.
21

CUNHA, Rogério Sanches. Lei 14.155/21 e os crimes de fraude digital - primeiras impressões e reflexos no CP e no CPP. Meu Site Jurídico (JusPodivm), 2021. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2021/05/28/lei-14-15521-e-os-crimes-de-fraude-digital-primeiras-impressoes-e-reflexos-no-cp-e-no-cpp/. Acesso em: 13 dez. 2023.

FBSP. Fórum Brasileiro de Segurança Pública. Os crimes patrimoniais no Brasil: entre novas e velhas dinâmicas. Anuário Brasileiro de Segurança Pública, 2022. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2022/07/07-anuario-2022-os-crimes-patrimoniais-no-brasil-entre-novas-e-velhas-dinamicas.pdf. Acesso em 24 nov. 2023.

GENNARINI, Juliana. Revista de Direito Penal e Processo Penal, ISSN 2674-6093, v. 2, n. 2, jul./dez. 2020.

GONÇALVES, Victor Eduardo Rios. Direito penal esquematizado: parte especial do Código Penal. - 8. ed. ? São Paulo: Saraiva Educação, 2018.
GRECO, Rogério. Curso de Direito Penal: parte especial. v. III. 7. ed. Rio de Janeiro: Ed. Impetus, 2010.

GOUSSINSKY, Eugenio. Crimes digitais têm forte alta em vários estados; saiba como prevenir. Portal R7, 2021. Disponível em: https://noticias.r7.com/tecnologia-e-ciencia/crimes-digitais-tem-forte-alta-em-varios-estados-saiba-como-prevenir-05052021. Acesso em: 12 dez. 2023.

GRECO, Rogério. Curso de Direito Penal: parte especial. v. III. 7. ed. Rio de Janeiro: Ed. Impetus, 2010, p. 228.

HUNGRIA, Nelson. Comentários ao Código Penal ? Vol. IX. Rio de Janeiro: Forense, 1958.

MIRABETE, Júlio Fabbrini e FABBRINI, Renato N./ Manual de direito penal: parte especial: arts. 121 a 234-B do CP ? volume 2, 36° edição, São Paulo, Atlas, 2021.