

DOS CRIMES CIBERNÉTICOS: UMA ANÁLISE DO CRIME DE ESTELIONATO PRATICADO PELA INTERNET

Letícia Hemerly de Moraes¹

Faculdade de Direito de Cachoeiro de Itapemirim

Izaias Corrêa Barboza Junior²

Faculdade de Direito de Cachoeiro de Itapemirim

RESUMO

Sem dúvidas, a internet é uma das maiores invenções do século XX, a partir do momento em que surgiu, permitiu o desenvolvimento de novos avanços tecnológicos que continuam evoluindo até os dias de hoje, transformando e facilitando o modo como nos relacionamos e vivemos, entretanto, com a expansão em larga escala, tem se tornado meio para que pessoas de má índole façam uso de forma indevida, utilizando-a para praticar os chamados crimes cibernéticos. O presente trabalho de conclusão de curso tem como objetivo discorrer sobre dos crimes cometidos através da internet, mais especificamente, no que se refere ao estelionato. De início, busca-se analisar os aspectos gerais da infração prevista no artigo 171 do Código Penal, bem como realizar uma breve análise sobre os demais crimes cometidos no ambiente virtual. Tem como foco principal o estudo do crime de estelionato virtual, abordando certas considerações gerais do delito, analisando o aumento do número de casos durante o período de isolamento imposto pela covid-19 e verificando a recente mudança suscitada pela Lei 14.155 de 2021, no supracitado crime. Para alcançar os objetivos, se fez necessário o uso de doutrinas, dispositivos contidos no Código Penal, artigos científicos, e também, pesquisas na internet. Ao final, pode-se concluir que o crime de estelionato virtual é aquele em que o agente utiliza-se dos meios digitais para obter vantagem ilícita em próprio benefício ou de outrem, induzindo ou mantendo a vítima em erro, por meio de artifício, ardil ou outro meio fraudulento, causando-lhe prejuízos. O aumento significativo do delito deve-se pelo fato do crescimento de usuários conectados a internet e a falsa sensação de impunidade. Apesar da alteração na Lei que versa sobre o crime em questão,

¹ Graduanda em Direito pela Faculdade de Direito de Cachoeiro de Itapemirim – FDCI. Correio eletrônico: lele_hemerly@hotmail.com

² Advogado. Graduado em Direito pela Faculdade de Direito de Cachoeiro de Itapemirim (1997). Professor da Faculdade de Direito de Cachoeiro de Itapemirim. Pós-graduado em Direito Civil e Processual Civil. Pós-graduado em Direito Processual Penal. Pós-graduado em Gestão Educacional. Pós-graduado em Ciências Criminais e Segurança Pública. Aluno do Curso Intensivo para Doutorado da Universidade de Buenos Aires. Correio eletrônico: izaiasadv@hotmail.com

restou demonstrado que o número de casos não diminuiu, tornando-a ineficaz até o momento.

Palavras-Chave: Estelionato. Crimes virtuais. Internet.

ABSTRACT

Without a doubt, the Internet is one of the greatest inventions of the 20th century. From the moment it first appeared, it allowed the development of new technological advances that continue to evolve to this day, transforming and facilitating the way we relate and live. However, with its large-scale expansion, it has become a means for malicious people to misuse it, using it to commit so-called cybercrimes. This final paper aims to discuss crimes committed over the Internet, more specifically, with regard to fraud. To begin with, it seeks to analyze the general aspects of the offense provided for in article 171 of the Penal Code, as well as to carry out a brief analysis of other crimes committed in the virtual environment. Its main focus is the study of the crime of cyber fraud, addressing certain general considerations of the crime, analyzing the increase in the number of cases during the period of isolation imposed by COVID-19 and verifying the recent change brought about by Law 14,155 of 2021, in the aforementioned crime. To achieve the objectives, it was necessary to use doctrines, provisions contained in the Penal Code, scientific articles, and also internet research. In the end, it can be concluded that the crime of cyber fraud is one in which the agent uses digital means to obtain illicit advantage for his own benefit or that of others, inducing or keeping the victim in error, through artifice, trickery or other fraudulent means, causing him losses. The significant increase in the crime is due to the growth of users connected to the internet and the false sense of impunity. Despite the change in the Law that deals with the crime in question, it was demonstrated that the number of cases did not decrease, making it ineffective to date.

Keywords: Fraud. Cybercrimes. Internet.

1 INTRODUÇÃO

É inegável que os avanços tecnológicos acarretaram em inúmeros benefícios para a sociedade moderna. Com o passar dos anos, os seres humanos estão cada vez mais dependentes desse tipo de ferramenta tornando-a essencial e indispensável para a vida cotidiana. Está presente desde as tarefas mais básicas como, por exemplo, estudar, se entreter, e até nas tarefas mais complexas, como fazer uma transferência bancária. Tudo isso se torna muito mais fácil, só é necessário um click e um dispositivo conectado a internet. Isso se deve com o advento do fenômeno mundial da *Globalização*, um processo de expansão econômica, política e cultural, tendo origem durante a época das grandes navegações, e que agora vem a ser cada vez mais extenso e abrangente, a nível mundial.

