UNIVERSIDADE FEDERAL DE JUIZ DE FORA
CAMPUS GOVERNADOR VALADARES
CURSO DE DIREITO

Lucas Eller Freitas de Alencar Miranda

OS IMPACTOS DA FALTA DE PUNIÇÃO PARA O CRIME DE ESTELIONATO DIGITAL NO BRASIL.

GOVERNADORVALADARES
2023

Lucas Eller Freitas de Alencar Miranda

OS IMPACTOS DA FALTA DE PUNIÇÃO PARA O CRIME DE ESTELIONATO DIGITAL NO BRASIL.

Trabalho de conclusão de curso apresentado ao Curso de Direito da Universidade Federal de Juiz de Fora – *campus* Governador Valadares, como requisito parcial para obtenção do título de Bacharel em Direito.

Orientador: Dr. Renato Santos Gonçalves

GOVERNADORVALADARES

2023

Lucas Eller Freitas de Alencar Miranda

OS IMPACTOS DA FALTA DE PUNIÇÃO PARA O CRIME DE ESTELIONATO DIGITAL NO BRASIL.

Trabalho de conclusão de curso apresentado ao Curso de Direito da Universidade Federal de Juiz de Fora – *campus* Governador Valadares, como requisito parcial para obtenção do título de Bacharel em Direito.

Aprovado em___ de_____ de_____.

BANCA EXAMINADORA

_____
Renato Santos Gonçalves
Universidade Federal de Juiz de Fora

_____
Hozana da Costa Barreiros
Universidade Federal de Juiz de Fora

_____
Dêner de Oliveira Maia
Universidade Federal de Juiz de Fora

AGRADECIMENTOS

Gostaria de expressar minha sincera gratidão a todas as pessoas que contribuíram para a realização deste trabalho e para a conclusão bem-sucedida do meu curso de Direito.

Primeiramente, agradeço a Deus, aquele que guia o meu caminho, me protege e nunca me abandona. Agradeço extremamente pela vida da minha namorada, minha companheira que me esteve comigo e me apoiou em todos os passos dessa caminhada universitária.

À minha família, Marcos e Zenilda, que nunca pouparam esforços para me ver atingindo meus objetivos. Victor e Isadora, que as vezes mesmo de longe, estavam lá para me apoiar e oferecer conselhos sempre que precisasse.

Aos meus amigos, Jéssica, Letícia, Lis, Gabriel e Murilo, meu agradecimento especial. O apoio emocional e incentivo que recebi de cada um de vocês foi essencial para superar os desafios ao longo deste percurso acadêmico.

Agradeço ao meu orientador, Renato Santos Gonçalves, por sua orientação valiosa e apoio constante que foram fundamentais para o desenvolvimento deste trabalho.

Agradeço também aos demais professores do curso de Direito, cujas aulas e conhecimentos enriqueceram minha compreensão da matéria e forneceram a base necessária para a realização deste estudo.

Agradeço aos colegas de turma, pela troca de experiências, discussões construtivas e pela amizade que tornou essa jornada mais significativa.

Por fim, agradeço a toda equipe da Delegacia de falsificações e defraudações, em especial a Lorena, Julia, Maria Luiza e Cleriston, que mesmo sem saber, contribuíram para a delimitação do tema deste estudo.

Cada um de vocês desempenhou um papel crucial no meu crescimento acadêmico e profissional, e por isso expresso minha profunda gratidão.

RESUMO

O tema do estudo aborda o problema da falta de punição relacionada ao crime de estelionato digital no contexto brasileiro. O estelionato digital representa uma ameaça crescente na era da tecnologia, e a ineficiência das medidas punitivas tem gerado consequências graves. O objetivo principal deste estudo é analisar os impactos que a falta de meios adequados de combate acarreta para a sociedade brasileira. Para isso, buscou-se conceituar cibercrime e estelionato digital; expor a relação entre pandemia do Covid-19 e o aumento dos casos de estelionato virtual; analisar os obstáculos que as instituições policiais enfrentam no combate ao crime cibernético; e comentar sobre a evolução legislativa relacionada ao ambiente e crimes virtuais. Foi utilizado o método dedutivo e exploratório, buscando-se compreender o fenômeno por meio de premissas. O estudo detém uma abordagem qualitativa e possui natureza básica. Por fim, este trabalho destaca a importância de uma abordagem abrangente e atualizada para enfrentar os desafios do estelionato digital no Brasil, a fim de garantir a proteção dos cidadãos, segurança jurídica e a adaptação da legislação às dinâmicas tecnológicas.

Palavras-chave: Falta de Punição. Crime. Estelionato digital. Crimes cibernéticos.

ABSTRACT

The theme of the study addresses the problem of the lack of punishment related to the crime of digital fraud in the Brazilian context. Digital fraud represents a growing threat in the age of technology, and the inefficiency of punitive measures has generated serious consequences. The main objective of this study is to analyze the impacts that the lack of adequate means of combat has on Brazilian society. To achieve this, we sought to conceptualize cybercrime and digital fraud; expose the relationship between the Covid-19 pandemic and the increase in cases of virtual fraud; analyze the obstacles that police institutions face in combating cybercrime; and comment on legislative developments related to the environment and virtual crimes. The deductive and exploratory method was used, seeking to understand the phenomenon through premises. The study has a qualitative approach and is basic in nature. Finally, this work highlights the importance of a comprehensive and updated approach to face the challenges of digital fraud in Brazil, in order to guarantee the protection of citizens, legal security and the adaptation of legislation to technological dynamics.

Keywords: Lack of punishment. Crime. Digital fraud. Cyber crimes.

SUMÁRIO

1. INTRODUÇÃO

O advento da internet modificou diversas áreas da sociedade, utilizada para trabalho, lazer, meio de informações, relacionamentos e etc. Responsável por grande desenvolvimento do globo, sua rapidez na propagação de informações permite que ela seja uma ferramenta facilitadora das mais diversas atividades cotidianas (DIAS, 2012).

Por mais que sejam incontáveis seus benefícios, à sociedade como um todo teve que se adequar às novas tendências, visto que essa ferramenta também é utilizada de maneira ardilosa. O anonimato, característica derivada dessa nova realidade, se tornou “prato cheio” para que criminosos pudessem praticar seus delitos sem estarem expostos às vítimas.

Sendo assim, o presente estudo tem como foco principal abordar sobre os impactos da impunidade para o crime de estelionato digital na sociedade brasileira e quais os motivos que acarretam esse fenômeno.

Levando em consideração o cenário atual sobre o baixo índice de punição para o crime de estelionato digital, o interesse nesse estudo surgiu durante um estágio realizado na delegacia de polícia civil da cidade de Governador Valadares, onde se percebe um grande crescimento da prática de golpes realizados no ambiente virtual, assim como os obstáculos para localizar os autores desses delitos. Além disso, por se tratar de um fator recente, o campo científico brasileiro carece de estudos focados nos cibercrimes.

Os problemas relacionados a impunidade desses delitos baseiam-se na dificuldade de acesso aos criminosos, decorrente de uma série de características presentes nos crimes cibernéticos, as quais os próprios autores utilizam de ferramenta para a prática, como o anonimato e a facilidade de acesso a novas vítimas, o que acarreta em um aumento do número de casos, e consequentemente, da quantidade de vítimas que se dirigem as instituições policiais, sobrecarregando-as.

Dessa forma, é possível notar que o estudo desse tema pode impactar direta ou indiretamente o estudo e desenvolvimento de técnicas precisas de prevenção e combate à prática dos golpes virtuais, trazendo maior seguridade tanto no âmbito patrimonial, quanto em matéria de proteção de dados pessoais para a população brasileira.

Nesse sentido, esse trabalho tem como propósito analisar os motivos para a falta de punição do delito de estelionato virtual e quais os impactos que acarreta para a sociedade brasileira. Para isso, buscou-se definir os conceitos de cibercrime e estelionato digital, identificar a relação entre pandemia e o aumento dos casos de golpes virtuais, apontar as razões pelas quais as instituições policiais enfrentam dificuldades na captura dos criminosos e por fim, discutir formas de combate aos golpes virtuais.

