

ESTELIONATO VIRTUAL CONTRA IDOSOS E SUA VULNERABILIDADE NO CIBERESPAÇO: ANÁLISE DAS RESPONSABILIDADES CÍVEIS E CRIMINAIS APLICÁVEIS AOS CASOS

VIRTUAL FRAUD AGAINST THE ELDERLY AND THEIR VULNERABILITY IN CYBERSPACE: ANALYSIS OF THE CIVIL AND CRIMINAL RESPONSIBILITIES APPLICABLE TO THE CASES

Artigo submetido em 21 de novembro de 2023

Artigo aprovado em 30 de novembro de 2023

Artigo publicado em 5 de dezembro de 2023

Cognitio Juris

Volume 13 - Número 52 - Dezembro de 2023

ISSN 2236-3009

Autor(es):

Karine Raquel Sousa Ascenso Rosa [1]

Ênio Walcácer de Oliveira Filho [2]

RESUMO: Este estudo explora a vulnerabilidade dos idosos diante do estelionato virtual, examinando os avanços tecnológicos e os desafios na identificação dos criminosos. O objetivo principal é avaliar a eficácia das medidas de prevenção e combate ao estelionato

virtual direcionado a idosos e pessoas vulneráveis. Os objetivos específicos incluem uma análise histórica do surgimento do estelionato na era digital, a avaliação do artigo 171 § 2º A do Código Penal, e a compreensão do papel da Convenção de Budapeste no auxílio à identificação e punição dos estelionatários. O estudo aborda também as mudanças na legislação e jurisprudência brasileiras relacionadas ao estelionato, oferecendo uma visão abrangente das transformações ao longo do tempo. Destaca-se a análise do impacto do ciberespaço no aumento dos casos de estelionato, revelando as interconexões entre a tecnologia e a prática desse crime. A metodologia adotada é a pesquisa bibliográfica, proporcionando uma análise aprofundada com base em fontes confiáveis. A combinação desses elementos busca contribuir para a compreensão da complexidade do estelionato virtual, especialmente quando direcionado a grupos mais vulneráveis da sociedade. Ao final, com base em toda a pesquisa, ficou constatado que toda a evolução da legislação e sua revolução ao passar dos anos contribuíram para que os idosos fossem amparados de forma especial pela lei.

Palavras-chave: ciberespaço; estelionato; idoso; internet; virtual.

ABSTRACT: This study explores the vulnerability of the elderly to cyberstalking, examining technological advances and the challenges in identifying criminals. The main objective is to evaluate the effectiveness of measures to prevent and combat cyber fraud targeting the elderly and vulnerable people. The specific objectives include a historical analysis of the emergence of fraud in the digital age, an evaluation of Article 171 § 2 A of the Penal Code, and an understanding of the role of the Budapest Convention in helping to identify and punish fraudsters. The study also addresses the changes in Brazilian legislation and case law relating to fraud, offering a comprehensive view of the transformations over time. It highlights the impact of cyberspace on the increase in cases of fraud, revealing the interconnections between technology and the practice of this crime. The methodology adopted is bibliographical research, providing an in-depth analysis based on reliable sources. The combination of these elements seeks to contribute to understanding the complexity of

virtual fraud, especially when it targets the most vulnerable groups in society. In the end, based on all the research, it was found that all the evolution of legislation and its revolution over the years have contributed to the elderly being protected in a special way by the law.

Keywords: cyberspace; fraud; elderly; internet; virtual.

INTRODUÇÃO

Sabe-se que os avanços tecnológicos, são de fato benéficos para diversos fins e tem contribuído para a qualidade de vida e otimização do tempo das pessoas, com maior eficiência e produtividade dos serviços, comunicação instantânea por meio das redes sociais, acesso à informação contribuindo para a democratização do conhecimento e para a educação, facilidade de acesso a serviços financeiros e avanços na ciência e na pesquisa. No entanto, os riscos de segurança que essa infinidade de serviços eletrônicos proporcionam a seus usuários tem crescido cada vez mais com a banalização das informações prestadas nos ambientes virtuais, comprometendo a privacidade das pessoas, tendo em vista a coleta de dados que as empresas usam para o cadastro de seus usuários.

Tendo em vista o crescimento dos serviços no meio digital, a sociedade encontra-se cada vez mais rendida ao uso de serviços nesse meio. E, tratando-se dos riscos de segurança possíveis, o grupo que será usado como objeto de estudo neste trabalho, se encontra em desvantagem em relação às demais pessoas, considerando a falta de familiaridade com a tecnologia em razão do acesso limitado, tornando-as mais vulneráveis a golpes fraudulentos.

A problemática tem como base a vulnerabilidade das pessoas idosas e com baixo nível de escolaridade diante do crime de estelionato no contexto dos avanços tecnológicos e nas dificuldades de identificação dos agentes do crime para puni-los da forma adequada, tendo em vista a alta gama de experiência dos agentes criminosos no âmbito virtual.