Porém, apesar de todas as vantagens, com o crescimento e o avanço da internet,

o meio virtual se tornou palco para a execução de diversos crimes, sendo estes chamados de crimes virtuais e também conhecidos, como crimes cibernéticos, crimes informáticos ou cybercrimes. Esses delitos podem assumir várias formas, desde infrações relacionadas a racismo e discriminação até crimes executados por meio de fraude realizados por indivíduos mal intencionados com o intuito de obter vantagens ilícitas em prejuízo de outrem por meio de indução ou manutenção deste em erro.

Vale mencionar, que com o surgimento e as medidas de restrições de contato físico impostadas pela pandemia do covid19, o número de casos envolvendo a prática desses crimes aumentaram significativamente, tendo em vista o longo período de isolamento social onde as pessoas se viram mais tempo em suas casas e ficaram ainda mais dependentes do uso dos aparelhos eletrônicos e do acesso à internet. Como efeito, os criminosos se aproveitaram desse período de fragilidade para atrair mais vítimas.

O tema em questão torna-se de suma importância em detrimento das constantes práticas de estelionato nos meios virtuais/digitais, e que em razão disso, tem sido um grande obstáculo para a atuação das autoridades policiais, sobretudo no que diz respeito à identificação do autor do crime e a grande dificuldade em se punir o criminoso. Desse modo, se tem a falsa sensação de impunidade, fato este que acarreta o crescimento do interesse pelos crimes virtuais.

Sendo assim, o presente artigo tem como objetivo discorrer a respeito dos crimes praticados através da internet, mais especificamente, no que se refere ao estelionato. De início, busca-se analisar os aspectos gerais do delito previsto no art.171 do Código Penal, bem como discorrer sobre a evolução das redes sociais e da internet, esclarecendo a sua importância para a sociedade atual e sua relevância no mundo.

O artigo também busca realizar uma breve análise sobre os demais crimes cometidos no ambiente virtual que também são considerados como cybercrimes. Tem como foco principal o estudo do crime de estelionato virtual, abordando algumas considerações gerais do delito, analisando o aumento do número de casos durante o período de isolamento imposto pela covid-19 e verificando a recente mudança trazida pela Lei 14.155 de 21, no supramencionado crime.

2 ASPECTOS GERAIS SOBRE O DELITO DE ESTELIONATO.

De início, far-se-á necessário realizar certas ponderações acerca da parte introdutória do crime de estelionato. Sem esse aspecto inicial, torna-se difícil o entendimento do que seria o estelionato virtual, assunto esse, que será tratado em tópico específico adiante. Logo, o presente tópico busca analisar aspectos gerais a respeito do crime em questão previsto no art.171 do Código Penal Brasileiro.

A palavra estelionato teve seu início na expressão grega *stellio*, que caracteriza uma espécie de lagarto que tem como peculiaridade a possibilidade de alterar a cor de sua pele para enganar suas presas. É possível observar que a origem da expressão estabelece uma correlação entre o animal supracitado e a conduta do indivíduo que pratica o crime de estelionato, o estelionatário, que por sua vez, se usa de artifícios arditos e fraudulentos para iludir alguém.

Ressalta-se que o ato de enganar não é uma conduta do homem atual, desde os tempos remotos e primórdios da humanidade, o ser humano já apresentava atitudes como essas. A Bíblia, no Livro de Gênesis, capítulo 27, relata o momento em que Jacó enganou seu pai, Isaque, se passando por seu irmão mais velho, Esaú, para receber a benção da primogenitura no lugar deste. Portanto, observa-se que o homem sempre se valeu da fraude para ocultar suas genuínas intenções, emoções, em outras palavras, para, de algum modo, esconder ou camuflar a verdade, com o propósito de obter vantagens, que teoricamente, lhe seriam indevidas (Greco, 2016, p. 844).

O estelionato retrata uma modalidade de crime patrimonial praticado mediante fraude, já que, o autor ao invés de usar a ameaça, violência à pessoa ou a clandestinidade, o mesmo se vale do engano ou o emprego para que a vítima, insensatamente, se deixa enganar, configurando, dessa forma, o delito em questão.

A figura típica fundamental do estelionato está previsto no art.171 do Código Penal (Brasil, 1940), punindo com pena de reclusão de um a cinco anos e multa, aquele que obtém, para si ou para outrem, vantagem ilícita, em prejuízo da vítima, a qual por sua vez, é induzida ou mantida em erro, mediante qualquer meio fraudulento.

Segundo Andreucci (2014) o estelionato é a obtenção da vantagem ilícita, para si ou para outrem, por meio da manutenção ou indução do indivíduo em erro, valendo-se de meios fraudulentos, modo ardil ou com o emprego de artifício. Nesse raciocínio, o criminoso, assegura a vantagem ilícita para si ou para alguém, através de diversas maneiras que manipulam a vítima, induzindo-a a erro.

Com a vigência da Lei nº 13.964/19, conhecida como pacote anticrime, à ação penal que anteriormente era de iniciativa pública incondicionada, passou a ser, em regra, pública condicionada à representação, salvo as exceções previstas no §5º do artigo 171 do Código Penal. Em resumo, sendo a fraude o ponto central do crime de estelionato, para a identificação e configuração deste são necessários quatro elementos que compõem o tipo penal, sendo eles: a ação do agente com o fim de obter vantagem ilícita, em prejuízo alheio; induzindo ou mantendo a vítima em erro, através de artifício, ardil, ou qualquer outro meio fraudulento, almejando vantagem ilícita para si ou para terceiro. (Greco, 2016).