A metodologia utilizada compreende uma análise dedutiva e exploratória, a fim de compreender o fenômeno estudado. O trabalho utiliza-se da abordagem qualitativa onde procura-se compreender e aprofundar nos fenômenos discutidos de forma abrangente, levando em conta qualidade dos dados analisados e não a quantidade. Será utilizado de pesquisa bibliográfica interpretando os fenômenos a partir de seus motivos e resultados. Ressalta-se a natureza básica, por não se aplicar diretamente a um caso específico, e sim a uma busca de conhecimento focado no combate à situação-problema para enfim atingir os objetivos apresentados.

2. CIBERCRIME

2.1 Sociedade Digital

Com os adventos da globalização, atualmente a internet é utilizada com diversas finalidades, seja educação, trabalho ou lazer, entretanto, seu surgimento em meados da década de 60 possuía desígnio militar. Em meio a guerra fria, os Estados Unidos, por meio da ARPA (Advanced Research Projects Agency), órgão que integrava o Departamento de Defesa Nacional norte americano, criou um arcaico sistema com o intuito de otimizar o envio de informações acerca de possíveis ataques sofridos (Pinho 2003, Capobianco 2010).

No território brasileiro, a Lei 12.965 de 23 de abril de 2014 define internet como:

> I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes. A Internet é a tecnologia que permite a comunicação entre pessoas de todos os lugares em tempo real. É a transmissão de dados entre os dispositivos que não estejam necessariamente conectados, portanto é possível identificar que a Internet facilita a vida do indivíduo que pretende praticar condutas delituosas (BRASIL, 2014).

Rapidamente difundida para o âmbito educacional, com o passar dos anos a internet foi se aprimorando e sendo difundida para as demais localidades do globo. Baseando-se nas falas de Wilson Dizard, Luís Monteiro (2001), em sua obra de mestrado conceitua o termo internet como “A internet (ou a “Rede” como também é conhecida) é um sistema de redes de computadores interconectadas de proporções mundiais”.

Castells ilustra o seguinte acerca da rapidez de propagação da internet:

> A Internet tem tido um índice de penetração mais veloz do que qualquer outro meio de comunicação na história: nos Estados Unidos, o rádio levou trinta anos para chegar aos sessenta milhões de pessoas; a TV alcançou esse nível de difusão em 15 anos; a Internet o fez em apenas três anos após a criação da teia mundial (CASTELLS, 1999, p.439).

Como a “rede” não se atém a barreiras físicas, após difundida para o globo, proporcionou um dinamismo jamais visto na troca de informações, onde certo indivíduo pode se comunicar com outro mesmo estando em lados opostos do globo. Esses fatores interligados deram início ao conceito de Sociedade Digital, pois através da tela de um dispositivo, uma pessoa tem acesso a um universo paralelo, detentores de sua própria cibercultura e ciberespaço (DIAS, 2012).

Por mais que a expansão digital tenha trazido inúmeras melhorias no cotidiano da sociedade, é inegável que ela também expõe seus usuários a riscos, sejam eles a intensa disseminação de informações falsas, exposições de dados pessoais e a uma nova modalidade de crime, os cibercrimes (NASCIMENTO, FELIX, 2023).

2.2 Conceituando Cibercrime

O cibercrime, ou também denominado crime cibernético, trata-se de um fenômeno recente, e por isso há discordância teórica quanto a sua exata nomenclatura e significado. Para Sérgio Marcos Roque, o cibercrime é: “toda conduta, definida em lei como crime, em que o computador tenha sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material.” Já para Simas (2014), o meio informático precisa estar correlacionado ao tipo legal, para que seja considerado cibercrime, mesmo que o bem tutelado não seja cibernético.

Devido a suas características e complexidades, os crimes cibernéticos carecem de um conceito amplo, visto que essa classificação aborda tipos penais distintos,

porém agora praticados no universo digital, tais como, estelionato, pornografia infantil, crimes contra a honra, racismo, etc.

Resumindo, o cibercrime divide-se em duas principais vertentes, inicialmente, a teoria de que o ambiente virtual é elemento essencial para a prática do crime, e sem ele o tipo seria inexistente, e por outro lado, de que o tipo penal já é existente, porém o uso de aparatos digitais potencializa novas formas de praticar o delito, ou seja, nas palavras de Simas (2014), oferece “novas formas de praticar antigos crimes”.

Dentre essas vertentes, o crime cibernético atua desde motivos pessoais, como o roubo de informações pessoais, fraude online, crimes patrimoniais, hacking, distribuição de conteúdos ilegais até questões que atentem contra organizações ou governos, a saber, ataques a infraestruturas críticas, roubo e vendas de dados corporativos, entre outros.

Independentemente das divergências de definição, é harmônico entre os juristas que a criminalidade informática representa uma ameaça à sociedade e afronta diretamente os direitos fundamentais de suas vítimas.

Por esse motivo, o cibercrime é um desafio crescente tanto para empresas, indivíduos e até mesmo nações, vez que, a tecnologia digital empenha função cada vez mais essencial na sociedade. Dessa forma, o tipo penal vem sendo alvo de alterações legislativas e demais medidas a fim de garantir maior segurança cibernética para suas organizações e população.

2.3 Teoria do Bem Jurídico

Introduzido no século XIX por Fritz Birnbaum, originalmente o conceito de bem jurídico era utilizado como instrumento teórico para justificar a aplicação das normativas penais como forma de proteção dos ideais morais da sociedade. Essa ideia é antagônica a até então doutrina dominante na época, em que Feuerbach pregava a aplicação do direito penal apenas para a proteção dos direitos subjetivos, ou seja, aqueles direitos já reconhecidos pelo ordenamento jurídico (STUCKENBERG, 2014).

A teoria do bem jurídico é um conceito fundamental no âmbito do direito penal, pois baseia-se na ideia de que esse campo jurídico deve se concentrar na proteção dos bens jurídicos, isto é, interesses e direitos que a sociedade em questão julgou como dignos de uma proteção mais restritiva. Dito isso, a teoria do bem jurídico busca

delimitar o escopo de atuação do direito penal, deliberando que a norma nacional deve tutelar criminalmente somente as condutas que afrontam direta ou indiretamente, a integridade dos ditos bens jurídicos (SILVA, 2011).

Para Stuckenberg (2014), a principal corrente de bem jurídico é: “uma norma penal só é legítima se apta a proteger algum bem jurídico pessoal”. Como bem jurídico pessoal, entende-se pelas circunstâncias essenciais para que um indivíduo consiga se desenvolver, físico e mentalmente, como ser humano. Dentre elas temos a vida, integridade física, liberdade, propriedade, entre outras, que devem ser especialmente protegidas devido ao seu status essencial (ROXIN, 2006).

Essa abordagem possui várias implicações, dentre elas, a limitação do direito penal. Por se tratar de uma violação institucionalizada de direitos fundamentais individuais, a aplicação do direito penal deve ser restrita para situações em que a sociedade carece de proteção contra condutas específicas, que violam as normas constitucionais, os bens jurídicos de outrem. Esta interpretação limita o poder punitivo do Estado, que não deve ser usado de forma excessiva ou arbitrária, devendo ser utilizado somente como último recurso (COSTA, 2014).

Outro ponto decorrente da teoria do bem jurídico diz respeito à proporcionalidade das punições. Instaurado para proteger os interesses relevantes à sociedade, a aplicação penal deve ser proporcional à gravidade da conduta violadora do direito. Dessa forma, caso a ameaça ou dano sejam mínimos, a penalidade aplicada deve ser proporcionalmente reduzida; em contrapartida, caso a conduta criminosa infrinja ou atente gravemente contra o bem protegido, tal fato deve ser levado em conta para aplicação de uma pena correspondente à gravidade da conduta praticada (COSTA, 2014).

