CESED - CENTRO DE ENSINO SUPERIOR E DESENVOLVIMENTO
UNIFACISA – CENTRO UNIVERSITÁRIO
CURSO DE BACHARELADO EM DIREITO

ANA LAURA SOARES VIEIRA

REPERCUSSÕES JURÍDICAS DO ESTELIONATO VIRTUAL QUANDO PRATICADO POR MEIO DAS REDES SOCIAIS

CAMPINA GRANDE - PB
2023

ANA LAURA SOARES VIEIRA

REPERCUSSÕES JURÍDICAS DO ESTELIONATO VIRTUAL QUANDO PRATICADO POR MEIO DAS REDES SOCIAIS

Trabalho de Conclusão de Curso - Artigo Científico - apresentado como pré-requisito para a obtenção do título de Bacharel em Direito pela UniFacisa – Centro Universitário
Área de Concentração: Direito Penal; Direito Processual Penal.
Orientador: Antônio Gonçalves Ribeiro Júnior.

CAMPINA GRANDE-PB
2023

Dados Internacionais de Catalogação na Publicação
(Biblioteca da UniFacisa)

XXXXX
Vieira, Ana Laura Soares.
Repercussões jurídicas do estelionato virtual quando praticado por meio das redes sociais / Ana Laura Soares Vieira. – Campina Grande-PB, 2023.

Originalmente apresentado como Artigo Científico de bacharelado em Direito da autora (bacharel – UniFacisa – Centro Universitário, 2023).
Referências.

1. Redes sociais. 2. Estelionato. 3. Responsabilização criminal I. Título.

CDU-XXXX(XXX)(XXX)
_____ Elaborado
pela Bibliotecária Rosa Núbia de Lima Matias CRB 15/568 Catalogação na fonte

Trabalho de Conclusão de Curso – Artigo Científico – Estelionato virtual: repercussões jurídicas do estelionato virtual quando praticado por meio das redes sociais, apresentado por Ana Laura Soares Vieira como parte dos requisitos para obtenção do título de Bacharela em Direito, outorgado pela UniFacisa – Centro Universitário.

APROVADO EM _____

BANCA EXAMINADORA:

_____
Prof. Antônio Gonçalves Ribeiro Júnior
Orientador

_____
Examinador

_____
Examinador

REPERCUSSÕES JURÍDICAS DO ESTELIONATO VIRTUAL QUANDO PRATICADO POR MEIO DAS REDES SOCIAIS

Ana Laura Soares Vieira [*]
Antônio Gonçalves Ribeiro Júnior [**]

RESUMO

No século XXI, a Internet passou a fazer parte do dia a dia dos cidadãos, principalmente através das redes sociais, que permitem aos usuários criar perfis, compartilhar informações e interagir. Em virtude da difusão da internet, houve uma alteração no *modus operandi* dos estelionatários, que passaram a utilizar as redes sociais enquanto meio para se conectar com as vítimas e obter vantagens ilícitas, caracterizando o chamado estelionato virtual. Atento às mudanças ocorridas, o legislador vislumbrou a necessidade de promulgar leis capazes de punir os agentes de acordo com a gravidade do delito, entrando em vigor a Lei n° 14.155, de 27 de maio de 2021, que adicionou os §§ 2°-A e 2°-B ao art. 171 do Código Penal. Neste contexto, partindo de uma pesquisa teórica, bibliográfica e, quanto aos objetivos, um estudo descritivo e explicativo, o presente trabalho objetiva estudar o crime de estelionato virtual, refletindo sobre a efetividade e adequação das leis existentes no ordenamento jurídico brasileiro para punir o delito. Busca-se também refletir sobre como se dá a conduta do estelionatário virtual e identificar as principais dificuldades enfrentadas pelas autoridades competentes para punir os infratores. A relevância da pesquisa reside na atualidade do tema, estabelecendo um debate acerca do papel da internet e das redes sociais enquanto meios facilitadores para a prática de crimes e sobre a dificuldade de identificar e punir os agentes que praticam o estelionato virtual.

Palavras-Chave: Redes sociais. Estelionato virtual. Responsabilização criminal.

ABSTRACT

In the 21st century, the Internet has become part of citizens' daily lives, mainly through social networks, which allow users to create profiles, share information and interact. Due to

[1*] Graduanda do Curso de Direito da UniFacisa – Centro Universitário. E-mail: vieiraanalaura71@gmail.com.
[2**] Professor Orientador. Especialista em Processo Civil e em Metodologia do Ensino Superior, professor de Processo Civil da UNIFACISA e Juiz de Direito do Tribunal de Justiça da Paraíba. E-mail agribeirojunior@yahoo.com.br.

the spread of the internet, there was a change in the modus operandi of the fraudsters, who started to use social networks as a means to connect with the victims and obtain illicit advantages, characterizing the so-called virtual fraud. Aware of the changes that have occurred, the legislator envisioned the need to enact laws capable of punishing agents according to the seriousness of the crime, coming into effect Law nº 14.155, of May 27, 2021, which added §§ 2°-A and 2°-B to art. 171 of the Penal Code. In this context, starting from a theoretical, bibliographical research and, regarding the objectives, a descriptive and explanatory study, the present work aims to study the crime of virtual fraud, reflecting on the effectiveness and adequacy of the existing laws in the Brazilian legal system to punish the crime. It also seeks to reflect on how the virtual fraudster behaves and identify the main difficulties faced by the competent authorities to punish offenders. The relevance of the research lies in the topicality of the topic, establishing a debate about the role of the internet and social networks as facilitators for the commission of crimes and on the difficulty of identifying and punishing agents who practice virtual fraud.