Nessa perspectiva, chega-se a conclusão que o estelionato é um delito no qual o agente age de modo manipulador, ilude e engana a vítima, fazendo-a acreditar em situações ilusórias almejando de obter alguma vantagem patrimonial. Desse modo, a pessoa é induzida a entregar seus bens, objetos, valor em dinheiro ou qualquer outra coisa que possua valor econômico, de forma voluntária, presumindo, que o criminoso esteja agindo com honestidade.

3 DOS CRIMES CIBERNÉTICOS: UMA BREVE OBSERVAÇÃO A RESPEITO DOS CRIMES PRATICADOS POR MEIO DA INTERNET.

Escondidos em jogos online, rede sociais, aplicativos de mensagem e em outras plataformas da internet, os criminosos acentuaram o uso do meio virtual para fazerem mais vítimas, aplicando golpes, praticando injúrias, ameaças, extorsões e até pedofilia. Considerando o disposto no tópico anterior, não se pode negar que a internet tornou-se, com o passar dos anos, uma importante ferramenta para o cotidiano no mundo

globalizado. Porém, apesar de todos os benefícios, com a expansão da rede mundial de computadores os indivíduos, que a utilizam, perderam de forma parcial a sua privacidade, ficando sujeitos e vulneráveis a riscos por consequência da grande exposição nas redes. De acordo com Spinielli, a internet tem contribuído consideravelmente com o aumento dos chamados crimes informáticos, tendo em vista que serve como meio para a prática criminosa.

Segundo o Grupo de Combate aos Crimes Cibernéticos da Procuradoria da República no Estado de São Paulo (BRASIL, 2006), dezenas de tarefas podem ser realizadas através da internet como, por exemplo, pagar contas, trocar mensagens, participar de salas de bate-papo, “baixar” arquivos de música, imagem ou texto, comprar produtos, solicitar serviços, acessar sites contendo informações de interesse pessoal entre outras coisas. Contudo, essas atividades trazem riscos aos usuários, uma vez que, em dado momento podem encontrar indivíduos com segundas intenções capazes de se aproveitarem da grande escala e velocidade em que ocorrem as trocas de informações para praticar crimes.

Dessa forma, apesar de todos os benefícios e ao mesmo passo que a internet facilita e auxilia em diversas tarefas no cotidiano do ser humano, ela é capaz de proporcionar riscos em igual equivalência, já que não se deve negligenciar o fato de existirem pessoas capazes de usarem o meio eletrônico para cometerem práticas ilícitas. Segundo o delegado Alan Luxardo, titular da Delegacia de Defraudações, unidade esta especializada e responsável por investigar golpes de notória proporção, afirma que a tecnologia ao mesmo tempo em que facilita a vida, também propicia que um estelionatário entre em contato com uma infinidade de vítimas em um breve período e, concomitantemente, se vale de meios que tornam a identificação do agente mais difícil.

Vale destacar que, o crime cibernético não deixa de ser um crime como qualquer outro constituído dentro da legislação brasileira. Conceitua-se crime cibernético pelo fato de ser praticado no âmbito de ferramentas vinculadas a internet ou mesmo através de ferramentas de mídia social, ou seja, os crimes virtuais são toda e qualquer atividade ilegal realizada com o uso da tecnologia.

O objetivo central de quem pratica esse tipo de delito é afetar a pessoa da vítima ou seu computador ou até uma rede maior de computadores, como é o caso de empresas e governos. De acordo com dados obtidos pela Safernet Brasil em parceria com o Ministério Público Federal (MPF) no ano de 2018, foram contabilizados cerca de 133.723 (cinto e trinta e três mil e setecentos e vinte e três) queixas de delitos virtuais. Entre os crimes virtuais mais corriqueiros estão os contra a pessoa, qual seja, calúnia, injúria, difamação, perfil falso, roubo de dados pessoais (conta de e-mail, conta de aplicativo e rede social), além dos crimes de pornografia infantil, homofobia, maus tratos contra animais, intolerância religiosa, xenofobia, neonazismo, apologia e incitação a crimes contra a vida entre outros, conforme mostra quadro abaixo.

Quadro 1. Tecnologia para o mal: Principais crimes cibernéticos praticados no Brasil no ano de 2018.



>> Tecnologia para o mal

Veja os principais crimes cibernéticos que ocorreram no Brasil em 2018

Violação	Incidência
Pornografia Infantil	60.002
Apologia e incitação a crimes contra a vida	27.716
Violência contra mulheres/misoginia	16.717
Xenofobia (principalmente contra nordestinos)	9.705
Racismo	8.337
LGBTfobia	4.244
Neonazismo	4.244
Maus-tratos contra animais	1.142
Intolerância religiosa	1.084
Tráfico de pessoas	509

Fonte: SaferNet Brasil

Fonte: Safernet Brasil.

Quadro 2. Denúncias por Tema: Número de casos ao longo dos anos.



Fonte: Safernet Brasil.