O crime de estelionato, assim como no ordenamento jurídico brasileiro, é considerado infração penal e, portanto, tratado no campo penal nos sistemas jurídicos de diversos países. Conforme apresentado, para que o delito seja abordado no campo criminal, ele deve atentar contra um bem jurídico, dito isso, o delito de estelionato, em breve análise, consiste na concessão de bens ou vantagens de terceiro, utilizando de meios fraudulentos. Essa conduta viola um bem jurídico protegido, o patrimônio, além de afetar a mente das vítimas ao induzi-las a erro.

Nesse viés, ao tipificar penalmente o delito de estelionato, o Estado busca construir uma relação de confiança na ordem pública, visto que, as vítimas desse crime agora podem se escorar no governo quando necessário. A intervenção penal

deveria conferir maior segurança nas relações entre indivíduos na sociedade, punindo aqueles que abusam dessa confiança para aplicar os golpes.

É de suma importância analisar se a imputação penal ao crime de estelionato realmente está cumprindo com sua finalidade pretendida, visto que, caso a tipificação atual não esteja sendo efetiva, faz-se necessário estudar novos meios de punição e combate, inclusive formas distintas do âmbito criminal.

Atualmente, o delito de estelionato é reprimido no âmbito criminal, pela condenação do criminoso, e também possui implicações na área cível. Quanto à condenação criminal, essa fundamenta-se no conceito de finalidade da pena. Independente da omissão do ordenamento penal quanto a esta matéria, o entendimento majoritário é de que, no Brasil, a pena possui tríplice finalidade, são elas: Retributiva, preventiva e educativa. Dessa forma, ao imputar penalmente esse delito, o Estado visa inicialmente dissuadir o possível criminoso a dar continuidade aos seus atos, tendo caráter de prevenção. Caso o delito seja praticado, a pena atua para responsabilizar os infratores, de maneira justa e proporcional. Por fim, a sanção penal possui função pedagógica, onde transmite para o infrator e para a sociedade acerca da gravidade dessas condutas fraudulentas (MEDEIROS, 2015).

No Brasil, é questionável dizer que a pena realmente atinge sua finalidade, visto que, em pesquisa realizada pelo Conselho Nacional de Justiça (2015), foi revelado que um em cada quatro condenados tornam-se reincidentes no Brasil. A pesquisa trata de indivíduos que sofreram o trânsito em julgado de sentença condenatória, dito isso, se apurar os casos cometidos e sem conclusão policial, os números podem ser ainda mais alarmantes. Por essa razão, já que a imputação penal ao crime de estelionato não é totalmente eficaz quanto a seu efeito de prevenção, de reeducação e reintegralização, infere-se que ela não atende sua finalidade doutrinária.

Em termos de responsabilidade civil, uma pessoa que comete o estelionato pode ser submetida a ressarcir a vítima por prejuízos materiais e morais sofridos em decorrência de fraude. Essa responsabilidade decorre do princípio geral do Direito que estabelece a obrigação de reparar os danos causados a terceiros em virtude de atos ilícitos (TJDFT, 2018).

Assim, a vítima do estelionato pode buscar peças por meio de ações civis para obter compensação financeira por danos materiais, como perdas financeiras diretas, e por danos morais, que envolvem o sofrimento psicológico decorrente do ilícito.

2.4 Estelionato Digital x Estelionato Tradicional

Em sua etimologia, a expressão estelionato origina da palavra grega *stelio*, nomenclatura atribuída a uma espécie de lagarto que se camufla no ambiente para ludibriar e capturar suas presas. Este fenômeno está diretamente relacionado ao tipo penal, visto que o criminoso utiliza de artimanhas para enganar as vítimas e obter vantagem indevida (RIBEIRO, 2019).

O crime de estelionato, está elencado no ordenamento jurídico brasileiro no rol de crimes contra o patrimônio. O Código Penal Brasileiro, Título II, Capítulo VI, artigo 171, caput, dispõe o seguinte:

> 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 um a cinco anos, e multa (BRASIL, 1940).

Baldan (2020), conceitua o estelionato como uma forma evoluída de captação do patrimônio alheio, visto que o criminoso utiliza de ferramenta diversa da violência para a obtenção do benefício ilegal pretendido. Nesse teor, a vítima não é acometida de dano físico, em contraponto, o autor visa atingir o mental do indivíduo ao utilizar de argumentos enganosos, conduzindo-o a erro.

Em viés semelhante, Andreucci (2014) ilustra estelionato como a prática criminosa em que o autor induz a vítima a erro por instrumento ardil ou fraudulento, a fim de obter benefício para si mesmo ou para um terceiro. Dessa forma, este delito baseia-se na má-fé do criminoso que busca enganar sua vítima para adquirir alguma vantagem, usualmente se tratando de vantagem patrimonial.

O estelionato tradicional (caput) e o estelionato digital possuem semelhanças em matéria de fraude, engano e obtenção ilegítima de vantagem. Todavia, essas modalidades divergem principalmente quanto aos meios e métodos utilizados. Sua modalidade tradicional utiliza de instrumentos físicos e presenciais, como cheques sem fundo e cartões clonados, enquanto o digital ocorre principalmente em ambiente virtual, utilizando da tecnologia para consumação do crime.

Além disso, o crime virtual tem por característica um alcance geográfico mais abrangente, visto que o criminoso pode estar localizado em qualquer local do mundo e aplicar os golpes em vítimas de qualquer parte do globo. Esse fator, somado ao

anonimato dos malfeitores e aos frequentes conflitos de jurisdição tornam, consequentemente, o delito virtual mais complexo e desafiador no tocante à investigação, se comparado a sua modalidade tradicional.

O estelionato é um crime em constante desenvolvimento, portanto é fundamental que o ordenamento jurídico brasileiro, assim como suas instituições legais, acompanhe essas transformações a fim de lidar de forma eficaz com os desafios impostos pela tecnologia (MOREIRA, MELLO, 2023).

Para fins de adequação à nova realidade, o ordenamento jurídico brasileiro, por meio da Lei nº 14.155/21 acrescentou algumas disposições em seu artigo 171 do Código Penal, direcionadas ao crime em meio eletrônico, a saber:

> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional (BRASIL, 2021).

Nota-se que essa adequação legislativa majora a pena base do crime de estelionato por considerar mais gravosa a conduta que utiliza do ambiente virtual para consumação, visto que essa prática dificulta a defesa da vítima, e ainda, oferece obstáculos para a investigação policial, já que o criminoso pode estar em qualquer local do globo.

Em 2022, mediante a Lei nº 14.478, o ordenamento normatizou o artigo 171-A do código penal, que trata sobre a disposição de ativos virtuais, com intuito de obter vantagem ilícita (BRASIL, 2022).

Dessa forma, observa-se a tentativa da legislação brasileira em se adequar às transformações tecnológicas ao impor maior rigidez legislativa ao crime de estelionato. Todavia, ainda há muito a ser feito, visto que, principalmente após a pandemia do COVID-19, os casos de golpes virtuais cresceram exponencialmente, sendo que os criminosos continuam encontrando brechas para praticarem seus atos ilícitos.

Para tanto, faz-se necessário analisar as variáveis envolvendo esta modalidade de crime para traçar medidas efetivas de combate ao crime, a fim de assegurar o bem jurídico patrimonial da coletividade, assim como garantir maior seguridade para todos.

3. A relação da pandemia do COVID-19 com o aumento dos casos de estelionato digital

Durante a pandemia global do COVID-19, em recomendação da Organização Mundial de Saúde (OMS), diversos locais do globo sofreram de políticas públicas de *lockdown*, ou seja, uma espécie de confinamento domiciliar com o intuito de desacelerar a propagação do vírus. Consequentemente, a população teve que adaptar suas relações sociais, educacionais e de trabalho à nova realidade, fato pelo qual aumentou muito o fluxo de pessoas que passaram a acessar a internet.