Keywords: Social networks. Virtual fraud. Criminal responsibility.

1 INTRODUÇÃO

O estelionato é um delito previsto no art. 171 do Código Penal, restando configurado quando o agente busca obter vantagem ilícita em prejuízo alheio através de uma conduta que induz ou mantém a vítima em erro, utilizando de artifício, ardil, ou outro meio fraudulento (BRASIL, 1940).

Apesar de o referido crime ser praticado e estar previsto enquanto ilícito antes da difusão da internet, verifica-se que as redes sociais criaram o espaço perfeito para a propagação em massa das condutas dos estelionatários, posto que ampliaram a capacidade de localizar e contatar as vítimas.

Neste contexto, estelionatários identificaram que a internet é o *locus* perfeito para encontrar e fazer novas vítimas, especialmente porque a identificação da autoria do delito se torna muito mais dificultosa, de modo que é mais custosa a punição da sua conduta pelo Estado.

Desse modo, o poder legislativo se viu obrigado a editar leis que fossem capazes de abarcar o estelionato virtual - a exemplo da Lei n° 14.155, de 27 de maio de 2021, que adicionou os §§ 2°-A e 2°-B ao art. 171 do Código Penal -, e os agentes estatais vislumbraram a necessidade de investimento em mecanismos tecnológicos que possibilitem a identificação dos criminosos, com vias a permitir sua investigação e posterior condenação.

Entretanto, a mera promulgação de leis não é suficiente para reprimir a conduta dos criminosos, já que as autoridades competentes muitas vezes acabam encontrando empecilhos à resolução do delito, que serão tratados ao longo do artigo em epígrafe.

Assim, partindo de uma pesquisa teórica, bibliográfica e, quanto aos objetivos, um estudo descritivo e explicativo, o trabalho em tela tem como objetivo principal estudar o crime de estelionato virtual, refletindo sobre a efetividade e adequação das leis existentes no ordenamento jurídico brasileiro para punir o delito.

Ademais, busca-se também refletir sobre como se dá a conduta do estelionatário virtual e identificar as principais dificuldades enfrentadas pelas autoridades competentes para punir os infratores.

Para alcançar os objetivos da pesquisa, parte-se dos seguintes questionamentos: a) As leis existentes no ordenamento jurídico brasileiro são adequadas para tipificar e permitir a punição dos estelionatários que praticam o delito através das redes sociais; b) De que forma o estelionatário virtual se utiliza das redes sociais para a prática do crime; c) Quais são as

principais dificuldades enfrentadas pelas autoridades para punir agentes que praticam estelionato virtual.

Para responder aos 3 (três) questionamentos, formulam-se as seguintes hipóteses: 1) Apesar de ser recente, a Lei n° 14.155, de 27 de maio de 2021 é extremamente importante, já que prevê a conduta da fraude eletrônica, também chamada de estelionato virtual, possibilitando a punição dos agentes com o rigor necessário; 2) Os criminosos se aproveitam da amplitude de acesso da internet e das redes sociais para identificar e abordar suas vítimas; 3) As principais dificuldades enfrentadas pelas autoridades são o anonimato, a ausência de uma jurisdição facilmente identificável e a ausência de provas, posto que as evidências podem ser facilmente apagadas ou modificadas.

Desta feita, a relevância da pesquisa reside na atualidade do tema proposto, estabelecendo um debate acerca do papel da internet e das redes sociais enquanto meios facilitadores para a prática de crimes e sobre a dificuldade de identificar e punir os agentes que praticam o estelionato virtual, seja pela inadequação legislativa ou pela ausência de capacidade técnica e de recursos necessários por parte das autoridades competentes.

2 CONCEITUAÇÃO E CARACTERÍSTICAS DO CRIME DE ESTELIONATO

O crime de estelionato possui previsão expressa no art. 171 do Código Penal, segundo o qual incorre no delito aquele que busca “Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento” (BRASIL, 1940).

Trata-se, portanto, de um crime patrimonial praticado mediante fraude, cuja pena é de reclusão, de um a cinco anos, e multa. Aqui, o agente ludibria a vítima para obter vantagem ilícita, praticando uma fraude.

O crime de estelionato tem como núcleo do tipo “obter”, ou seja, o agente alcança a vantagem indevida enganando a vítima que, por sua vez, contribui com o agente ativo do delito sem, contudo, notar que seu patrimônio está sendo lesado.

> Pune-se aquele que, por meio da "astúcia', "da esperteza", do "engodo", da "mentira', procura despojar a vítima do seu patrimônio fazendo com que esta entregue a coisa visada espontaneamente, evitando, assim, retirá-lo por meios violentos. Em suma, o agente busca lesar a vítima em seu patrimônio, de maneira sutil, mas sempre segura. A fraude pode ser empregada para induzir ou manter a vítima em erro. No ato de induzir (incutir) é o agente quem cria na vítima a falsa percepção da realidade. Já na manutenção, a própria vítima se encontra equivocada e o fraudador, aproveitando-se dessa circunstância, emprega os meios necessários para mantê-la nesse estado, não desfazendo o engano percebido. (CUNHA, 2016, p. 341)

Ao induzir a vítima, o agente cria uma situação que não condiz com a realidade, enganando-a. Além de criar, o autor do delito pode também manter a pessoa no erro em que se encontrava anteriormente, se aproveitando dele. Em ambos os casos, estará configurado o estelionato, que permitirá ao agente a obtenção da vantagem ilícita através de uma manifestação de vontade viciada da vítima.