Segundo a Central Nacional de Denúncias de Crimes Cibernéticos da Safernet foram recebidas e processadas cerca de 14.476 (quatorze mil e quatrocentos e setenta e seis) denúncias anônimas de neonazismo na internet no ano de 2021. O número é 60,7% maior que as 9.004 (nove mil e quatro) denúncias registradas em 2020. Além do delito mencionado acima, a pornografia infantil e LGBTfobia registraram aumento de denúncias entre 2021 e 2020. Foram cerca de 101.833 (cem mil e um e oitocentos e trinta e três) denúncias de pornografia infantil, um aumento de 3,65% em relação a 2020. Sobre LGBTfobia, 5.347 (cinco mil e trezentos e quarenta e sete) denúncias foram recebidas pela Safernet em 2021, 1% mais que em 2020. (Safernet, 2022).

Conforme relatório da companhia de cibersegurança Symantec, o Brasil ocupa a terceira posição mundial em ataques cibernéticos, ficando atrás apenas da China e dos Estados Unidos - ocupantes, respectivamente, do primeiro e segundo lugares. Especialistas afirmam que esse quadro, o qual caracteriza um elevado salto em relação ao ano de 2017 momento em que o país ocupava o 7º lugar no ranking, é em razão do grande aumento de dispositivos móveis no território nacional. (L, 2021).

Em um contexto geral, a internet trouxe inúmeros benefícios para a sociedade moderna, oferecendo rapidez e facilidade na execução de tarefas, além de proporcionar maior interação entre as pessoas. Porém, apesar de todas as maravilhas, trouxe consigo

riscos ao usuário, uma vez que são expostos a pessoas mal-intencionadas que podem se aproveitar das facilidades da rede para cometer delitos e causar dano a outrem, além de estarem submetidos à perda de privacidade.

4 DO CRIME DE ESTELIONATO PRATICADO NA INTERNET (ESTELIONATO VIRTUAL).

Restou demonstrado anteriormente que o delito de estelionato se dá a partir do momento em que alguém com o intuito de obter para si ou para outrem, vantagem ilícita, induz ou mantém a vítima em erro, se utilizando de artifício, ardil ou qualquer outro meio fraudulento, causando-lhe prejuízos. Desse modo, por sua vez, os delitos virtuais são aqueles praticados no ambiente virtual através de meios eletrônicos e o acesso à internet.

Logo, percebe-se que a metodologia empregada para cometer crimes virtuais é a mesma utilizada por outros crimes já conhecidos. O que distingue dos delitos elencados no ordenamento jurídico penal brasileiro é a técnica utilizada, porém o resultado final que se busca é idêntico da conduta tipificada. O intuito do agente pode ser de iludir um indivíduo para obter uma vantagem patrimonial ou pessoal, confundir suas vítimas ou até mesmo se apropriar ilegalmente de informações pessoais com o fim de utilizá-las em benefício próprio (Oliveira; Dani, 2011).

De acordo com Ataíde (2017) o crime de estelionato virtual ocorre no momento em que os criminosos forjam e-mails, links etc. falsos, com a pretensão de não serem identificados e conseqüentemente garantem algo que sabem ser impossível de ser executado, porém fazem a garantia em troca de alguma vantagem, que comumente, é patrimonial. Em resumo, o estelionato se configura a partir do induzimento da vítima, valendo-se de meios eletrônicos, dispondo de lacunas que lhe são permitidas para auferir vantagens. Ante o exposto, conclui-se que o delito de estelionato virtual é aquele em que a pessoa na posse de instrumentos tecnológicos e acesso a internet, realiza a ação de induzir ou manter a vítima em erro, valendo-se de quaisquer meios fraudulentos, com o objetivo de obter vantagem ilícita para si ou para outrem.

Na maioria das vezes, a prática do estelionato em ambiente virtual é executada por indivíduos que possuem considerável conhecimento e entendimento sobre tecnologia e internet, que outrora poderiam agir de outra forma, porém optam por se aventurar no espaço virtual do crime para prejudicar e enganar pessoas, conseguindo algum tipo de benefício com esta artimanha. Ressalta-se que a única diferença entre o estelionato real e o estelionato virtual, é o *modus operandi*, onde este é praticado no espaço físico em quanto aquele é realizado no espaço virtual através da internet.

Um dos fatores que corroboram para pratica desse crime cibernético é a falsa sensação de que o ambiente virtual é um “lugar sem leis” em conjunto com a facilidade do crime, visto que o criminoso se expõe menos. Para Mendes (2021), a comodidade do infrator contribui com essa pratica, pois ele tem a ciência que a investigação contra ele será difícil. Além do crime de estelionato virtual não possuir uma pena exorbitante, a facilidade de se ocultar na internet faz com que muitos indivíduos migrem para essa atuação criminosa no meio virtual.

Um dos meios mais corriqueiros de estelionato no ambiente virtual é a invasão do correio eletrônico da vítima, principalmente daquelas que dispõe do hábito de consultar seus extratos bancários e saldos por algum dispositivo eletrônico, em especial pelo computador. Nesta situação, o estelionatário encontra algum jeito de realizar a clonagem da página autêntica da internet banking do usuário e faz com que a vítima tente acessar sua conta, sem ter a ciência que os dados ali inseridos serão interceptados por um terceiro de má-fé que irá utiliza-los posteriormente de forma indevida. (FEITOZA, 2012).