A partir de estudos divulgados pelo Centro de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC.BR), no ano de 2020, o Brasil alcançou 152 milhões de usuários, correspondente a 81% da população acima dos 10 anos e a 83% das residências do país. Essa realidade representa um aumento de 7% se comparados a 2019, ano anterior.

Como consequência do aumento do fluxo de pessoas utilizando os aparatos digitais, os criminosos também se adaptaram. Estima-se que o número de casos de estelionato digital aumentou em quase 500% do ano de 2018 até 2021, segundo dados publicados no Fórum Brasileiro de Segurança Pública (FBSP), isto é, em números brutos, no ano de 2018 foram registrados 7.591 casos, enquanto no ano de 2021, já haviam sido registrados 60.590 casos de estelionato em sua modalidade virtual (FBSP, 2022).

Nesse viés, Rafael Alcadipani, especialista em segurança pública, diz o seguinte: “O criminoso sempre vai buscar o maior lucro com o menor risco. O estelionato é um crime que depende de representação, a pessoa tem que ir lá e decidir que quer denunciar a pessoa. As penas não são tão altas quanto um roubo ou um furto”.

Por essas condições, os criminosos enxergam positivamente o crime de estelionato, já que ele apresenta menor risco de captura, ainda mais em sua modalidade virtual, que anulam quase totalmente as chances de flagrante. Ao ser um delito condicionado à representação, em muitos dos casos, as vítimas acham não valer a pena se deslocarem até as delegacias para darem início a um inquérito policial. E, por fim, caso sejam capturados, as penas são mais brandas.

Com a fabricação das vacinas do COVID-19 e sua distribuição às massas, aos poucos a vida fora dos ambientes eletrônicos foi voltando à normalidade, entretanto,

o número de casos de golpes virtuais continuou a crescer na sociedade brasileira. Em 2022, o Brasil registrou um aumento de 66,2% de casos de estelionato digital, segundo dados da FBSP.

Infere-se, portanto, que a pandemia do COVID-19 e suas medidas de segurança popularizaram a nova tendência do crime de estelionato praticado em modalidade virtual, visto que após o relaxamento das medidas de *lockdown*, os criminosos não voltaram a seu modo de execução anterior, mas continuaram a operar em meios cibernéticos, possivelmente por observarem um menor risco em suas práticas ilícitas nesse meio.

4. Obstáculos das instituições policiais na investigação e combate aos golpes virtuais

Existe uma vertente de pensamento popular que o sistema judicial brasileiro é insuficiente para o julgamento eficaz do delito de estelionato. Essa afirmação resulta no sentimento de insatisfação popular ante a persecução penal, principalmente em sua fase pré judicial, ou seja, quanto à investigação criminal. Os casos de estelionato no Brasil se tornaram tão frequentes, que as vítimas passaram a se acomodar e em alguns casos, nem se preocupam em procurar as instituições policiais para representarem a favor da apuração criminal.

Tal fato, juntamente com o excesso de demanda em virtude do aumento do número de casos, contribui para o recrutamento de novos criminosos, o que agrava exponencialmente a situação vivenciada. Dito isso, este tópico abordará sobre os principais obstáculos da investigação criminal para os casos de estelionato digital.

Para compreender os principais obstáculos existentes no combate aos golpes virtuais, a priori deve-se estudar a realidade das instituições policiais brasileiras, principalmente da polícia civil, responsável pela investigação criminal e demais diligências iniciais da persecução penal.

A Polícia Civil brasileira é uma das instituições responsáveis pela manutenção da segurança pública da sociedade. É importante observar que a Polícia Civil, atua em âmbito estadual, com sua estrutura e hierarquia regulamentadas por lei complementar e estatutos próprios para cada estado. Esta instituição possui competência para apurar os delitos praticados dentro de suas respectivas jurisdições.

Tal diretriz limita a atividade policial dentro de suas próprias jurisdições, fato que apresenta consequências positivas e negativas.

Derivado do federalismo brasileiro, a União concede a cada ente federativo estadual o poder de dispor sobre suas instituições policiais. Dessa forma, cada ente federativo mantém suas corporações de acordo com suas demandas e realidade.

Nesta última década, o Sindicato dos Servidores da Polícia Civil do Estado de Minas Gerais (SINDPOL/MG) debateu sobre a pauta de déficit e sucateamento da Polícia Civil. Dentre as pautas, as principais são acerca da precariedade de servidores públicos, o que resulta em jornadas de trabalho que extrapolam as 40 horas semanais, e falta de reconhecimento, já que devida a alta demanda, e poucos servidores, torna-se comum o atraso no serviço (SANTOS, 2011).

Mesmo diante dessa realidade de sucateamento, com poucos servidores e muita demanda, a polícia ainda enfrenta alguns obstáculos como as barreiras territoriais, a impessoalidade dos criminosos, a constante evolução dos golpes digitais e a facilidade na abertura de contas laranja em instituições financeiras.

No tocante às barreiras territoriais, para que haja uma troca de informações entre a instituição de um estado para com outro, é necessário a realização de diligências que, assim como as demais ações processuais, são reguladas por prazos instituídos por lei. No caso dos crimes de estelionato digital, em que todas as ações são muito dinâmicas, inclusive quanto a transferências de valores, onde rapidamente o dinheiro se perde em meio a diversas transferências bancárias, essa troca de informações entre as polícias estaduais deveria ocorrer em uma dinâmica similar a atividade criminosa, caso contrário a eficácia da investigação sofrerá prejuízos.

É fato que a interceptação criminosa é menos danosa à sociedade, já que oferece menos prejuízo às vítimas, face a possibilidade de reaver seus bens prejudicados. Porém, a realidade existente entre as polícias estaduais, ou até dentro do mesmo estado, mas em jurisdições distintas, não se evolui à altura da demanda, e no caso dos crimes cibernéticos, quando o objeto do crime sai da sua origem, aumentam consideravelmente as dificuldades e o tempo tomado na solução dos casos.

Além da possibilidade de se encontrarem espalhados pelo mundo, o anonimato que as plataformas virtuais oferecem aos seus usuários é outro fator que dificulta, e muito, a atuação policial em situações de ocorrência criminal. Respaldados pelas leis de proteção de dados, as redes sociais utilizam de criptografias de ponta para proteger

as interações de seus usuários, o que dificulta no acesso à informações essenciais nos casos de investigação policial, uma vez que, as autoridades brasileiras passam a depender da colaboração de empresas do setor privado para seguimento de suas investigações (FERREIRA, OLIVEIRA, 2023).

Outrossim, a falta de preparo das instituições policiais, que não investem no treinamento adequado de seus servidores, somado à enorme quantidade de dados gerados na internet, tornam o rastreamento de informações relevantes um desafio, principalmente nos casos em que envolvem investigações em larga escala (FERREIRA, OLIVEIRA, 2023). Os criminosos por outro lado, aproveitam do despreparo policial, para constantemente evoluírem seus métodos, desenvolvendo novas táticas e técnicas para contornar as medidas de segurança existentes e atingir seus objetivos.

Por fim, um dos pilares para a efetividade dos estelionatos digitais remetem a facilidade de abertura de contas em instituições financeiras, em especial nas instituições cujo atendimento seja especificamente on-line (RODE, ROHDEN, 2022). Como um dos elementos constitutivos do tipo penal do estelionato diz respeito à obtenção de vantagem, essa vantagem geralmente se traduz em valores patrimoniais, portanto, para que isso ocorra nos golpes cibernéticos, o valor obtido deve ser transferido para uma conta de acesso dos golpistas. Entretanto, caso os valores fossem enviados para contas bancárias de autoria dos criminosos, seria simples para as autoridades solucionarem o caso e submeter os indivíduos ao aparato penal.