O objetivo geral deste artigo é verificar a eficácia das medidas de prevenção e combate aos

casos de estelionato virtual direcionado a idosos e vulneráveis, e para isso, urge a necessidade de entender a caracterização do crime e como este se desenvolveu ao longo dos anos e com a chegada da era digital, analisar os instrumentos de cooperação para a criação de medidas de segurança, identificar as principais artimanhas utilizadas pelos agentes do crime para chegarem ao seu objetivo final e os obstáculos enfrentados pelas autoridades judiciais para identificar esses agentes.

1- DO SURGIMENTO DO CRIME DE ESTELIONATO

Embora o estelionato tenha se adaptado aos avanços tecnológicos e se intensificado na era digital, sua origem remonta a tempos antigos, muito antes do surgimento dessas tecnologias.

A prática do engano e da fraude sempre esteve presente na história da humanidade. Segundo Estefam (2023) a denominação da palavra “estelionato” surgiu do nome “stellio”, que se referia a um lagarto que mudava de cor para enganar suas vítimas, daí surgiu o paralelo, que relacionou a prática biológica do inseto com as práticas fraudulentas e a intenção de obter benefícios em desfavor de outrem.

Ao passar dos tempos, de década para década, a tipificação do crime foi se moldando e incorporando um rol taxativo em sua composição.

O Código Penal francês de 1810 incriminava a obtenção ou tentativa de obtenção de vantagem patrimonial, por meio de manobras fraudulentas. [...] O Código Criminal do Império (1830) adotou o nomen juris “estelionato”, prevendo várias figuras, além da seguinte descrição genérica: “todo e qualquer artifício fraudulento, pelo qual se obtenha de outrem toda a sua fortuna ou parte dela, ou quaisquer títulos” (BITENCOURT, 2020, pág. 158).

No código penal republicano de 1890, o capítulo IV abarca o *estelionato, abuso de confiança e outras fraudes*, e o elemento presente em todos eles é o “enganar”, sempre visando a obtenção de vantagem em dinheiro ilícita em desfavor de alguém para que lhe fosse dado a

referida vantagem (de boa fé por parte da vítima que foi enganada). O art 5º do referido capítulo do código, traz um exemplo claro do que foi dito anteriormente “Usar de artificios para surprehender a boa fé de outrem, iludir a sua vigilância, ou ganhar-lhe a confiança; e induzindo-o a erro ou engano por esses e outros meios astuciosos, procurar para si lucro ou proveito”. (BRASIL, 1890)

1.1- DA TIPIFICAÇÃO DO CRIME DE ESTELIONATO NA ATUALIDADE

No ordenamento jurídico brasileiro, o crime de estelionato está tipificado no art. 171 do Código Penal “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” sendo que, nas mesma pena incorre outros delitos, entre eles, a fraude eletrônica.

§ 2º-A. a pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo (Brasil, 2023)

Desta feita, resta claro que o bem jurídico tutelado é do patrimônio e sua inviolabilidade, que está assegurado na constituição de 1988 no rol de direitos fundamentais presentes no art 5º, que no inciso XXII diz: “é garantido o direito de propriedade”; e no inciso XXIII: “a propriedade atenderá a sua função social”. Ou seja, ninguém pode ter seu patrimônio, que faz parte da sua propriedade, violados por outrem, sendo dever do estado, a proteção deste patrimônio.

Há de se observar que a lei do crime de estelionato não apenas defende a figura ofendida, que teve seu patrimônio violado, mas, age principalmente para punir os autores do crime.

O crime de estelionato — destacava Manzini — “não é considerado como um fato limitado à agressão do patrimônio de Tício ou de Caio, mas antes como manifestação de delinquência

que violou o preceito legislativo, o qual veda o servir-se da fraude para conseguir proveito injusto com dano alheio, quem quer que seja a pessoa prejudicada em concreto. O estelionatário é sempre um criminoso, mesmo que tenha fraudado em relações que, por si mesmas, não merecem proteção jurídica, porque sua ação é, em qualquer caso, moral e juridicamente ilícita. (BITENCOURT, 2020, pág. 159)

Continuando a ideia anteriormente evidenciada, cumpre falar sobre os sujeitos desta relação. De um lado, tem-se o sujeito ativo, aquele que comete o crime, podendo ser qualquer pessoa, sem nenhuma condição especial, e do outro, tem se o sujeito passivo, aquele que sofre a lesão patrimonial, podendo ser uma pessoa física ou jurídica.

Cumpre ressaltar que o crime de estelionato somente existe na modalidade dolosa, não se admitindo a mera culpa do agente. Desta forma, necessita-se que o agente tenha a intenção e a consciência do prejuízo que causa a outrem para obter a vantagem ilícita.