O tipo penal menciona ainda os meios pelos quais o agente pratica o delito, sendo eles: a) Artifício; b) Ardil; c) Qualquer outro meio fraudulento.

Conforme Cleber Masson (2018, p. 749), o artifício se caracteriza pela fraude material, de modo que o autor usa algum instrumento para ludibriar a vítima. O autor exemplifica a situação da seguinte maneira: "'A' veste-se com o uniforme de uma oficina mecânica para que 'B' voluntariamente lhe entregue seu automóvel". Por outro lado, ele explica que ardil é a fraude moral, traduzida pela conversa enganosa, de modo que o autor do crime convence a vítima para obter vantagem indevida.

O art. 171 ainda informa que o delito pode ser praticado através de "qualquer outro meio fraudulento", trazendo uma previsão genérica que permite o alcance de uma gama maior de condutas.

Importante mencionar que se trata de um crime comum, uma vez que não se exige qualquer condição especial do sujeito ativo. Logo, qualquer pessoa pode praticar o estelionato. Do mesmo modo, o sujeito passivo (vítima) pode ser qualquer um que sofra a lesão ao patrimônio na forma descrita no tipo penal, podendo ser física ou jurídica (de direito público ou de direito privado).

Ademais, conforme entendimento pacífico do Supremo Tribunal Federal, o sujeito passivo pode ser tanto a pessoa enganada, quanto a prejudicada, ainda que uma seja ente público. Neste contexto, vejamos ementa de decisão do STF no julgamento do Habeas Corpus nº 84.735-8:

> EMENTA: PENSÃO RECEBIDA APÓS O FALECIMENTO DA PENSIONISTA. RECURSOS SOB A ADMINISTRAÇÃO MILITAR. COMPETÊNCIA DA JUSTIÇA MILITAR. ESTELIONATO. SUJEITO PASSIVO. Estelionato praticado por pessoa que, mediante assinatura falsa, se fez passar por pensionista falecida para continuar recebendo os proventos de pensão militar depositados no Banco do Brasil. Recursos sob a administração militar. Competência da Justiça Militar para processar e julgar a respectiva ação penal (artigo 9º, III, "a" do Código Penal Militar). **A jurisprudência do Supremo Tribunal Federal é pacífica no sentido de que o sujeito passivo, no crime de estelionato, tanto pode ser a pessoa enganada quanto a prejudicada, ainda que uma seja ente público**. Ordem denegada. (STF. HC n° 84.735-8. Relator: Ministro Eros Grau. Data de julgamento: 17/05/2005) (grifo nosso)

O estelionato é compatível com a coautoria e com a participação. Por outro lado, a vítima deve ser pessoa certa e determinada. Ainda, a vantagem obtida pelo agente ativo deve ser ilícita, ou seja, sem qualquer justificação legal, e precisa se caracterizar o prejuízo patrimonial do ofendido, lesando-o.

Não se admite, contudo, a modalidade culposa, posto que deve haver o dolo do agente no sentido de obter a vantagem. Além disso, é um crime material e instantâneo, cuja consumação somente ocorre quando há o prejuízo da vítima e a lesão ao patrimônio (MASSON, 2018).

Outrossim, admite-se a modalidade tentada e se procede mediante representação, excetuados os casos em que a vítima é a Administração Pública, direta ou indireta, criança ou adolescente, pessoa com deficiência mental, maior de 70 anos ou incapaz, hipótese em que será incondicionada, e, via de regra, a competência para processar e julgar é da Justiça Estadual comum. (BRASIL, 1940)

Há, também, as figuras equiparadas ao estelionato, previstas no § 2º do art. 171 do Código Penal, sendo elas a disposição de coisa alheia como própria, a alienação ou oneração fraudulenta de coisa própria, defraudação de penhor, fraude na entrega de coisa, fraude para recebimento de indenização ou valor de seguro, fraude no pagamento por meio de cheque e a fraude eletrônica, que será objeto de análise do presente trabalho.

Desse modo, apesar da relevância de todas as formas equiparadas acima colacionadas, o presente trabalho se debruça apenas sobre os § 2º-A e § 2º-B, que tratam da fraude eletrônica, tendo em vista o tema em estudo.

Para compreender o assunto proposto, é imprescindível que, inicialmente, seja objeto de análise as redes sociais, analisando suas peculiaridades e o papel que desempenham na prática do estelionato virtual para, em seguida, abordar os mecanismos jurídicos criados para coibir a prática delitiva.

3 REDES SOCIAIS COMO MEIO FACILITADOR PARA A PRÁTICA DE CRIMES

A história da internet é bastante complexa e envolve uma série de eventos e tecnologias que se desenvolveram ao longo de décadas. A Internet é uma rede global de computadores que permite a comunicação e o compartilhamento de informações em escala mundial. Sua história remonta à década de 1960, quando a Agência de Projetos de Pesquisa

Avançada do Departamento de Defesa dos Estados Unidos (ARPA) criou a ARPANET, uma rede de computadores que conectava universidades e centros de pesquisa (CASTELLS, 2003).

A ARPANET usava o protocolo de comunicação *Transmission Control Protocol/Internet Protocol* (TCP/IP), que se tornaria o padrão da Internet. Nos anos 1970, a ARPANET se expandiu para outras instituições governamentais e acadêmicas, e surgiram as primeiras redes de computadores internacionais (CASTELLS, 2003).

A Internet como a conhecemos hoje começou a se desenvolver na década de 1980, quando a *National Science Foundation* (NSF) dos Estados Unidos patrocinou a *National Science Foundation Network* (NSFNET), uma rede nacional de computadores que conectava instituições de pesquisa e universidades (LEMOS, 2003).