O ponto central da problemática, baseia-se no fato de que os dados pessoais utilizados para abertura de contas são, em geral, de outras vítimas, que têm seus CFPs e demais informações usadas para abrirem contas em seus nomes, sem ao menos saberem disso. Dessa forma, as vítimas, sem seu consentimento, se tornam laranjas dos criminosos, que utilizam de uma rede de contas e transferências, para mascarar o destino final do ativo patrimonial.

Esse fenômeno, somado as barreiras de jurisdição estaduais e transnacionais, anonimato, constante evolução das técnicas utilizadas nos golpes, aumento significativo de casos nos últimos anos, e a falta de preparo e sucateamento das instituições policiais, são os principais responsáveis para a falta de punição para o crime de estelionato digital no Brasil.

4.1 A responsabilidade das instituições financeiras nos golpes digitais

Conforme apontado anteriormente, uma das variáveis facilitadoras para a prática dos golpes cibernéticos, diz respeito a abertura de contas bancárias laranja. A questão a ser debatida remete-se em, até quando, as instituições financeiras devem ser solidariamente responsáveis pela restituição dos prejuízos gerados às vítimas desse crime.

Para fins didáticos, contas laranja remetem-se a um tipo de fraude, onde um indivíduo utiliza os dados pessoais de um terceiro, para abrir uma conta bancária a fim de realizar as movimentações pretendidas. Dessa forma, a conta laranja pode ser utilizada para a receptação e repasse de valores adquiridos ilegalmente sem ter ciência da origem desse dinheiro (RIBEIRO, p.122, 2023). Como os dados utilizados são de terceiros, muitas vezes sendo vítimas de golpes anteriores, não é possível traçar um nexo causal entre as transferências, o que dificulta as investigações.

Enquanto os bancos grandes, como caso do Banco do Brasil, Caixa Econômica Federal, possuem diretrizes de "*know your client"*, traduzido em "conheça seu cliente", os bancos digitais possuem critérios mais brandos para abertura de contas, bastando o fornecimento de dados, e envio de fotos de documentos e de perfil para "comprovarem" sua identidade (FERNANDES, ZANI, 2023). Todavia, esses critérios são extremamente suscetíveis a fraudes, já que em diversos casos os documentos e fotos enviadas são alvos de montagens ou demais técnicas para fraudar a identidade de terceiro.

Esse assunto já foi pauta de discussão pelo Presidente do Banco Central, Roberto Campos Neto, que afirmou o seguinte: "A gente vê que tem um número de contas laranjas que são abertas, que estão mais relacionadas a essas plataformas onde o processo de abertura é mais fácil". Dito isso, as autoridades financeiras já estão a par da realidade bancária, e estão estudando maneiras de restringir a abertura de contas nessas instituições com atuação predominante on-line (NETO, 2021).

Outra prática frequentemente utilizada pelos criminosos refere-se ao *"phishing"*. Esta expressão deriva-se da palavra "*fishing*", em que sua tradução para a língua portuguesa se remete à ação de pescar. Ou seja, este termo concerne a uma técnica de fraude online onde, a partir de meios fraudulentos, os indivíduos agem na intenção de obter informações pessoais de terceiros, como por exemplo, senhas de aplicativos financeiros e demais dados bancários (PINHEIRO, 2022).

Como forma de maximizar a eficiência dos golpes, os fraudadores copiam a logo, endereço eletrônico, entre outros elementos identificadores da instituição original, alteram algum detalhe e entram em contato com as vítimas que, acreditando se tratar da entidade original, são induzidos ao erro e oferecem seus dados aos criminosos.

Por mais que a culpa dos golpes digitais recaia sobre os fraudadores, pode-se afirmar que as instituições bancárias possuem certa responsabilidade quanto a esta realidade, visto que em alguns casos, o vazamento de dados teve origem da própria instituição. Em acórdão, referente ao REsp 2.077.278, a 3ª Turma do Superior Tribunal de Justiça julgou, por unanimidade, pela responsabilidade da instituição bancária em casos de vazamento de dados pessoais e sigilosos de clientes.

Nesse viés, a Ministra Nancy Andrighi, relatora do recurso, afirmou o seguinte:

> Assim, para imputar a responsabilidade às instituições financeiras, no que tange ao vazamento de dados pessoais que culminaram na facilitação de estelionato, deve-se garantir que a origem do indevido tratamento seja o sistema bancário. Os nexos de causalidade e imputação, portanto, dependem da hipótese concretamente analisada (ANDRIGHI, 2023).

É fato que os bancos detêm uma grande quantidade de dados pessoais que, caso sejam vazados, podem acarretar em diversos prejuízos aos clientes. Dessa forma, os estelionatários utilizam de tecnologias ilícitas para violar esses dados sigilosos dos clientes, porém, como essas informações estavam em posse das entidades financeiras, cabe a elas assumir responsabilidade pela fraude em determinados casos (TJRJ, 2023).

Como é a imagem da instituição financeira em cheque, assim como a integridade de seus clientes, é necessário que essas entidades adotem algumas medidas preventivas e protetivas, a fim de combater os problemas elencados. Aqui estão algumas atitudes a serem desenvolvidas: Uso de criptografia e demais tecnologias para proteção de dados; Medidas de monitoramento de transações; Educação e comunicação clara com os clientes, acerca das maneiras em que o banco entra em contato com os consumidores e de possíveis atitudes suspeitas; Respostas dinâmicas e efetivas em casos de incidentes.

Além disso, faz-se necessário a adoção de métodos mais seguros para abertura de contas, a fim de diminuir a incidência de contas laranja, já que estas

atentam contra o status quo de segurança da sociedade. Caso a instituição não adote as medidas adequadas para promover a segurança de seus clientes, ela pode ser considerada responsável perante a lei dos prejuízos acarretados por possíveis fraudes, conforme disposto na Súmula 479 do Superior Tribunal de Justiça (BRASIL, 2012).

5. Análise da Legislação Penal Brasileira aplicável aos cibercrimes

Com o advento da internet, a circulação de informações foi otimizada a níveis nunca antes vistos. Seja qual for o acontecimento, ele circula o globo em instantes e, rapidamente, um indivíduo do outro lado do mundo tem acesso a informações sobre o fato ocorrido. Essas relações cotidianas simbolizam o dinamismo em que as sociedades contemporâneas estão inseridas onde, os indivíduos são bombardeados com novas tendências de diversos aspectos, seja moda, lazer, lifestyle, até questões relacionadas a padrões morais, ética, questões ligadas a direitos, legislação, entre outros.

Dessa forma, o ordenamento jurídico nacional também deve se adequar a esta nova realidade social, de forma a adaptar a legislação vigente em detrimento das novas características da sociedade. Dito isto, o ordenamento brasileiro há cerca de 11 anos vem modificando seus dispositivos legais a fim de legislar sobre esses assuntos emergentes.

5.1 Lei Carolina Dieckmann e o marco para a tipificação específica aos delitos digitais.

Considerado um marco para a regulação de normas focadas nos crimes cibernéticos, a Lei nº 12.737/12, apelidada de Lei Carolina Dieckmann, ganhou grande repercussão na mídia nacional, pois a vítima do caso se tratava de uma atriz brasileira. A mesma teve algumas fotos íntimas vazadas de seu computador, sem seu consentimento, enquanto a máquina estava em uma loja de assistência técnica. O infrator ainda entrou em contato com a vítima por um e-mail, no qual continha um link malicioso, o qual deixaria o dispositivo da vítima vulnerável a invasões. Após, chantageou-a a pagar uma quantia específica, caso contrário distribuiria em massa as

fotos íntimas da atriz que não cedeu às ameaças, e com isso teve suas fotos vazadas (FERREIRA, 2021).

O autor do crime foi indiciado por extorsão, nos termos do artigo 158 do Código Penal Brasileira, face a presença de chantagem com o objetivo de receber vantagem econômica indevida, elemento tipificador do delito de extorsão. Todavia, o ato praticado pelo infrator extrapola o crime previsto no artigo 158 do Código Penal, visto que a privacidade da vítima também foi violada pela invasão de dispositivo informático, fato que até então não era penalizado pela legislação brasileira (BRASIL, 1940).