APELAÇÃO. ESTELIONATO. RECEPÇÃO. SENTENÇA ABSOLUTÓRIA. RECURSO DO MP. CONDENAÇÃO. IMPOSSIBILIDADE. AUSÊNCIA DE PROVAS ACERCA DO DOLO NO ESTELIONATO. IN DUBIO PRO REO. RECEPÇÃO. INEXISTÊNCIA DE CRIME ANTERCEDENTE. ATIPICIDADE. ATIPICIDADE DA CONDUCTA. RECURSO CONHECIDO E DESPROVIDO. I - Inviável a condenação pelo crime de estelionato, quando não comprovado o dolo preordenado na conduta do réu, ou seja, a intenção manifesta no momento do ajuste, de enganar a empresa com o propósito de obter proveito econômico ilícito. II - Não havendo prova firme da autoria delitiva, deve ser aplicado o princípio in dubio pro reo, para absolvição do acusado. III - O crime de recepção é acessório, sendo necessária a prova de crime anterior para sua tipificação. No caso, não comprovada a origem ilícita dos objetos, porquanto não demonstrado o delito de estelionato, deve ser mantida a absolvição pela atipicidade da conduta. IV - Recurso conhecido e desprovido. (TJ-DF 0000499-16.2017.8.07.0002, Relator: NILSONI DE FREITAS CUSTODIO, Data de Julgamento: 10/09/2020, 3ª Turma Criminal, Data de Publicação: Publicado no DJE : 23/09/2020 . Pág: Sem Página Cadastrada.)

Assim, resta claro que um dos requisitos para a caracterização do crime é o dolo, não havendo a tipificação do crime de estelionato em que o agente tenha agido com mera culpa ao causar o engano por parte da vítima.

1.1.1- Da necessidade de representação da vítima

Desde tempos antigos, o crime de estelionato não exigia que a vítima expressasse seu desejo de processar o autor, sendo automaticamente passível de denúncia pelo Ministério Público. Isso o caracterizava como um crime de ação penal pública incondicionada à representação da vítima. Contudo, a situação mudou com a implementação do pacote anti-crime (Lei 13.964/19). Agora, em geral, a ação penal está sujeita à representação da vítima, conforme estabelecido no texto da lei, com apenas algumas exceções, conforme o texto do próprio art. 171 do CP.

§ 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. (Incluído pela Lei nº 13.964, de 2019)

Após as alterações legislativas em questão, houve incerteza por parte de muitos quanto à possibilidade de aplicação retroativa da lei em benefício do réu em processos já em andamento antes da implementação do pacote anti-crime.

Todavia, a partir do julgamento do HC 180.421/SP, de relatoria do Ministro Edson Fachin,

ocorrido em 22/6/2021, a Segunda Turma decidiu pela retroatividade da necessidade de representação da vítima nas acusações em andamento por estelionato, crime em relação ao qual a Lei 13.964/2019 alterou a natureza da ação penal para condicionada à representação da vítima (§ 5º do art. 171 do Código Penal). (STF, 2023, online)

Conforme citado acima, o Supremo Tribunal Federal (STF) já consolidou o entendimento de que a lei não retroagirá para beneficiar os réus já condenados, mas apenas como condição de procedibilidade para os casos em que ainda não foi oferecida denúncia, ou nas ações em que ainda não houve trânsito em julgado. Desta forma, caso a vítima não ofereça a denúncia no prazo de 30 dias a contar do conhecimento do fato, haverá a decadência.

2. DO CIBERESPAÇO E O UNIVERSO VIRTUAL

Sabemos que o ciberespaço é uma realidade, repleta de informações e redes que conectam pessoas independentemente de suas localizações. Reconhecemos, entretanto, que mesmo se dedicássemos uma vida inteira à sua exploração, ainda não seríamos capazes de desvendar todas as suas complexidades. Assim, quando questionados sobre o que é o ciberespaço e onde ele reside, provavelmente nossa mente nos trará uma definição simplificada. Isso ocorre porque o ciberespaço é uma presença constante, sempre presente, independentemente de estarmos ativamente envolvidos com ele ou não.

Suas múltiplas facetas continuam a se expandir em camadas cada vez mais profundas e, embora não seja tangível, ele é visível para nós. Pode ser considerado como um universo paralelo, onde existe uma realidade própria que pode variar entre o real e o imaginário. Essa percepção ajuda a explicar por que o conceito de ciberespaço está presente tanto na literatura quanto na ciência, apesar de que em ambas, os conceitos se casam e formam a definição do que é esse “mundo de informações” que é o ciberespaço.

Segundo Lévy (2001) a dinâmica imaterial do ciberespaço está intrinsecamente ligada ao avanço das forças produtivas do sistema capitalista, que incessantemente buscam acelerar o

fluxo de capital e transações comerciais em escala global. Isso, por sua vez, demanda significativos investimentos em tecnologia da informação. As manifestações das técnicas no atual estágio de produção do espaço social se materializam em sistemas de satélites, extensas redes de cabos de fibra ótica, data centers, inovações contínuas em software e hardware, e representam preocupações fundamentais em diversos campos da ciência e disciplinas acadêmicas que se dedicam a compreender esses elementos associados ao ciberespaço.

Neste sentido, pode-se considerar que o ciberespaço é um meio essencial para a promoção da globalização nacional, visto que facilita a promoção dos negócios em maior proporção entre os países.

No entanto, apesar dos inúmeros benefícios que o ambiente virtual proporciona aos seus usuários, como a conectividade global, acesso à informação, comércio eletrônico, acesso à informação, entretenimento, e também servir de um espaço onde as pessoas podem se expressar dentro dos limites da lei, o ciberespaço traz consigo suas mazelas e a principal delas é a quantidade de delitos ali dentro perpetrado, o que podemos chamar de cibercrimes, apesar de existir outros termos que classificar as condutas delituosas.