Contudo, foi apenas na década de 1990 que a Internet se difundiu, posto que a ARPANET foi desativada e a Internet tornou-se uma rede pública global, formando uma rede de computadores, momento em que os provedores montaram redes próprias, tomando por base o projeto da ARPANET (CASTELLS, 2003).

No século XXI, a Internet se tornou ainda mais importante enquanto ferramenta de comunicação e colaboração em todos os níveis. A partir de então, o uso da Internet se disseminou na sociedade, adentrando cada vez mais as residências dos cidadãos e passando a fazer parte do dia a dia deles.

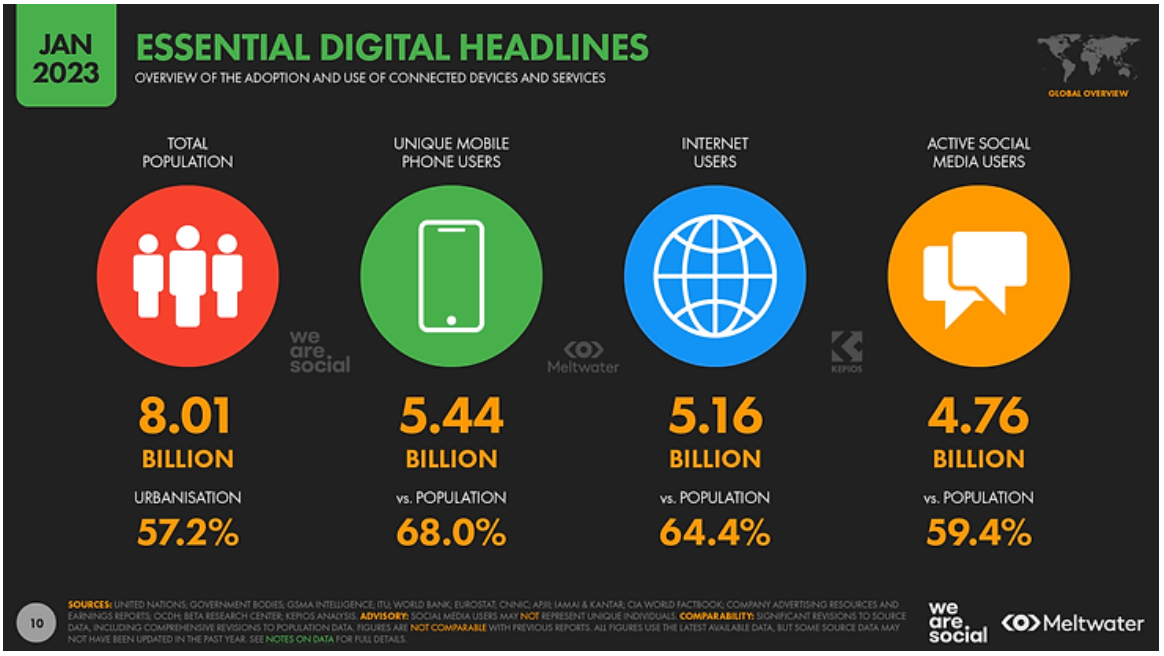
Neste contexto, surgiram as chamadas redes sociais, que são plataformas online que permitem aos usuários criar perfis, compartilhar informações, se conectar com outras pessoas e interagir através de mensagens, comentários ou outras formas de comunicação digital. A crescente popularidade das redes sociais e dos dispositivos móveis também mudaram drasticamente a forma como as pessoas usam a Internet e se comunicam entre si.

> Estamos em uma realidade em que hoje seria impensável viver sem a tecnologia, uma vez que está presente em todos os espaços do nosso desenvolvimento cotidiano comum. A tecnologia está presente em todas as atividades da nossa vida: no lar, nos veículos e nos transportes, em nossos locais de trabalho e de estudo, assim, fazendo parte ativa da revolução digital. Em suma, não se deve esquecer que a tecnologia existe para servir ao homem, para proporcionar uma vida mais fácil e agradável por meio de inovações tecnológicas que a melhore e a simplifique. (PINOCHET, 2014).

De acordo com o estudo realizado pelo "We Are Social e Hootsuite" (2021), empresa líder em gerenciamento de mídias sociais, que realizam curadoria de conteúdo, agendamento e publicação de postagens, existem cerca de 150 milhões de usuários de redes sociais no Brasil, o que corresponde a cerca de 70,3% (setenta vírgula três por cento) da população local.

São exemplos de redes sociais utilizadas do Brasil o Instagram, o Twitter, o Facebook, o Youtube e o Whatsapp.

Ainda conforme o "*We Are Social e Hootsuite*" (2023), 59,4% (cinquenta e nove vírgula quatro por cento) da população mundial utiliza as redes sociais e 64,4% (sessenta e quatro vírgula quatro por cento) acessa a internet. Segundo o estudo, o total global de usuários da Internet aumentou 1,9% (um vírgula nove por cento) nos últimos 12 meses:



Fonte: We Are Social e Hootsuite (2023)

Diante da relevância da Internet, seu acesso é garantido pelo artigo 7º da lei 12.965, de 23 abril de 2014, também conhecido como Marco Civil da Internet, segundo o qual o acesso à internet é essencial ao exercício da cidadania (BRASIL, 2014).

Entretanto, devido ao amplo uso da Internet, tornou-se recorrente a prática de crimes através das redes sociais, e com o delito de estelionato não foi diferente. As redes, ao facilitar e amplificar o acesso à informação e a interação social, também se tornaram um *locus* perfeito para a ação dos criminosos, que passaram a utilizá-las como um meio para encontrar e abordar suas vítimas.