Mediante a repercussão nacional do caso, em 03 de dezembro de 2012 foi sancionada a Lei 12.737, a qual tipificou o crime de invasão de dispositivos informáticos, atualmente previsto pelo artigo 154-A do Código Penal Brasileiro. Esta legislação foi um marco significativo ao abordar de maneira específica os crimes cibernéticos, introduzindo uma inovação notável ao instituir o tipo penal relacionado à invasão de dispositivos informáticos (ALMEIDA, MENDONÇA, CARMO, SANTOS, SILVA, AZEVEDO, 2013).

O artigo 154-A do CPB dispõe o seguinte:

> 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.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º , aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.” (BRASIL, 2019).

A priori, o dispositivo legal apresentado tipificou criminalmente um ato que até então não possuía previsão legal, todavia, devido ao contexto em que a lei foi criada, onde a vítima se tratava de pessoa pública e por isso houve pressão popular, a Lei foi criada às pressas, e por isso apresenta algumas características passíveis de crítica. O caput do dispositivo condiciona o crime somente à casos de violação de mecanismos de segurança, ou seja, para que se configure crime, a vítima deve ter um antivírus, senhas, ou outros dispositivos que ofereçam segurança, caso contrário, a invasão não será punida (FERREIRA, 2021).

Mesmo que passível de críticas, com o advento da Lei 12.737, a população passou a ficar amparada pela Lei em alguns casos específicos de ataques informáticos e, talvez o ponto principal, iniciou uma gama de debates focados na área de crimes cibernéticos, campo jurídico que até então era uma espécie de “terra sem lei”.

5.2 Principais dispositivos legais aplicáveis aos crimes cibernéticos

Após a Lei nº 12.737/12, uma das principais legislações brasileiras que tratam sobre o uso da internet corresponde à Lei nº 12.965/14, conhecida como Marco Civil da Internet. Esse dispositivo legal estabelece princípios, garantias, direitos e deveres relacionados ao uso da internet no território brasileiro, a fim de assegurar a inviolabilidade e sigilo das interações privadas de seus usuários.

A lei nº 12.965 serve como regulamento para a utilização dos serviços derivados do uso da internet, buscando resguardar a proteção dos direitos individuais de seus usuários de forma que também garanta a segurança e estabilidade da rede. Todavia, a mesma não tipificou criminalmente novas condutas derivadas do uso de aparatos informáticos.

No ano de 2015, foi promulgada a Lei nº 13.185, denominada Lei Anti-bullying. Esta lei visa o combate ao bullying e a proteção das crianças e adolescentes no ambiente virtual, onde estabelece mecanismos de denúncia e ajuda para atos de violência e assédio virtual.

Outro grande marco legislativo para a garantia de seguridade virtual dos usuários da internet, foi a promulgação da Lei nº 13.709/18, Lei Geral de Proteção de Dados (LGPD), que embora não seja exclusivamente foca à crimes cibernéticos, ela dispõe de regulamentos a serem seguidos sobre a coleta e armazenamento de dados

pessoais pelas entidades privadas, com foco na proteção da privacidade de seus usuários.

5.3 Evolução legislativa quanto ao crime de estelionato virtual

O Código Penal de 1940 foi pioneiro na tipificação criminal para o crime de estelionato no território brasileiro. O código anterior penalizava condutas de falsificação de documentos públicos ou privados, porém não possuía uma abordagem tão abrangente se comparado ao artigo 171 do Código Penal vigente. Dito isso, com a promulgação do código penal brasileiro de 1940, o estelionato passou a ser criminalizado no Brasil. Desde então, este dispositivo legal sofreu algumas alterações, mas sua essência permaneceu a mesma.

Apesar das modificações implementadas a partir da Lei Carolina Dieckmann, o número de casos envolvendo crimes virtuais continuou a crescer, especialmente durante o período de Pandemia do COVID-19, indicando que as ações tomadas pelo poder legislativo não surtiram o resultado pretendido. Ciente da alta no número de casos, em 2021 foi sancionada a Lei nº 14.155, que promoveu alterações no Código Penal, introduzindo a modalidade de fraude eletrônica em seu texto. Além disso, esta lei foi responsável por agravar a pena referente a prática de crimes cibernéticos (GALINDO, 2022).

No tocante ao crime de estelionato, após a promulgação da Lei nº 14.155/21, foram incluídos no corpo do artigo 171 do Código Penal o §2º-A, §2º-B e §4º, que dispõem o seguinte:

> 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 um a cinco anos, e multa
> § 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. (Incluído pela Lei nº 14.155, de 2021)
> § 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. (Incluído pela Lei nº 14.155, de 2021)
> Estelionato contra idoso ou vulnerável (Redação dada pela Lei nº 14.155, de 2021)

> § 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. (Redação dada pela Lei nº 14.155, de 2021)
> (BRASIL, 2021).

Infere-se, portanto, que, para o legislador brasileiro, as punições anteriormente aplicadas, eram ineficientes quanto à finalidade preventiva da pena, já que a mesma não desestimulava a prática do delito pelos infratores. Dessa forma, a solução encontrada foi no sentido de majorar a pena aplicada para os crimes cibernéticos. Observa-se ainda, que o aumento das penalidades são diretamente proporcionais ao aumento da dificuldade de identificação do malfeitor, já que por si só a pena em meio digital é mais grave, e ainda deve ser agravada para os casos em que o criminoso encontra-se em território internacional, conforme disposto no parágrafo 2º-B.

Outrossim, a Lei 13.964 de 2019, popularmente conhecida como pacote anti crime, inclui no texto do artigo 171 do Código Penal o parágrafo 5º, a saber:

> § 5º Somente se procede mediante representação, salvo se a vítima for: (Incluído pela Lei nº 13.964, de 2019)
> I - a Administração Pública, direta ou indireta; (Incluído pela Lei nº 13.964, de 2019)
> II - criança ou adolescente; (Incluído pela Lei nº 13.964, de 2019)
> III - pessoa com deficiência mental; ou (Incluído pela Lei nº 13.964, de 2019)
> IV - maior de 70 (setenta) anos de idade ou incapaz.
> (BRASIL, 2019).

O parágrafo quinto do artigo 171, Código Penal, incluí esse dispositivo legal no ramo das ações penais públicas condicionadas, isto é, não basta a prática delitiva para que o poder estatal inicie sua pretensão punitiva, mas sim uma condição anteriormente expressa em lei, no caso exposto seria a representação do ofendido, ou seja, uma espécie de autorização da vítima para que tenha início à ação penal (LOPES JR, 2021).

Por mais que esta alteração legislativa aparente não gerar consequências significativas, no ramo do estelionato cibernético ela se tornou pontual, visto que condicionar o início da investigação criminal ao interesse dos ofendidos, impede as forças policiais de tomarem medidas rápidas e eficazes no combate ao delito. Dessa forma, conforme exposto anteriormente, devido ao anonimato dos infratores e a constante evolução dos golpes digitais, caso o delito seja consumado, o atraso no início das investigações dificulta severamente sua eficácia.

É clara a permissibilidade que o ambiente virtual traz para a prática de crimes cibernéticos, onde as características dessa modalidade criminosa, como o anonimato dos infratores, propiciam sua impunidade. Todavia, o Estado deve estar preparado para garantir a eficácia de seus dispositivos legislativos, a fim de promover a paz dos indivíduos ofendidos (FELIX, NASCIMENTO, 2023).

6. CONSIDERAÇÕES FINAIS

A conjuntura social atual exige que as pessoas estejam conectadas ao ambiente virtual para a realização de diversas atividades. Nesse sentido, embora tenha proporcionado benefícios significativos aos usuários, esse cenário também contribuiu para o aumento nos crimes cibernéticos. Devido ao crescimento significativo tanto de usuários quanto de crimes que envolvem o ambiente virtual, surgem desafios significativos a serem enfrentados pelas autoridades policiais.