Rossini (2004) classifica em uma de suas obras, utilizando a terminologia “delito informático”, que é possível conceituar a ação como a conduta que se enquadra nos parâmetros típicos e ilícitos de um crime ou contravenção penal, que pode ser dolosa ou culposa, realizada por pessoa física ou jurídica. Essa conduta ocorre com o uso de meios de informática, seja em um ambiente conectado à rede ou fora dele, e, de alguma forma, prejudica a segurança da informática, que engloba elementos como integridade, disponibilidade e confidencialidade.

2.2- DO ESTELIONATO NO CIBERESPAÇO

Com o avanço da tecnologia, os criminosos encontraram uma oportunidade para cometer

uma ampla gama de delitos sem que pudessem ser identificados, e com uma alta diversidade de informações e facilidade para que isso se concretizasse.

Além da facilidade em praticar o ato em si, os delituosos contam com a vantagem de poder praticá-los em qualquer lugar, a qualquer momento. Para isso, eles contam com a vantagem e a facilidade em manusear os meios tecnológicos. E, à medida em que a segurança das redes de computadores ou sistemas bancários são reforçados contra ataques cibernéticos e roubo de informações, eles se especializam na prática de decodificar os sistemas que serão invadidos.

Hacker e cracker são agentes distintos. Hacker, em inglês, significa “fuçador”. O termo aponta aquele que possui alta habilidade técnica para lidar com sistemas de computação ou comunicações em rede. Na verdade, o hacker procura invadir máquinas de terceiros para satisfazer seu próprio ego, como se fosse para vencer o desafio tido como invencível. Sua intenção não costuma ir além de fuçar determinado sistema. Podemos dizer que a conduta do hacker, se fosse tipificada com a ideia acima, seria um crime de mera conduta, já que não apresenta nenhuma lesão efetiva a um bem jurídico. Na maioria das vezes o hacker invade sistemas informáticos alheios apenas para provar que é capaz de tal proeza. Seria, hipoteticamente, uma “invasão de domicílio moderna”. Cracker, ou pirata digital, é a pessoa especialista em sistemas informatizados, que invade sistemas alheios, sem autorização. Porém, seu objetivo é adulterar programas e dados, furtar informações e valores e praticar atos de destruição deliberada. O cracker destaca-se por ser autor de grandes fraudes eletrônicas, que causam expressivos prejuízos a usuários privados e às instituições públicas. (Conte, Fiorillo, 2016, pág 62)

De acordo com Ataíde (2017) o crime de estelionato virtual ocorre quando os infratores, por meio de links, e-mails falsos e outros meios digitais, buscam ocultar sua identidade e prometem realizar ações que sabem ser impossíveis, muitas vezes em troca de vantagens financeiras. Em resumo, o estelionato virtual se concretiza ao iludir a vítima,

fazendo uso de recursos digitais e explorando as vulnerabilidades que esses meios oferecem para obter benefícios.

É inegável que o crime de estelionato virtual existe tendo em vista os inúmeros casos já registrados até então. No entanto, não existe na legislação o termo “estelionato virtual”, assim, muitos infratores acabam encarando a falta do termo, como uma brecha na lei para cometer os delitos na internet como se ali fosse uma espécie de “manto protetor”. No entanto, de acordo com CRUZ e RODRIGUES (2018) Os crimes cometidos com o uso da internet são passíveis de tipificação, e sempre que os autores desses crimes são identificados, eles estão sujeitos a punições legais. O que pode levar alguns a acreditar na impunidade é a ausência explícita da palavra “internet” nas leis, mas, independentemente dos meios empregados, se um indivíduo realizar ações que se enquadrem nas características do crime de estelionato, conforme estipulado no artigo 171, ele estará sujeito às penalidades previstas para esse crime.

Até meados dos anos 2000, quando os meios tecnológicos ainda não tinham tanta relevância na vida dos brasileiros, o ciberespaço ainda não contava com muitas restrições, dessa forma, era uma espécie de “terra sem lei”.

Conforme o entendimento de Loveluck, a partir desse ponto, impulsionado pelos avanços tecnológicos e sua crescente integração no cotidiano, juntamente com a proliferação de ferramentas que simplificam a vida dos usuários e o aumento de influência política e econômica, o estado iniciou a adoção de mecanismos destinados a regular o ciberespaço, consolidando seu papel regulatório. Isso ocorreu devido ao surgimento de empresas virtuais, o que, por sua vez, sobrecarregou o sistema judiciário com um grande número de litígios envolvendo essas empresas. Dessa forma, surgiu a necessidade imperativa de estabelecer supervisão nesse novo ambiente. Entretanto, a regulamentação do ciberespaço por meio da lei penal, embora existam leis específicas em muitos casos, frequentemente se revela ineficaz por conta de alguns fatores, um deles é devido à complexidade em identificar os

usuários.