Existem diferentes tipos de crimes que podem ser cometidos por meio das redes sociais. Alguns exemplos incluem o *cyberbullying*, em que o criminoso passa a assediar, intimidar, difamar ou ameaçar outras pessoas online, os golpes e fraudes através da criação de perfis falsos ou informações enganosas ou enganar as pessoas para obter informações pessoais, podendo ser tipificado enquanto pode crime contra a honra (calúnia, difamação ou

injúria, previstos nos arts. 138, 139 e 140 do Código Penal, respectivamente), o *stalking*, prática prevista no art. 147-A do CP, que consiste na perseguição reiterada, ameaçando a integridade física ou psicológica, restringindo a capacidade de locomoção ou invadindo ou perturbando a liberdade ou privacidade da vítima (BRASIL, 1940), e o estelionato virtual (art. 171, § 2º-A do Código Penal).

No contexto dos delitos praticados através da internet, o estelionatário, particularmente, é um dos criminosos que mais aproveitou a expansão da interação social propiciada pelas redes sociais para fazer novas vítimas, inovando na prática do delito, isto porque, ao utilizar a Internet para agir ilicitamente, dificulta a identificação da autoria do delito, tornando mais custosa a ação do Estado para puni-lo.

> "É o estelionato, como já ficou dito, forma de criminalidade evolutiva, crime do homem civilizado [ou do homo economicus] e que toma vulto com o progresso e o desenvolvimento. O mundo moderno oferece-lhe, dessarte, clima propício, pela multiplicidade de relações jurídicas que a expansão econômica e o desenvolvimento das atividades humanas impõem. Ora, o equilíbrio e a harmonia social exigem que essas relações se assentem sobre o pressuposto da boa-fé, e daí o objetivo particular da lei de tutelá-la, ameaçando com a pena as violações da lisura, da honestidade, que, como imperativo constante, deve reinar nas relações jurídicas [e econômicas], em torno das quais a vida hodierna se agita. Esse interesse é eminentemente social, pelo que somos dos que pensam que a tutela do dispositivo não se dirige tanto a proteger a boa-fé individual no negócio jurídico – já que aceitamos que o crime existe ainda que a vítima não se tenha havido com grande lisura – mas é inspirada no interesse público de reprimir de qualquer maneira a fraude causadora do dano alheio. (NORONHA, 1988, p. 362)

Desta forma, o estelionato virtual (ocorrido através da Internet), passou a ser praticado através da criação de páginas falsas, que visam obter vantagem ilícita patrimonial da vítima, por exemplo. Outra forma encontrada pelos criminosos para abordar suas vítimas, é o golpe do amor, conhecido como estelionato sentimental por meio do qual o agente se aproveita da afeição da pessoa enganada e a usa para obter vantagem financeira, utilizando-se de falsas promessas de casamento, entre outras.

É importante ressaltar que o uso das redes sociais para a prática de crimes não deve levar à demonização das próprias plataformas, posto que elas também desempenham um papel crucial na conectividade, disseminação de informações úteis e engajamento comunitário.

No entanto, é fundamental que as empresas proprietárias das redes virtuais e os usuários estejam conscientes dos riscos associados e tomem medidas para combater e prevenir o uso indevido e criminoso dessas plataformas. Isso pode incluir o estabelecimento de

políticas rigorosas de uso, denúncia de comportamentos criminosos às autoridades competentes e a conscientização contínua sobre os perigos existentes.

Verifica-se, portanto, que apesar de ser um ambiente muito benéfico para os indivíduos, facilitando o acesso a informações e conectando pessoas de todos os países, as redes sociais também se tornaram locais usados para a abordagem de vítimas por criminosos, por servirem enquanto meio para dificultar a identificação dos autores dos delitos e a punição pelo Estado.

Objetivando enfrentar e contornar as dificuldades para punir os agentes que praticam crimes através das redes sociais, o Legislador brasileiro visualizou a necessidade de modificar a lei, se adequando à Era Digital, de forma a possibilitar a aplicação das penas aos que violam as normas para obter vantagens ilícitas. Neste sentido, no próximo tópico serão abordadas a legislação concernente ao tema e as repercussões jurídicas correlatas.

4 DAS INOVAÇÕES PROMOVIDAS PELA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A lei nº 13.709, de 14 de agosto de 2018, também conhecida como Lei Geral de Proteção de Dados (LGPD) representa um marco no cenário de segurança jurídica em uma época digital, uma vez que traz penalidades para aqueles que, em posse de dados pessoais, possuem o dever de proteção dos "direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (BRASIL, 2018) e não o fazem corretamente.

Em virtude da previsão de multas e outras sanções administrativas previstas na Seção I do Capítulo VIII da LGPD, que incluem desde a advertência e a concessão de prazo para regularização até a proibição parcial ou total do exercício de qualquer atividade relacionada ao tratamento de dados (BRASIL, 2018), muitos criminosos passaram a utilizar a vulnerabilidade das empresas que não investem em sistemas de segurança para chantagear os gestores, conforme explica o artigo publicado pela FLOWTI (2021):

> Os cibercriminosos, viram na LGPD uma maneira a mais de pressionar as empresas a pagarem pelo resgate de dados. Ao invadirem os computadores das empresas e roubarem os dados críticos e pessoais de colaboradores, clientes e parceiros, eles expõem as falhas de segurança da informação da empresa, revelando uma falha na adequação às exigências da LGPD, abrindo caminho para a empresa ser multada pela Agência Nacional de Proteção de Dados. Geralmente, especialmente nos famosos ataques de Ransomware, os bandidos não fazem nada com os dados, apenas os mantêm em sua posse e bloqueiam o acesso aos dados. Assim a empresa acaba ficando refém do criminoso, que inicia a chantagem (FLOWTI, 2021).