A pesquisa desenvolvida observou que a falta de punição para o crime de estelionato digital acarreta alguns impactos negativos na sociedade brasileira, dentre eles, o encorajamento de novos indivíduos embarcarem nesse ramo que, embora seja ilegal, é bastante lucrativo, e alimenta a insatisfação popular com os órgãos judiciários.

Os objetivos do estudo foram alcançados, visto que foi possível explanar as características do delito de estelionato digital, sua diferença com a modalidade tradicional, assim como a evolução legislativa e análise dos motivos que acarretam a impunição para esse crime.

Por mais que o Estado promoveu evoluções legislativas no tocante aos crimes cibernéticos, o número de casos de ataques virtuais continua a subir no território brasileiro, demonstrando que mesmo evoluída, a legislação vigente por si só não é suficiente para desencorajar os criminosos de praticarem o estelionato digital.

Para que seja instaurada uma medida inicial eficaz de combate aos crimes cibernéticos, a legislação deve ser amparada por uma investigação eficiente das instituições policiais. Todavia, a realidade é de sucateamento da polícia civil, órgão que enfrenta carência de servidores, onde muitas vezes um único profissional é submetido fica a cargos de várias obrigações distintas, além da falta de cursos de capacitação para que esses funcionários atuem de maneira incisiva nos casos em questão.

Esses fatores somados ao anonimato dos infratores, constante evolução dos golpes, facilidade de abertura de contas bancárias em nome de laranjas e necessidade de colaboração de instituições privadas na concessão de informações sobre os casos, agravam os obstáculos a serem superados pelos investigadores.

Assim, conclui-se, que esse estudo contribuiu para identificar as características e os principais problemas enfrentados na luta contra o estelionato cibernético, sendo isso o pontapé inicial para começar a traçar métodos eficientes de combate aos crimes digitais.

Dito isso, a fim de frear o crescimento de casos, as instituições financeiras devem estabelecer métodos mais rígidos de comprovação de identidade para abertura de contas bancárias, com o intuito de diminuir a ocorrência de contas laranja, podendo até estender a responsabilidade civil às entidades financeiras. Outrossim, pode-se instituir prazos mais rígidos de respostas das instituições privadas à ofícios emitidos pelos órgãos legais, no intuito de tornar as investigações policiais mais dinâmicas.

Diante de tais considerações, evidencia-se a necessidade premente de medidas eficazes para lidar com a falta de punição no contexto do crime de estelionato digital, dada sua influência direta nos mecanismos de segurança e confiança no ambiente virtual. É imperativo que o legislador e as instâncias responsáveis adotem estratégias que aprimorem a legislação existente e fortaleçam os meios de investigação e repressão, a fim de preservar a integridade da sociedade brasileira diante dos desafios impostos pelo avanço tecnológico.

Somente por meio de uma abordagem integral e colaborativa, envolvendo setores públicos e privados, será possível construir um ambiente digital mais seguro e protegido contra os impactos nefastos do estelionato digital, promovendo, assim, uma sociedade mais resiliente e protegida frente às nuances do cenário tecnológico em constante evolução.

REFERÊNCIAS BIBLIOGRÁFICAS

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

CAETANO, Guilherme. Estelionato digital explode no Brasil e cresce 500% em 4 anos. São Paulo, 28 de junho de 2022. Disponível em <https://oglobo.globo.com/brasil/noticia/2022/06/estelionato-digital-explode-no-brasil-e-cresce-500percent-em-4-anos.ghtml>. Acesso em: 28 out. 2023.

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

Cavalcanti, Gabriela Soares. Schonblum, Paulo Maximilian W M. Contas-corrente utilizadas como meio para instrumentalização de fraude: estudo de caso. Migalhas. 25 de mar. 2021. Disponível em: <https://www.migalhas.com.br/depeso/342345/conta-corrente-utilizada-como-meio-para-instrumentalizacao-de-fraude>. Acesso em: 05 nov. 2023.

Código Penal. Decreto-Lei 2.848, de 07 de dezembro de 1940. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 08 nov. 2023.

Conselho Nacional de Justiça. Um em cada quatro condenados reincide no crime, aponta pesquisa. Disponível em: <https://www.cnj.jus.br/um-em-cada-quatro-condenados-reincide-no-crime-aponta-pesquisa/>. Acesso em: 25 de out. 2023.

COPOBIANCO, Ligia. **A Revolução em Curso:** Internet, Sociedade da Informação e Cibercultura. Estudos em Comunicação nº7 - Volume 2, p. 175-193. São Paulo, 2010. Disponível em <https://ec.ubi.pt/ec/07/vol2/capobianco.pdf>. Acesso em 03 out, 2023.

COSTA, Francisco Lozzi da. **Limitações Constitucionais do Poder Punitivo do Estado**. Monografia de Conclusão de Curso (Pós graduando em Direito) – Curso de Direito, Faculdade de Direito de Presidente Prudente. Presidente Prudente, 2014.

DIAS, Vera Marques. **A problemática da Investigação do Cibercrime**. DATAVENIA. 2012. p. 63 – 88. Disponível em <https://www.datavenia.pt/ficheiros/pdf/datavenia01.pdf#page=63>. Acesso em 12 out. 2023.

DINIZ, F. F.; CARDOSO, J. R.; PUGLIA, E. H. P. O crime de estelionato e suas implicações na era contemporânea: o constante crescimento dos golpes via internet. **LIBERTAS DIREITO**, *[S. l.]*, v. 3, n. 1, 2022. Disponível em: https://www.periodicos.famig.edu.br/index.php/direito/article/view/215. Acesso em: 15 nov. 2023.

FELIX, Ysmara Padilha. NASCIMENTO, Yris Assíria Alves. **A vulnerabilidade dos idosos diante dos crimes cibernéticos**.2023. Trabalho de conclusão de curso (Graduação em Direito) – Curso de Direito, Universidade de Potiguar. Natal/RN, 2023.

FERNANDES, Alessandro. ZANI, João. Open Banking e Know Your Customer: Impactos da LGPD na veracidade de cadastros compartilhados pelas instituições financeiras. Revista da PGBC, v. 16, n. 2, p. 43 – 58, 2022. Art. 3. Disponível em: <https://revistapgbc.bcb.gov.br/revista/article/view/1161>. Acesso em: 03 out. 2023.

FERREIRA, MesakeMitrioni. OLIVEIRA, Talita Júnia Ramos. **Os Crimes cometidos no Ambiente Virtual e a Eficácia da Investigação Policial**. Artigo Científico (Bacharelando em Direito) – Curso de Direito, Centro Universitário UNA de Belo Horizonte. Belo Horizonte, 2023.

FERREIRA, Sarah Pereira. **Crimes Cibernéticos:** A ineficácia da legislação brasileira. Pontíficia Universidade Católica, Goiânia/GO, 2021. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/1709>. Acesso em: 09 nov. 2023.

FILGUEIRAS, Isadora Cavalli de Aguiar. LIMA, Thaís Soldera de. **CIBERCRIME**. ETIC 2015 – Encontro de Iniciação Científica. Disponível em <http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/5025/4818>. Acesso em 15 nov, 2023.

FREITAS, Larissa Ribeiro Carvalho de. **Crimes Contra a Honra em Ambiente Virtual:** O ato de condenação da geração z e sua ideia de invisibilidade. Trabalho de Conclusão de Curso (Bacharelando em Direito) – Curso de Direito, Universidade de Taubaté. Taubaté/SP, 2021.

HONÓRIO, Gustavo; PAIVA, Deslange; Stabile, Arthur. Estelionatos no Brasil mais que quadruplicam em cinco anos, e golpes virtuais disparam após pandemia, revela Anuário. São Paulo, 20 de julho de 2023. Disponível em <https://g1.globo.com/sp/sao-paulo/noticia/2023/07/20/estelionatos-no-brasil-mais-que-triplicam-em-cinco-anos-e-golpes-virtuais-disparam-apos-pandemia-revela-anuario.ghtml>. Acesso em: 28 out. 2023.