O princípio end-to-end, já explanado, traz como consequência a falta de instrumentos confiáveis de autenticação de usuários, a grande liberdade de utilização do ciberespaço para qualquer fim e a possibilidade publicação com grande alcance (global) em tempo real sem qualquer tipo de controle prévio. Acrescente-se que, *prima facie*, o protocolo TCP/IP não exige, por si só, que o usuário seja identificado antes de transmitir informações, que não há como saber o endereço físico de uma conexão (endereços de IP são lógicos e não físicos, sem determinação de localização geográfica) e que não é possível saber o que o usuário está fazendo em um dado momento, visto que, como dito, o protocolo TCP/IP apenas envia pacotes de dados por meio da Rede sem verificar o conteúdo (LEONARDI, 2019, p. 45)

A ausência de fronteiras geográficas no ciberespaço tem sido um desafio constante na aplicação da lei desde os primeiros casos de delitos virtuais até os dias de hoje, tendo em vista que, os crimes cometidos online não respeitam barreiras nacionais, o que complica significativamente a jurisdição e a aplicação das leis.

Nesse contexto, o sistema jurídico recorre à colaboração de normas de direito penal internacional para enfrentar esses desafios, como por exemplo, por meio de tratados internacionais que desempenham um papel essencial na regulamentação e resolução de conflitos legais no espaço digital. Eles estabelecem diretrizes compartilhadas entre nações, permitindo a harmonização das leis e a cooperação para lidar com crimes cibernéticos que transcendem fronteiras nacionais.

2.2.3- Da convenção de budapeste

Com o crescente aumento de crimes por meio das redes de computador, surgiu a necessidade de que fosse firmado um tratado que tratasse do tema, com o objetivo de cooperação entre os estados para que fossem criadas leis internas como meio de combate aos crimes cibernéticos e visando soluções mais rápidas e eficazes. Então, no dia 23 de

novembro de 2001, foi firmado em Budapeste, a convenção sobre o crime cibernético. Sendo promulgado no Brasil, no dia 12 de abril de 2023, por meio do Decreto Nº 11.491, assinado pelo então Vice-presidente da república Geraldo Alckimin. Para fins de esclarecimento, segundo o art. 1, alínea a da Convenção sobre o crime cibernético (2001) o termo “computador” designa qualquer aparelho ou um conjunto de aparelhos interconectados ou relacionados entre si que asseguram, isoladamente ou em conjunto, pela execução de um programa, o processamento eletrônico de dados.

O respectivo tratado citado acima, não trata especificamente sobre o crime de estelionato, no entanto, é recomendado que sejam criados, dentro da leis internas dos países signatários, medidas para tipificar como crime atos praticados com a intenção de lesar alguém por meio da rede de computadores, tais como: Acesso ilegal, interceptação ilícita, violação de dados, interferência em sistema, uso indevido de aparelhagem, falsificação informática e fraude informática. Todos os artifícios citados acima, são utilizados como meio de obter vantagem ilícita ao patrimônio de outras pessoas por meio das redes de computadores. A convenção também traz em seu corpo, a responsabilidade penal da pessoa jurídica diante dos casos tipificados como crime. Ao final, é acordado entre os países a forma em que se estabelecerá a extradição nos casos tipificados como crime, a assistência mútua em relação a medidas cautelares e a assistência mútua em relação a poderes investigativos.

Seguindo as descobertas de Boiteux (2004) a referida convenção foi desenvolvida não apenas com o intuito de instituir novos delitos, mas também para definir regulamentos do processo penal, harmonizando práticas do direito penal internacional e negociando acordos relacionados à tecnologia da informação, assim estabelecendo um regime rápido e efetivo de cooperação internacional.

Ao buscar harmonizar práticas do direito penal internacional, a convenção demonstra uma abordagem colaborativa e integradora. Essa busca por harmonização não apenas promove a eficácia das medidas legais, mas também reforça a ideia de uma comunidade global

interconectada, onde a cooperação é essencial para enfrentar questões jurídicas complexas e transfronteiriças, como o crime objeto deste estudo.

3- EVOLUÇÕES NA LEGISLAÇÃO E NA JURISPRUDÊNCIA BRASILEIRA ACERCA DO CRIME DE ESTELIONATO

Neste capítulo, serão apresentados os projetos de lei que visavam alterar o texto do artigo 171 do Código Penal, juntamente com a evolução dessas propostas ao longo dos anos.

De início, vale tratar sobre o Projeto de Lei do Senado de nº 76/2000 com a seguinte Ementa: Define e tipifica os delitos informáticos, e dá outras providências. O objetivo central do projeto era estabelecer como crime o uso indevido da informática, bem como a violação da inviolabilidade de dados e sua comunicação. Isso implicava criminalizar a retirada de informações privadas de bancos de dados, atos que ameaçam a vida e a integridade física das pessoas, crimes contra o patrimônio fiscal, ofensas à moral pública e a segurança nacional. Exemplos disso incluem a adulteração ou divulgação de informações declaradas como reservadas por razões de segurança nacional. O protocolo legislativo teve início no dia 27/03/2000, e restou prejudicado no dia 09/07/2008. O processo foi arquivado dois meses após essa data, no mesmo ano.