Inspirada pela *General Data Protection Regulation*, ordenação europeia que visa a proteção dos mesmos direitos que a LGPD, a Lei nº 13.709/2018 inseriu no Ordenamento Jurídico Brasileiro normas que devem ser observadas na coleta e armazenamento de dados pessoais de pessoas naturais, dotando o procedimento de transparência e segurança (LOPES, 2021).

Com vistas a promover a fiscalização e aplicação das penalidades, foi instituída a Autoridade Nacional de Proteção de Dados Pessoais (ANPD), órgão indispensável para a consecução do objetivo da LGPD.

A legislação em comento tem especial relevância no contexto estudado, posto que o estelionato virtual poderia ocorrer também através do uso de dados vazados ou mal armazenados por empresas, facilitando a atividade criminosa.

Assim, ao prever penalidades e um órgão fiscalizador, a LGPD fomenta um comportamento mais cuidadoso daqueles que armazenam essas informações pessoais, sendo uma ferramenta importantíssima para a prevenção de crimes virtuais.

5 ESTELIONATO VIRTUAL

Conforme explicitado anteriormente, o estelionato virtual é uma forma de fraude que ocorre pela internet ou outras formas de comunicação eletrônica. Ele envolve a utilização de técnicas enganosas para obter informações pessoais e financeiras das vítimas, visando benefício próprio dos fraudadores.

Os criminosos que praticam o estelionato virtual utilizam uma série de métodos para enganar suas vítimas, desde a criação de sites falsos até a utilização de técnicas de *phishing* (fraude eletrônica que consiste em enganar os usuários para que prestem informações pessoais e financeiras confidenciais) por meio de e-mails e mensagens.

Outra forma de estelionato virtual é a criação de sites falsos, que se parecem com sites legítimos, mas na verdade são criados por fraudadores para enganar as vítimas. Esses sites falsos podem ser usados para coletar informações pessoais, como senhas e números de cartão de crédito, ou para vender produtos falsificados ou inexistentes.

Por se efetivar através da Internet, é muito mais dificultosa a identificação e a punição do agente criminoso. Neste sentido, quanto à autoria no estelionato virtual, o problema reside na identificação do delinquente, isto porque ele escondido por trás de uma rede virtual, diferentemente do criminoso comum, que está exposto (BIASOLI, 2010).

Atento às modificações na prática dos delitos promovidas pelo amplo acesso às redes sociais, o legislador brasileiro promulgou a lei n° 14.155, de 27 de maio de 2021, que alterou o art. 171 do Código Penal, incluindo os §§ 2°-A e 2°-B, tipificando a fraude eletrônica (SILVA; SANTOS, 2021).

Assim, o § 2°-A do art. 171 do Código Penal trouxe a figura do estelionato qualificado, também conhecido como estelionato majorado, que consiste em uma forma agravada do crime. Neste sentido, o estelionato qualificado se caracteriza pelo cometimento de crimes por meio de redes sociais, contatos telefônicos, envio de correio eletrônico ou por qualquer outro meio fraudulento (BRASIL, 2021).

Por outro lado, o §2°-B prevê o aumento da pena de 1/3 (um terço) a 2/3 (dois terços), se o crime de estelionato virtual for praticado mediante a utilização de servidor mantido fora do território nacional (BRASIL, 2021)

Para além das mencionadas alterações, a Lei em referência também inseriu o §4° no artigo 171, o qual prevê o aumento da pena de 1/3 (um terço) ao dobro, se o crime for cometido contra idoso ou vulnerável (BRASIL, 2021).

Assim, verifica-se que a referida Lei promoveu uma alteração extremamente relevante no Código Penal, visando coibir e punir os crimes praticados através da Internet, porém, ainda não produz resultados expressivos neste sentido, uma vez que a identificação dos autores é extremamente dificultosa nessa modalidade de delito.

> O número de esquemas tem crescido tanto que o Instagram, em novembro de 2018, se posicionou contra os perfis criminosos. O ambiente online acaba facilitando ações ilegais, por conta da dificuldade de rastrear o criminoso e a falta de informação dos internautas de como denunciar. Esses perfis são mais difíceis de identificar que do um Fake comum, pois eles agem como se fossem reais — postam fotos, legendas, Stories e informações que conferem legitimidade para o perfil, que pode ser pessoal ou institucional. Estima-se que o Instagram pode ter até 95 milhões de perfis falsos. (LUDGERO, 2020)

A punição dos crimes praticados através da internet é bastante desafiadora, principalmente devido à natureza virtual e globalizada da rede. As principais dificuldades enfrentadas pelas autoridades para punir os agentes podem ser resumidas da seguinte maneira: a) Anonimato (muitos criminosos usam pseudônimos ou identidades falsas na internet, o que dificulta sua identificação); b) Jurisdição (a internet não reconhece fronteiras físicas, o que torna difícil definir qual a jurisdição aplicável a um crime cometido na rede); c) Prova (as evidências dos crimes na internet são difíceis de serem coletadas e preservadas, pois podem ser facilmente apagadas ou modificadas); d) Velocidade (crimes na internet podem ser

cometidos e disseminados rapidamente, o que dificulta a ação das autoridades em coibir e investigar); e) Capacidade técnica (muitas vezes, os órgãos responsáveis pela investigação e punição desses crimes não possuem a capacidade técnica e os recursos necessários para lidar com a complexidade da tecnologia envolvida) (AMARAL, 2022).