JÊIOR, Júlio César Alexandre.**CIBERCRIME**: UM ESTUDO ACERCA DO CONCEITO DE CRIMES INFORMÁTICOS. **Revista Eletrônica da Faculdade de Direito de Franca**, *[S. l.]*, v. 14, n. 1, p. 341–351, 2019. DOI: 10.21207/1983.4225.602.Disponível em: <http://revista.direitofranca.br/index.php/refdf/article/view/602.>. Acesso em: 13out. 2023.

LOPES JR., Aury. Direito Processual Penal - 18. ed. - São Paulo: Saraiva Educação, 2021.

MEDEIROS, WelberthRonine de. Finalidade da pena: Direito ao esquecimento. Revista Eletrônica do Ministério Público do Estado de Goiás, Goiânia, ano XVIII, n. 9, pág. 295-312, jul./dez. 2015.

MORAIS, Jair Antônio Raposo. **Análise dos índices de criminalidade frente aos delitos praticados no ambiente virtual**. 2021. Artigo Cientifico (Graduação em Direito) – Curso de Direito, Faculdade Evangélica de Goianésia. Goianésia/GO, 2021.

MOREIRA, Danilo. **E-commerce durante a pandemia e o aumento do estelionato digital**. 2022. Trabalho de Conclusão de Curso (Graduação em Direito) – Curso de Direito, Universidade São Judas, São Paulo, 2022.

NOGUEIRA, Flavio Mirã de Souza. NOLASCO, Loreci Gottschalk. **CRIMES CIBERNÉTICOS – DESAFIOS PARA O DIREITO**. Revista Jurídica Direito, Sociedade e Justiça/RJDSJ, São Paulo, v. 9, n. 16, Jan.-Jun./2022. Disponível em: <https://periodicosonline.uems.br/index.php/RJDSJ/article/view/6973/4907>. Acesso em: 08 de out. 2023.

OLIVEIRA, Caio Victor. **Fake News e discursos de ódio a partir das eleições de 2018:** A inépcia do Poder Judiciário em combater antes e durante o pleito eleitoral e a consequente incapacidade em reparar o dano. 2021. Trabalho de Conclusão de Curso – Curso de Direito, Universidade Federal de Campina Grande. Sousa/PB, 2021.

PEREZ, Fabíola. Brasileiros sofrem 208 golpes por hora; alta é de 37,9%. São Paulo, 20 de julho de 2023. Disponível em:<https://noticias.uol.com.br/cotidiano/ultimas-noticias/2023/07/20/puxado-por-golpes-eletronicos-estelionatos-sobem-379-homicidios-caem.htm#:~:text=Os%20estelionatos%20em%20meio%20eletr%C3%B4nicos,Catarina%2C%20com%201.249%2C7>. Acesso em: 01 nov. 2023.

PINHEIRO, R. PL institui a “Lei de segurança do PIX”. Senado Notícias. 2022. Disponível em: https://www12.senado.leg.br/noticias/audios/2022/02/pl-institui-a-201cleide-seguranca-do-pix201d. Acesso em: 13 out. 2022.
Superior Tribunal de Justiça. Recurso Especial nº 2.077.278 – SP (2023/0190979-8) Ministra Relatora Nancy Andrighi. São Paulo, julgado em 03 out. 2023.

RIBEIRO, Eliete da Silva. Crime de Estelionato – Uma análise da evolução sob a égide da impunidade na cidade de Manaus. 2019. Disponível em: <https://semanaacademica.org.br/system/files/artigos/crime_de_estelionato_-_uma_analise_da_evolucao_sob_a_egide_da_impunidade_na_cidade_de_manaus_eliete_da_silva_ribeiro_0.pdf>.

RIBEIRO, Gabriel Santos. **O Estelionato por Meios Digitais:** A problemática da responsabilização. Anais do XII Simpósio Internacional de Análise Crítica do Direito, Jacarezinho/PR, UENP, 2023, p. 111 – 125.

ROCHA, Glauco Capper. FILHO, Veridiano Barroso de Souza. **Da guerra às emoções**: história da internet e o controverso surgimento do Facebook. Alcar – Associação Brasileira de Pesquisadores de História da Mídia IV Encontro Regional Norte de História da Mídia – Rio Branco/AC – 19 e 20/05/2016, p. 1 – 16.

ROHDEN, SF; RODE, J. O impacto da experiência de consumo na percepção e no comportamento dos clientes do banco digital. **Revisão da Gestão do Varejo** , São Paulo (SP), v. 1, pág. e22, 2023. DOI: 10.53946/rmr.v3i1.22. Disponível em: <https://www.rmr.emnuvens.com.br/rmr/article/view/22>. Acesso em: 07 nov. 2023.

ROQUE, Sérgio Marcos. Criminalidade informática: crimes e criminosos do computador. São Paulo: ADPESP Cultural, 2007. P. 25.

ROXIN, Claus. Strafrecht. AllgemeinerTeil Band I: Grundlagen. Der Aufbau der Verbrechenslehre. 4. Auflage. München: C.H. Beck, 2006. (Há tradução para o espanhol da segunda edição, de Diego-Manuel Luzón Peña, Miguel Díaz y García Conlledo e Javier de Vicente Remesal. Derecho penal - parte general: Fundamentos. La estructura de lateoríadel delito. Madrid: Civitas, 1997.)

SILVA, Davi Castro. **A TEORIA DOS DIREITOS FUNDAMENTAIS E O BEM JURÍDICO PENAL:** Análise da vinculação da teoria do bem jurídico penal à Constituição com fundamento na dogmática dos direitos fundamentais. 2011. Dissertação (Mestrado em Direito Público) – Curso de Direito, Universidade Federal da Bahia, Salvador, 2011.

SIMAS, Diana Viveiros. **O Cibercrime**.2014. Dissertação (Mestrado em Ciências Jurídico-Forenses) – Curso de Direito, Universidade Lusófona de Humanidades e Tecnologias. Lisboa, 2014.

SINDPOL/MG, Sindicato dos Servidores da Polícia Civil do Estado de Minas Gerais. Situação de Sucateamento da Polícia Civil Motiva Pedido de Exoneração de Delegado. Belo Horizonte, 06 de junho de 2011. Disponível em: <https://sindpolmg.org.br/situacao-de-sucateamento-da-policia-civil-motiva-pedido-de-exoneracao-de-delegado/>. Acesso em: 05 nov. 2023.

SOUSA, Rodrigo de. **CIBERCRIMES:** O Uso da Internet como Instrumento Para a Prática de Delitos e a Evolução da Legislação Penal Brasileira no Combate aos Crimes Virtuais. Trabalho de Conclusão de Curso (Bacharel em Direito) – Curso de Direito. Três Pontas, 2022.

STUCKENBERG, Carl-Friedrich. As Deficiências Constitucionais da Teoria do Bem Jurídico. REVISTA ELETRÔNICA DE DIREITO PENAL E POLÍTICA CRIMINAL - UFRGS. VOL.2,N.º 1, p. 1 – 13, 2014. Disponível em: <https://seer.ufrgs.br/index.php/redppc/article/view/51810/31972>. Acesso em: 12 out. 2023.

TJDFT. Condenado por estelionato deverá restituir valores obtidos de forma maliciosa. Disponível em <https://www.tjdft.jus.br/institucional/imprensa/noticias/2019/marco/condenado-por-estelionato-devera-restituir-a-vitima-os-valores-obtidos-de-forma-maliciosa>. Acesso em 24/11/2023.

TJRJ. Instituição Financeira deve indenizar cliente por danos causados com vazamento de dados sensíveis. Disponível em <https://www.tjrj.jus.br/web/portal-conhecimento/noticias/noticia/-/visualizar-conteudo/5736540/194018251>. Acesso em 13 de novembro de 2023.