Portanto, conforme exposto acima, essa forma típica de estelionato no mundo virtual se dá a partir do momento em que o agente se vale de meios para clonar a página verdadeira do usuário fazendo-o acreditar que se encontra no lugar certo, inserindo, dessa forma, seus dados pessoais, após invadir o correio eletrônico da vítima.

Segundo o delegado Brenno Andrade, titular da Delegacia Especializada de Repressão aos Crimes Cibernéticos do Estado do Espírito Santo, a prática mais comum está relacionada a contas falsas no Whatsapp. O estelionatário utilizando-se de fotos da vítima, se identifica para amigos e parentes e informa que está com um novo número, e

posteriormente pede alguma vantagem patrimonial (Ribeiro, 2021). Conforme mostra fotos abaixo:

Foto. Golpe do WhatsApp



Fonte: Mundo Conectado.

Não é incomum os criminosos se passarem por parentes através de apps de mensagens, mais especificamente pelo whatsapp, com o intuito de enganar a vítima. São inúmeros os casos de pessoas que tiveram prejuízos ao transferirem, por exemplo, uma quantia em dinheiro ao golpista que se passava pelo filho em um aplicativo de mensagem.

Também se configura crime de estelionato virtual quando o criminoso realiza anúncios falsos em inúmeros sites ou cria páginas na internet, fingindo estar vendendo algo que na verdade não existe, com intenção de induzir a vítima a realizar a compra e, conseqüentemente, o pagamento de um produto que nunca chegará a receber, aproveitando-se da boa-fé dos consumidores e gerando prejuízo patrimonial para os mesmos. Outro tipo recorrente nos dias atuais é o chamado estelionato sentimental ou efetivo. Esse crime ocorre no momento em que há a promessa de relação afetiva em troca de bens ou dinheiro da vítima.

Recentemente a plataforma de streaming Netflix produziu um documentário a

respeito do, talvez, maior 171 de todos os tempos. O documentário intitulado “O Golpista do Tinder” narra a história de mulheres verdadeiras que foram enganadas por Shimon Hayut que se apresentava como Simon Leviev, um bilionário e empresário do ramo de diamantes, criando todo um cenário mentiroso no aplicativo de relacionamento para conseguir conquistar o coração e o dinheiro de “namoradas” iludidas. Foram anos enganando e falindo mulheres ao redor do mundo, nesse período de tempo ele conseguiu defraudar mais de \$ 10 milhões de dólares, oriundos do seu esquema de golpes, usados para sustentar a sua vida de luxo.

É preciso atenção quando estamos no ambiente virtual, pois a cada dia que passa fica cada vez mais difícil de identificar um possível golpe. Algumas recomendações são claras: não informe dados pessoais e não se cadastre em sites de procedência duvidosa e desconhecidos, ao receber um link suspeito não abra e nem clique, desconfie de pedidos feitos pelo Whatsap, SMS ou outros aplicativos, não compartilhe senhas entre outras informações de caráter pessoal.

Em vista disso, é possível observar que são inúmeros os tipos de estelionato cibernético e com o passar dos anos os criminosos vão evoluindo, acrescentando e modificando a sua forma de realizar o supracitado crime.

5 O AUMENTO DE CASOS DURANTE O ISOLAMENTO SOCIAL IMPOSTO PELA PANDEMIA DO COVID 19.

É notório observar que, as práticas de crimes virtuais cresceram drasticamente no Brasil durante os últimos anos. Isso se fundamenta pelo fato da maior utilização dos meios digitais para a realização de tarefas do dia a dia, agravada pelo distanciamento social imposto pela pandemia do covid19, pelo fácil manejo dos meios virtuais e pela dificuldade de punir os criminosos.

No que se refere ao delito de estelionato não é diferente, de acordo com a pesquisa “2019 Global Identity and Fraud Report” realizada pela empresa “Experian”, indicou que o Brasil ocupava o terceiro lugar no ranking mundial em registros de fraudes

eletrônicas, antes mesmo do surgimento da pandemia do coronavírus.

É inegável que o uso de computadores, tablets, celulares aumentou durante a pandemia de Covid-19. Segundo a Agência Nacional de Telecomunicações (Anatel), o consumo de internet no território brasileiro cresceu durante o isolamento social, sendo este um aumento entre 40% e 50%. Com o uso acentuado dos meios digitais, esse momento tornou-se propício para o cometimento de crimes nos ambientes virtuais, em especial o crime de estelionato.

De acordo com a matéria do R7, exibida no Jornal da Record no dia 16/12/2021, houve, de janeiro a novembro, mais de 44 milhões de tentativas de golpes virtuais em todo Brasil. O relatório da Apura Cybersecurity Intelligence, empresa especializada em ameaças digitais, constatou, entre o mês de março e maio de 2020, um crescimento de mais de 41.000% de sites suspeitos.

Outro dado importante divulgado pelo G1 – Globo, afirma que a quantidade de golpes de estelionato em ambiente virtual aumentou no Estado do Rio de Janeiro no início das restrições (março de 2020) decorrentes da pandemia. Conforme o Instituto de Segurança Pública (ISP) os golpes ocorridos de forma online aumentaram de 11,8% para 24,3%. No ano anterior, durante o mesmo mês, somente 7,9% dos casos aconteceram na internet, segundo mostra os dados abaixo:

Quadro 1. O aumento do número de casos de estelionato Virtual durante isolamento social no Estado do Rio de Janeiro.