Buscando averiguar as principais dificuldades das autoridades para punir quem pratica estelionato virtual, os estudiosos Daniela Regina Gabriel Machado e Sérgio Grott (2022) realizaram uma pesquisa, entrevistando o delegado-geral da Polícia Civil da cidade de Macapá-AP, Sr. Antônio Uberlândio de Azevedo Gomes. Vejamos:

> Ademais, Uberlândio informa que do ponto de vista do criminoso, há diminuição dos riscos inerentes à sua atividade, pois agindo por meio digital, evita a possibilidade de eventual confronto direto com as forças policiais de segurança pública e, por vezes, seu único instrumento para a prática delitiva consiste em um mero aparelho celular. Além disso, os crimes são cometidos à distância, em várias ocasiões, em outras unidades federativas, distantes da residência da vítima, o que dificulta tanto na notificação à Polícia Judiciária pela crença da vítima na impunidade, quanto à própria atividade investigativa, que demanda cooperação interestadual. Ainda de acordo com o delegado, outro ponto que merece destaque, é o acesso a telefones celulares por parte de criminosos que já estão cumprindo pena em presídios. Não raro, esses celulares são compartilhados entre vários detentos na mesma cela, o que também torna difícil a elucidação da autoria delitiva. (MACHADO; GROTT, 2022, p. 6)

Para tentar superar essas dificuldades, é importante que as autoridades sejam capacitadas e tenham recursos para investigar e punir esses crimes, além de promover a cooperação internacional para enfrentar a natureza global dos crimes na internet. Também é necessário que os usuários da internet estejam cientes dos riscos e adotem medidas de segurança para proteger suas informações.

Verifica-se, nesse sentido que, por ser um delito complexo, o estelionato virtual e os demais cibercrimes somente poderão ser coibidos através de uma conjunção de fatores, não bastando a mera existência de uma legislação adequada, de modo que é necessária a realização de investimento em tecnologia e recursos, o incentivo à cooperação internacional e interestadual, bem como a educação e conscientização dos usuários da internet, o monitoramento e a fiscalização das atividades criminosas na internet por parte das autoridades competentes, prevenindo a disseminação de conteúdos ilegais.

6 METODOLOGIA

Na intenção de obter uma compreensão pertinente do tema estudado e, paralelamente, realizar abordagens teóricas gerais ao estudo analítico-crítico, quanto à natureza, foi adotada a pesquisa teórica. Quanto ao procedimento, foi utilizada a pesquisa bibliográfica e, quanto aos objetivos, trata-se de estudo descritivo e explicativo.

Desta feita, visando compreender o tema, utilizou-se da bibliografia de autores renomados, a exemplo de Cléber Masson, Edgard Magalhães Noronha, Rogério Sanches Cunha e Manuel Castells, entre outros, construindo um estudo vasto e aprofundado do assunto proposto.

7 CONSIDERAÇÕES FINAIS

O presente artigo apresenta um estudo bibliográfico, teórico e, quanto aos objetivos, descritivo e explicativo, e se propôs a estudar o crime de estelionato virtual, refletindo sobre a efetividade e adequação das leis existentes no ordenamento jurídico brasileiro para punir o delito.

Para alcançar tal objetivo primário, foram cumpridos os seguintes objetivos secundários: refletir sobre como se dá a conduta do estelionatário virtual, bem como identificar as principais dificuldades enfrentadas pelas autoridades competentes para punir os infratores.

A partir das informações da pesquisa, observa-se que o crime de estelionato não é nenhuma novidade, estando tipificado no art. 171 do Código Penal, entretanto, em virtude das relações sociais estabelecidas através das redes sociais, em ampla escala, os estelionatários encontraram novos meios para inovar na prática do delito, se aproveitando especialmente do alcance e da oportunidade de encontrar novas vítimas.

A internet, enquanto forma de comunicação global e compartilhamento de informações em escala mundial, surgiu na década de 1960. Contudo, a internet como a conhecemos hoje somente se desenvolveu na década de 1980 e, apenas na década de 1990 se difundiu, tornando-se uma rede pública.

A partir de então, ano após ano o uso da internet foi aumentando e, no século XXI, ela se tornou a ferramenta de comunicação mais importante, tendo como grande expoente as redes sociais, que conectam pessoas e propiciam o compartilhamento veloz de informações.

Neste contexto, as redes sociais se revelam presentes e difundidas na sociedade, no Brasil, por exemplo, em 2021 existiam cerca de 150 milhões de usuários, o que corresponde a

cerca de 70,3% (setenta vírgula três por cento) da população local, conforme estudo realizado pelo "*We Are Social e Hootsuite*".

Em virtude do amplo uso da Internet e das redes sociais, cada vez mais os crimes passaram a ser praticados através dos meios virtuais, isto porque, além de facilitar e amplificar o acesso à informação e a interação social, também serviram como um meio para encontrar e abordar vítimas de forma mais "segura" para o criminoso que, ao utilizar a internet para agir ilicitamente, dificulta a identificação da autoria, tornando mais custosa a ação do Estado.

Deste modo, para contornar as diversas dificuldades para punir os agentes que praticam crimes através das redes sociais, o Legislador modificou o art. 171 do Código Penal, introduzindo os §§ 2°-A e 2°-B, tipificando a fraude eletrônica, que nada mais é que o estelionato virtual.