Em seguida, no mesmo ano, o projeto de lei do Senado nº 137/ foi protocolado, visando estabelecer novas penalidades para os crimes cometidos com o uso de tecnologia da informação e telecomunicações. No entanto, esse projeto de lei também restou prejudicado e foi arquivado no ano de 2008.

Em 2003, foi iniciado o projeto de lei na Câmara que promoveu alterações no Decreto-Lei nº 2848, de 07 de dezembro de 1940 - Código Penal, bem como na Lei nº 9296, de 24 de julho de 1996. Esse projeto foi finalmente promulgado como lei no ano de 2012, sofrendo um veto parcial, resultando na criação da Lei nº 12.735 de 30/11/2012.

Mesmo após essas alterações na legislação vigente, não foi incluído no texto que tipifica o crime de estelionato a expressão “Estelionato virtual”, fato esse que ainda nos dias de hoje gera controvérsias na aplicação da lei.

Em 2014, um marco significativo foi estabelecido na regulamentação da internet no Brasil com a promulgação da Lei nº 12.965/14, conhecida como o “marco civil da internet”. Essa legislação revolucionária delineou princípios, garantias, direitos e deveres que moldaram o cenário digital contemporâneo. Fundamentada no respeito à liberdade de expressão, a lei estabelece diretrizes para a atuação da União, Estados, Distrito Federal e municípios nesse domínio. Os pilares fundamentais dessa legislação incluem a salvaguarda da liberdade de expressão, comunicação e manifestação de pensamento, conforme preconizado pela Constituição Federal. Além disso, o “marco civil da internet” reforça a importância da proteção da privacidade e dos dados pessoais, alinhando-se estritamente às disposições legais pertinentes. Ao enfatizar a garantia da liberdade de expressão, a legislação não apenas estabelece parâmetros claros para a atuação dos diversos entes federativos, mas também promove um ambiente digital mais seguro e transparente. Nesse contexto, a proteção da privacidade e dos dados pessoais assume papel crucial, assegurando que o uso da internet respeite não apenas os princípios legais, mas também os direitos individuais dos usuários.

Assim, o “marco civil da internet” emerge como uma peça legislativa essencial, redefinindo as bases para a interação online no Brasil e destacando a importância da liberdade, privacidade e proteção de dados no ambiente digital contemporâneo.

Posteriormente a isso, no ano de 2018, foi aprovada a Lei nº 13.709/2018, conhecida por Lei Geral de Proteção de Dados, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL,2018)

A LGPD, Lei Geral de Proteção de Dados, trouxe disposições que regulam o tratamento de dados pessoais por pessoas físicas e jurídicas, com foco na defesa de direitos fundamentais, como intimidade, privacidade, segurança, propriedade, reputação e dignidade, conforme previsto no art. 5º da Constituição Federal. Ela estabelece regras para a coleta e processamento de dados pessoais, promovendo a transparência nas relações entre indivíduos e empresas. Além disso, a LGPD é aplicável em todo o território brasileiro, assegurando a segurança dos dados pessoais da população. Isso evidencia que a LGPD teve um impacto significativo nas responsabilidades de órgãos e empresas no que diz respeito à coleta e segurança de dados pessoais, contribuindo para mitigar riscos de cibercrimes.

3.1- DO ESTELIONATO CONTRA A PESSOA IDOSA E SUA VULNERABILIDADE NO CIBERESPAÇO

Com o advento da Lei nº 13.228/2015 que alterou o texto do art. 171 do Código Penal, trazendo causa de aumento de pena para o crime cometido contra pessoas idosas, que de acordo com o art. 1º da Lei nº 10.741/2003 são pessoas de idade igual ou superior a 60 (sessenta) anos, quem cometer o crime de estelionato contra pessoas dessa faixa etária ou pessoas consideradas como vulneráveis responderá pelo crime com a majorante de $\frac{1}{3}$ (um terço) ao dobro da pena. (BRASIL, 2015).

Esse amparo se deu principalmente devido às disposições trazidas na Lei nº 10.741/2015, que dispõe no art. 10 que “ É obrigação do Estado e da sociedade assegurar à pessoa idosa a liberdade, o respeito e a dignidade, como pessoa humana e sujeito de direitos civis, políticos, individuais e sociais, garantidos na Constituição e nas leis.”

De acordo com o estudo de Cardoso (2023), em 28 de maio de 2021, uma nova lei foi oficialmente publicada no Diário Oficial da União, introduzindo um aumento nas penas para crimes virtuais cometidos contra idosos. De acordo com pesquisas conduzidas pela Federação Brasileira de Bancos, houve um alarmante aumento de 60% nos crimes contra idosos durante o período da pandemia.

Esse fenômeno se desencadeou devido à própria natureza isolante da pandemia. No caso dos idosos, essa solidão se agravou, pois muitos deles já estavam enfrentando o isolamento social como parte de sua rotina. As causas do isolamento da pessoa idosa na sociedade são variadas, mas em sua maioria ocorre em razão da diminuição de sua produtividade em meio aos tempos atuais, tanto por conta da idade avançada, como em razão da falta de conhecimento das novas ferramentas do mercado de trabalho, incluído a rede de internet e seus similares.