Fonte: ISP

Até o ano de 2021, o percentual teve um aumento de mais de oito vezes e chegou a 31,5% - isto é, uma a cada três vítimas de estelionato foi abordada por algum aparelho tecnológico, sejam através de mensagens por celular, por meio de algum telefonema, e principalmente através da internet e aplicativos como, por exemplo, o WhatsApp.

No estado do Espírito Santo, o crime de estelionato cibernético superou o número de roubos. Em conformidade com o Painel de Crimes Contra o Patrimônio lançado pelo Governo do Estado, os casos envolvendo o delito de estelionato aumentaram 49,7% em comparação com o ano anterior à pandemia. Com um crescimento exorbitante, foram registrados no ano de 2021 quase duas vezes mais golpes do que roubos em vias públicas. Durante os primeiros oito meses de 2021, a ferramenta registrou cerca de 20 mil crimes de estelionato, em contrapartida, os delitos de roubos somaram 11, 8 mil ocorrências no mesmo período. (Ribeiro, 2021).

Não foi diferente no Estado do Mato Grosso. No primeiro semestre do ano de 2021, os casos envolvendo as fraudes virtuais aumentaram 19% em comparação com o mesmo período do ano anterior, foram registradas 7.491 denúncias entre janeiro e junho. Esse levantamento foi realizado pela Superintendência do Observatório de Segurança da Secretaria de Estado de Segurança Pública (Sesp-MT). Entre as práticas mais comuns está a clonagem do WhatsApp, representando 27% das ocorrências.

Isto posto, é inegável que houve um crescimento exorbitante do número de casos de estelionato virtual em todo o Brasil durante a pandemia do Covid-19. Infelizmente pessoas de má índole utilizaram um momento de vulnerabilidade, incertezas e medo para cometer crimes em detrimento de outras pessoas. Sendo assim, devido ao espantoso e chocante número de casos, e com o objetivo de combater alguns dos cybercrimes, o delito de estelionato disposto no artigo 171 do Código Penal sofreu uma mudança necessária. A lei 14.155/21 entrou em vigor e alterou certos parágrafos, bem como acrescentou outros que tratam a respeito da fraude eletrônica.

5 ALTERAÇÃO DA LEI DOS “CRIMES CIBERNÉTICOS”.

Com o alarmante aumento do número de denúncias envolvendo o crime de estelionato cibernético, restou necessário realizar mudanças no ordenamento jurídico para tentar evitar novas condutas, e inibir os agentes de praticarem o delito em questão.

O presidente da República, Jair Bolsonaro, no dia 27 de maio de 2021 sancionou a lei 14.155/21 que modifica o Código Penal brasileiro, tornando mais severa a pena para os crimes que infringem dispositivos informáticos, estelionato e furtos cometidos através da internet ou por meio de instrumentos eletrônicos. Essa lei tem origem no Projeto de Lei (PL) 4.554/2020 proposto pelo Senador Izalci Lucas do partido PSDB-DF e foi aprovada pelo Senado no começo do mês de maio de 2021. Ao expor o projeto no ano de 2020, o senador salientou que o Brasil ocupava o terceiro lugar no ranking mundial em registros de fraudes eletrônicas, sendo uma das razões a branda legislação para penalizar esse tipo de conduta (Baptista, 2021).

O primeiro artigo alterado foi o 154-A que dispõe sobre a invasão de dispositivo informático. Este delito foi introduzido no Código Penal Brasileiro através da Lei nº 12.737/12, conhecida como “Lei Carolina Dieckmann”, isto porque, a atriz havia sido vítima da conduta acima mencionada quando não havia ainda figura típica específica. A Lei nº 14.155/2021 promoveu quatro alterações no crime do art. 154-A: alterou a redação do caput, acrescentando a incidência do tipo penal; majorou a pena do delito na sua forma básica; bem como majorou a causa de aumento de pena do §2º e a pena qualificadora do §3º.

A referida Lei também ocasionou duas alterações no crime de furto previsto no art. 155 do CP inserindo o § 4º-B, que prevê a qualificadora de furto mediante fraude cometido por meio de dispositivo eletrônico ou informático e acrescentou o § 4º-C, com duas causas de aumento de pena relacionadas com o § 4º-B. Também foi incluído na lei o crime denominado “fraude eletrônica”, que se configura quando o criminoso comete o crime utilizando-se de informações que foram consentidas pela própria vítima ou por terceiros, induzindo-a a erro através de contatos telefônicos, aplicativos, redes sociais ou

através do correio eletrônico fraudulento ou qualquer outro meio análogo. Entre as alterações, foram incluídos os §§ 2º-A e 2º-B no artigo 171 do Código Penal, que versam sobre a fraude eletrônica, com o seguinte texto:

§ 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)

A nova redação da lei incluiu no Código Penal a pena de reclusão de quatro a oito anos e multa quando a vítima for ludibriada a fornecer informações através das redes sociais ou qualquer outro meio, sendo admissível a majoração da pena caso o crime seja praticado com o auxílio de servidor localizado em outro país. A partir dessa premissa, serão punidos crimes realizados em sites de venda e compra de produtos, redes sociais, aplicativos de interação social, como WhatsApp e Apps de namoro, idioma entre outros, quando a fraude é realizada com a utilização de informações fornecidas pela própria vítima ou por um terceiro induzido a erro.