Apesar disso, verifica-se que a mera alteração legislativa e a existência de leis que tipifiquem corretamente a conduta não é suficiente para que o agente delituoso seja identificado e punido, isto porque a investigação dos crimes praticados através da internet é bastante desafiadora em virtude do anonimato dos criminosos, que usam pseudônimos ou identidades falsas, das dificuldades de definir qual a jurisdição aplicável a um crime cometido na rede, de obter as provas necessárias, já que as evidências podem ser facilmente apagadas ou modificadas, bem como devido à velocidade de cometimento e disseminação dos crimes cometidos virtualmente, à ausência de capacidade técnica e recursos dos órgãos responsáveis pela investigação e punição.

Neste esteio, para contornar os problemas explicitados, as autoridades devem ser capacitadas e receber recursos suficientes para desempenhar suas funções adequadamente, sendo imprescindível também que ocorra o incentivo estatal à cooperação internacional para enfrentar a prática dos delitos virtuais, atentando-se para sua natureza global.

Além das iniciativas mencionadas, deve ocorrer uma conscientização dos usuários, de modo que estejam cientes dos riscos e adotem medidas de segurança para se proteger, devendo o Estado promover o monitoramento e a fiscalização das atividades criminosas na internet, prevenindo e coibindo a disseminação de conteúdos ilegais.

REFERÊNCIAS

AMARAL, Jean Carlos Rossafa do. **Crimes cibernéticos e as dificuldades no processo de investigação para os crimes na internet**. 2022. Disponível em: <https://conteudojuridico.com.br/consulta/artigo/58454/crimes-cibernticos-e-as-dificuldades-no-processo-de-investigao-para-os-crimes-na-internet>. Acesso em: 22 abr. 2023.

BIASOLI, Luiz Carlos de Sales. **Da necessidade de tipificação do crime de estelionato praticado na internet**. 2010. Disponível em: < https://conteudojuridico.com.br/consulta/Monografias-TCC-Teses-E-Book/19147/da-necessidade-de-tipificacao-do-crime-de-estelionato-praticado-na-internet>. Acesso em: 12 abr. 2023.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília, DF: Centro Gráfico, 1988.

_____. **Decreto-Lei nº 2.848, de 7 de setembro de 1940. Código Penal.** Rio de Janeiro, RJ, 7 set. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 18 abr. 2023.

_____. **Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF, 23 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 18 abr. 2023.

_____. **Lei nº 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 24 out. 2023.

_____. **Lei nº 14.155, de 27 de maio de 2021.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm>. Acesso em: 22 abr. 2023.

CASTELLS, Manuel. **A galáxia da internet:** Reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003.

CUNHA, Rogério Sanches. **Manual de direito penal**: Parte especial (arts. 121 ao 361). 8. ed. rev., ampl. e atual. Salvador: Juspodvim, 2016.

FLOWTI. **A importância da LGPD no combate aos cibercrimes.** 2021. Disponível em: https://flowti.com.br/blog/a-importancia-da-lgpd-no-combateaos-cibercrimes. Acesso em: 20 out. 2023.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. 5. ed. São Paulo: Atlas, 1999.

LEMOS, André. **Cibercultura e mobilidade:** A era da conexão. Disponível em: < https://facom.ufba.br/ciberpesquisa/andrelemos/cibermob.pdf>. Acesso em: 10 abr. 2023.

LOPES, A. M. **Direito Digital e LGPD na Prática**. São Paulo: Editora Rumo Jurídico, 2021.

LUDGERO, Paulo Ricardo. **O que são Scammers? Entenda a fraude**. 2020. Disponível em: <https://ludgeroadvocacia.jusbrasil.com.br/artigos/883306590/o-que-sao-scammers-entendaa-fraude>. Acesso em: 15 abr. 2023.

MACHADO, Daniela Regina Gabriel Machado; GROTT, Sérgio. **Estelionato virtual:** Uma análise da prática e repressão desse crime na cidade de Macapá-AP, entre os anos de 2018 a 2021. 2022. Disponível em: < http://periodicos.ceap.br/index.php/rcmc/article/view/149/92 >. Acesso em: 23 abr. 2023.

MASSON, Cleber. **Direito penal:** parte especial, arts. 121 a 212. 11. ed. rev., atual. e ampl. São Paulo: MÉTODO, 2018.

NORONHA, Edgard Magalhães. **Direito penal**. 23. ed. São Paulo: Editora Saraiva, 1988.

PINOCHET, L. **Tecnologia da Informação e Comunicação**. Rio de Janeiro: Grupo GEN, 2014. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788595153196/>. Acesso em: 13 abr. de 2023.

SILVA, Francielly Juliana; SANTOS, Ramon João Marcos dos. **O estelionato praticado por meio da internet:** Uma visão acerca dos crimes virtuais. 2021. Disponível em: < https://repositorio.animaeducacao.com.br/bitstream/ANIMA/18080/1/TCC%2001.12.21%20dep%C3%B3sito%20final.pdf>. Acesso em: 23 abr. 2023.

WE ARE SOCIAL E HOOTSUITE - DIGITAL 2021 [RESUMO E RELATÓRIO COMPLETO]. **AMPER**, 25 de fevereiro de 2021. Disponível em: <https://www.amper.ag/post/we-are-social-e-hootsuite-digital-2021-resumo-e-relat%C3%B3rio-completo>. Acesso em: 21 abr. 2023.

WE ARE SOCIAL E HOOTSUITE - DIGITAL 2023 [RESUMO E RELATÓRIO COMPLETO]. **AMPER**, 25 de janeiro de 2023. Disponível em: < https://www.amper.ag/post/we-are-social-e-hootsuite-digital-2023-visao-geral-global-resumo-e-relatorio-completo>. Acesso em: 21 abr. 2023.