À medida que o isolamento se tornou mais severo, as redes sociais se transformaram em uma forma de companhia para aqueles que, devido à falta de interação social, já se viam distantes da convivência com a sociedade em geral. No entanto, a carência de conhecimento tecnológico, em especial pela falta de familiaridade com a evolução da internet, tornou os idosos mais vulneráveis a golpes e enganações nas plataformas de redes sociais, e o que deveria ser apenas um meio de distração para eles, por vezes acaba resultando em sérios danos patrimoniais.

4- CONCLUSÃO

Este artigo aborda de maneira central o estelionato virtual direcionado a idosos no ambiente digital, ressaltando a vulnerabilidade dessa faixa etária no ciberespaço. A pesquisa explora como os idosos são alvos frequentes de crimes cibernéticos, examinando as implicações legais para os infratores e destacando medidas de responsabilização no âmbito cível e criminal. Esse enfoque é motivado pela crescente incidência de crimes cibernéticos contra os idosos, especialmente o estelionato virtual, devido à vulnerabilidade dessa parcela da população e às dificuldades enfrentadas com os avanços tecnológicos.

Para uma compreensão mais aprofundada, foram estabelecidos quatro objetivos específicos. O primeiro deles, apresentado no capítulo 1, oferece uma análise histórica do crime de estelionato, percorrendo as diferentes formulações legais ao longo do tempo, desde o Código

Penal francês de 1810 até o decreto lei nº 2.848 de 1940, que trouxe a definição legal do crime de estelionato no art. 171 do CP. Este delineamento histórico serve como base para o segundo objetivo específico, que consiste em analisar o artigo 171 § 2º A do Código Penal e compreender como a Convenção de Budapeste, um tratado internacional do qual o Brasil é signatário, pode contribuir para identificar e punir estelionatários.

No decorrer da análise, foram identificados fatores cruciais relacionados à contribuição da Convenção de Budapeste. A tipificação de atos relacionados ao estelionato virtual entre os países signatários é um desses fatores, assim como a responsabilidade penal da pessoa jurídica, possibilitando a responsabilização de empresas por práticas fraudulentas ligadas ao estelionato virtual. O tratado também estabelece regras para a extradição nos casos tipificados como crime, facilitando a transferência de indivíduos acusados de estelionato virtual entre os países signatários. Além disso, prevê assistência mútua em relação a medidas cautelares e poderes investigativos, promovendo uma cooperação eficaz entre as autoridades dos países envolvidos. O terceiro objetivo específico desta pesquisa concentrou-se na análise das evoluções na legislação e na jurisprudência brasileira referentes ao crime de estelionato. Ao longo do estudo, constatou-se que ao passar dos anos houve iniciativas significativas para modificar a legislação, buscando estabelecer novas penalidades para o uso indevido da informática. No entanto, dois dos primeiros projetos nesse sentido acabaram sendo prejudicados pela câmara do senado.

Apesar desses contratempos, ao longo do tempo, observaram-se alterações legislativas consideravelmente positivas no ordenamento jurídico brasileiro. É notável que, embora não tenha sido incluída no texto que tipifica o crime de estelionato a expressão “Estelionato virtual”, essas modificações contribuíram para aprimorar o sistema legal.

Finalmente, o ordenamento jurídico brasileiro foi enriquecido com a promulgação da lei nº 12.965/14, conhecida como o “Marco Civil da Internet”, e da lei nº 13.709/18, reconhecida como “LGPD – Lei Geral de Proteção de Dados”. Essas leis representam marcos significativos

na regulamentação da internet e na proteção dos dados, contribuindo para um ambiente jurídico mais robusto e alinhado com as demandas contemporâneas da sociedade digital.

Diante do exposto, evidencia-se que o ciberespaço não apenas serve como terreno fértil para o incremento dos casos de estelionato virtual, dada a sua condição central na proliferação desse delito, mas também se destaca como o epicentro da comunicação e conectividade globais. Essa dinâmica possibilita a interação entre indivíduos, independentemente de sua localização geográfica, enquanto a ampla disseminação de informações, o florescimento da economia digital e os impactos advindos da coleta e uso de dados online exacerbam ainda mais as condições propícias à prática criminosa.

Nesse contexto, os idosos, abordados de maneira específica ao longo deste estudo, emergem como uma parcela da sociedade particularmente suscetível aos avanços tecnológicos e à cotidiana onda de golpes virtuais. Diante dessa vulnerabilidade inerente, torna-se premente a consideração de medidas que visem à proteção desse grupo, sendo aumento de pena nos crimes perpetrados contra os idosos uma resposta necessária e fundamentada.

No percurso desta pesquisa, a metodologia bibliográfica se revelou instrumental na coleta e análise dos dados apresentados, proporcionando uma base sólida para as conclusões aqui delineadas. Dessa forma, este trabalho busca não apenas elucidar as ramificações do estelionato virtual, mas também oferecer subsídios para a reflexão e ação no sentido de mitigar os impactos nefastos desse fenômeno na sociedade contemporânea.

REFERÊNCIAS

ÂNGELO, T. **Ação por estelionato não pode seguir sem representação da vítima, decide Zanin**. Disponível em:

<<https://www.conjur.com.br/2023-ago-08/acao-estelionato-nao-seguir-representacao-vitima>>

. Acesso em: 10 out. 2023.