Vale destacar que os criminosos, muitas vezes, exploram idosos, pessoas mais vulneráveis, ou seja, pessoas que não possuem capacidade suficiente para entender que estão sendo vítimas de um golpe. Pensando nisso, a Lei de crime cibernético trouxe uma agravante prevista no § 4º do artigo 171 do CP, dispondo que:

Estelionato contra idoso ou vulnerável

§ 4º A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso (Brasil, 2021).

Nesta senda, a pena que pode ser de 4 a 8 anos, aumenta de 1/3 ao dobro se o crime é cometido contra vítima idosa ou vulnerável, levando em consideração a

relevância do resultado gravoso.

Essa medida foi extremamente necessária, tendo em vista o atual cenário em que se encontra. Com a facilidade de se realizar transações bancárias e com o surgimento de novos meios de pagamento, como por exemplo, o Whatsapp, Pix, Picpay, tornou –se de suma importância as alterações trazidas, tendo em vista que novas tecnologias vão surgindo e conseqüentemente os meios para praticar golpes e fraudes também. Dessa forma, todas as mudanças que possuem o condão de minimizar os riscos das práticas fraudulentas e punir os delitos cometidos através da internet de modo mais rigoroso são sempre bem-aceitas.

Porém apesar das medidas mais duras, o aumento do número de casos ainda persiste. Segundo dados obtidos pela Secretaria de Segurança Pública de Goiás (SSP- GO), cerca de 9,4 mil crimes de estelionato cibernético foram registrados, somente nos três primeiros meses do ano de 2022. Com o advento da Lei nº. 14.155/21, apenas em julho do ano de 2021 que o espaço virtual passou a integrar ao Registro de Atendimento Integrado (RAI) da polícia, segundo a SSP. Sendo assim, a Secretaria de Segurança Pública do estado de Goiás só possui conhecimento dos casos envolvendo a pratica de fraude virtual a partir da data acima mencionada, e afirma que a tendência foi de crescimento com o passar dos meses (Brito, 2022). Conforme mostra tabela abaixo com os dados fornecidos pela SSP:

Meses 2021/2022	N° de casos registrados
Julho/2021	1.886
Agosto/2021	2.252
Setembro/2021	2.035
Outubro/2021	2.221
Novembro/2021	2.839
Dezembro/2021	3.079
Janeiro/2022	3.200
Fevereiro/2022	2.800
Março/2022	3.300

Fonte: SPP.

De acordo com estudos da 16ª edição do Anuário do Fórum Brasileiro de

Segurança Pública desde o aumento percentual de 179% no ano de 2021, o crime de estelionato cibernético não teve queda em nenhum dos 26 estados da Federação.

É notório observar que os casos envolvendo o crime de estelionato ainda estão em alta desde o início da pandemia, até o presente momento não houve uma redução de golpes praticados no ambiente virtual.

Dito isso e conforme exposto acima, percebe-se que a lei 14.155/21 tem como objetivo inibir a conduta do crime acima mencionado e muito embora, tenha sido empregada em momento oportuno para tentar reduzir a atividade criminosa endurecendo e ampliando as penas para crimes cibernéticos e virtuais, nota-se que não se obteve êxito, até o momento, isso porque o estelionato praticado por intermédio da internet é cada vez mais constante e eficiente.

CONCLUSÃO

Perante o exposto, pode-se concluir que a internet foi um grande marco para a humanidade. Ela revolucionou a vida do ser humano, possibilitando uma maior interação entre as pessoas, facilitando a execução de atividades diárias, movimentando a economia, proporcionando lazer, criando relacionamentos, abrangendo o alcance de informações, entre tantas outras coisas. Porém, apesar de todas as vantagens, facilidades e benefícios que a internet trouxe ao longo dos anos para a sociedade atual, também acarretou diversas questões problemáticas, incluindo, principalmente, o uso indevido da mesma com o fim a prática de atos ilícitos, conhecidos como crimes cibernéticos.

A perda de forma parcial da privacidade, a falsa sensação de impunidade e as facilidades que a internet oferece são uns dos muitos atrativos que pessoas mal-intencionadas se utilizam das redes para causar mal a outrem. Não se pode negar, que com os avanços proporcionados pelo surgimento da internet, o modo de execução dos crimes, nela praticados, também tiveram suas evoluções e variações. Nesse sentido, foi possível constatar que os delitos virtuais se tornaram cada vez mais frequentes ao decorrer do tempo e em especial, o estelionato virtual.

Restou demonstrado que o delito de estelionato praticado no ambiente virtual se dá a partir do momento em que indivíduos na posse de dispositivos eletrônicos conectados a internet com o intuito de obter para si ou para outrem, vantagem ilícita, induz ou mantém a vítima em erro, se utilizando de artifício, ardil ou qualquer outro meio fraudulento, causando-lhe prejuízos.