ATAÍDE, Amanda Albuquerque de. **Crimes Virtuais: uma análise da impunidade e dos danos causados às vítimas**. Maceió, 2017. Disponível em:<

http://www.faaiesa.edu.br/aluno/arquivos/tcc/tcc_amanda_ataide.pdf> . Acesso em:

20 out 2023.

BRASIL. **Constituição Federal**. Brasília: Senado Federal, 1988. Disponível em:

<http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm> . Acesso em: 23 jun. 2023.

BRASIL. **Decreto nº 11.491, de 12 de abril de 2023**. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Brasília, 12 de abril de 2023. Disponível em:

<https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm> . Acesso em: 23 jun. 2023.

BRASIL. **Decreto nº 847, de 11 de outubro de 1890**. Promulga o Código Penal. Sala das sessões do Governo Provisório, 11 de outubro de 1890, 2º da Republica. Disponível em:

<https://www.planalto.gov.br/ccivil_03/decreto/1851-1899/d847.htm> . Acesso em: 23 jun. 2023.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. In: **Diário Oficial da República Federativa do Brasil**, Brasília, DF, 23 de abr. 2014. Disponível em:

<https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> . Acesso em: 16 nov. 2023.

BRASIL. Superior Tribunal de Justiça - STJ. Recurso ordinário em habeas Corpus 226.632 .

AGRAVO REGIMENTAL NO HABEAS CORPUS. IMPETRAÇÃO DO MANDAMUS PARA DISCUTIR A ADMISSIBILIDADE DOS RECURSOS EXTRAORDINÁRIOS. FUNDAMENTO DA DECISÃO AGRAVADA NÃO INFORMADO. SÚMULA N. 182 DO SUPERIOR TRIBUNAL DE JUSTIÇA - STJ. RECURSO NÃO CONHECIDO. Relator: MIN. CRISTIANO ZANIN. Brasília-DF, 8 de agosto de 2023: Disponível em: <<https://www.conjur.com.br/dl/acao-estelionato-nao-seguir.pdf>> . Acesso em: 1 nov. 2023.

BRASIL. Tribunal de Justiça do Distrito Federal e Territórios. **Apelação criminal nº 0000499-16.2017.8.07.0002**. Relator: Desembargadora NILSONI DE FREITAS CUSTODIO. Brasília, 23 de setembro de 2020. Disponível em:

<https://jurisprudencia.s3.amazonaws.com/TJ-DF/attachments/TJ-DF_00004991620178070002_ff179.pdf?AWSAccessKeyId=AKIARMMD5JEA067SMCVA&Expires=1687493717&Signature=8MqgX806hqe36EuC7LaPUnFM%2BoI%3D> . Acesso em: 23 jun 2023.

BITENCOURT, Cezar Roberto. Capítulo XVIII ESTELIONATO. **Tratado de Direito Penal**: Parte Especial. 19. ed. São Paulo, 2023. p. 158, 159.

BOITEUX, Luciana. **Crimes informáticos**: Reflexões sobre a política criminal inseridas no contexto internacional atual. Revista Brasileira de Ciências Criminais. São Paulo: Revista dos Tribunais, 2004.

CABETTE, E. L. S. **Estelionato e representação: novo entendimento do STF**. Disponível em: <<https://meusitejuridico.editorajuspodivm.com.br/2023/05/02/estelionato-e-representacao-no-vo-entendimento-do-stf/>> . Acesso em: 16 out. 2023.

ESTEFAM, André. Capítulo VI DO ESTELIONATO E OUTRAS FRAUDES. **Direito**

Penal: Parte Especial. 10. ed. São Paulo, 2023. p. 238.

FIORILLO, C. A. P. ; CONTE, C. P. Capítulo 5 Delitos perpetrados no meio ambiente

virtual. **Crimes no Meio Ambiente Digital:** e a sociedade da informação. 2. Ed. São Paulo, 2016. p. 62

FIGUEIRÊDO, Simone de Sá Rosa; REIS, Elton Gomes. Poder e norma no ciberespaço. Revista Thesis Juris, 2022. Disponível em:

<<https://periodicos.uninove.br/thesisjuris/article/view/22684/9903>> Acesso em: 16 out. 2023.

LEONARDI, Marcel. **Fundamentos de direito digital.** São Paulo: Revista dos Tribunais, 2019.

LÉVY, Pierre. O que é o virtual?. Coimbra: **Quarteto**,2001.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal.** São Paulo: Memória Jurídica, 2004.

[1] Acadêmica de Direito na Faculdade Serra do Carmo- FASEC.

[2] Mestre em Prestação Jurisdicional e Direitos Humanos, especialista em Ciências Criminais e em Direito e Processo Administrativo. Graduado em Direito e em Comunicação Social, todos os cursos pela Universidade Federal do Tocantins (UFT). Professor de Processo Penal pela Fasec. Professor do curso de pós graduação em Ciências Criminais da UFT e de Processo Penal no curso de Pós Graduação da Idasp. Escritor de obras jurídicas. Delegado de Polícia Civil do Tocantins.