Foi possível identificar várias formas com que o crime em questão pode ser praticado, sendo a mais comum por meio de aplicativos de mensagens e rede social. Com o advento da pandemia do Covid-19, os números envolvendo o estelionato praticado pela internet aumentaram drasticamente, uma vez que as pessoas se viram mais dentro de suas casas e conseqüentemente mais online.

Como forma de tentar inibir tal conduta se fez necessário à criação da Lei 14.155/21 que versa a respeito dos crimes cibernéticos, com o intuito de torna-se mais rígidas as penas para delitos cometidos em ambiente virtual. Porém, apesar da criação da referida lei em boa hora, a mesma não se fez suficiente para diminuir a prática. Os números de casos envolvendo o estelionato virtual são crescentes mesmo após a aplicação da norma no ordenamento jurídico brasileiro. Portanto, chega-se a conclusão de que as normas previstas na nova Lei dos crimes virtuais não demonstrou eficácia, ou seja, são insuficientes para reprimir a prática do crime de estelionato praticado pela internet.

REFERÊNCIAS

ANDREUCCI, Ricardo Antonio. **Manual de Direito Penal**. 10 ed. São Paulo: Saraiva, 2014.

ANDREUCCI, Ricardo Antonio. O crime de estelionato cibernético ou virtual. *In*: **Empório Direito [online]**, 2021. Disponível em: <https://emporiodireito.com.br/leitua/o-crime-de-estelionato-cibernetico-ou-virtual>.

ATAIDE, Amanda. Crimes Virtuais: **Uma análise da impunidade e dos danos causados às vítimas**. 2017. Trabalho de Conclusão de Curso (Graduação em Direito) – Curso de Direito, Instituto de Ensino Superior de Alagoas (IESA), Maceió, 2017.

BAPTISTA, Rodrigo. Lei com penas mais duras contra crimes cibernéticos é sancionada. *In: Agência Senado [online]*, 2021. Disponível em: <https://www12.senado.leg.br/noticias/materias/2021/05/28/lei-com-penas-mais-duras-contracrimenes-ciberneticos-e-sancionada>.

BRASIL, 2021. **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.

BRITO, Leticia. Nove mil goianos sofrem golpe na Internet só nos três primeiros meses de 2022. *In: Diário do Estado [online]*, 2022. Disponível em: <https://diariodoestadogo.com.br/nove-mil-goianos-sofrem-golpe-na-internet-so-nos-tres-primeiros-meses-de-2022-177835/> > Acesso em: 14 jun. 2022.

FERREIRA, Rafaela. Aumento do uso da internet faz crescer o número de crime cibernéticos. *In: Jornal Opção [online]*, 2022. Disponível em: <https://www.jornalopcao.com.br/ultimas-noticias/aumento-do-uso-da-internet-faz-crescer-o-numero-de-crimes-ciberneticos-374687/>.

G 1. Casos de golpes virtuais aumentam durante o isolamento social no RJ, diz ISP. *In: G1 [online]*, 05 jun. 2020. Disponível em: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2020/05/06/casos-de-golpes-virtuais-aumentam-durante-o-isolamento-social-no-rj-diz-isp.ghtml>.

GRECO, Rogério. **Curso de Direito Penal: parte especial. v. 2: introdução à teoria geral da parte especial: crimes contra a pessoa**. 16. ed. Niterói: Impetrus, 2019.

MOREIRA, Paulo Roberto Silvério. Estelionato praticado por meio da internet: uma visão acerca dos crimes digitais. *In: Migalhas [online]*, 2022. Disponível em: <https://www.migalhas.com.br/depeso/359821/estelionato-praticado-por-meio-da-internet>.

OLIVEIRA, Hesrom César de. **Cybercrimes: Do Estelionato Virtual**. Orientador: Prof. Lincoln Martins. 2020. 48f. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Curso de Direito, Faculdade Evangélica de Rubiataba, Rubiataba, 2020.

OLIVEIRA, Luiz Gustavo Caratti de; DANI, Marília Gabriela Silva. Os crimes virtuais e a impunidade real. **Âmbito Jurídico**, Rio Grande, a. 14, n. 91, ago. 2011.

R7. Estelionato virtual é o campeão dos golpes aplicados no Brasil em 2021. *In: R7*

[online], São Paulo, 16 dez. 2021. Disponível em: <https://noticias.r7.com/jr-na-tv/videos/estelionato-virtual-e-o-campeao-dos-golpes-aplicados-no-brasil-em-2021-16122021>.

ROCKCONTENT. Conheça a história da internet, sua finalidade e qual o cenário atual. *In: Rockcontent [online]*, 2020. Disponível em: <https://rockcontent.com/br/blog/historia-da-internet/>. Acesso em: 6 abr. 2022.

SAFERNET. Denúncias de neonazismo à Safernet aumentam 60% em um ano. *In: Safernet [online]*, 2021. Disponível em: <https://new.safernet.org.br/content/denuncias-de-neonazismo-safernet-aumentam-60-em-um-ano#>.

SAGARIONI, Mariana. Denúncias de pornografia infantil no Telegram dobram em um ano, aponta SaferNet. *In: MobileTime [online]*, 2022. Disponível em: <https://www.mobiletime.com.br/noticias/18/02/2022/denuncias-de-pornografia-infantil-no-telegram-dobraram-em-um-ano-aponta-safernet/>.

SILVA, Francielly Juliana; SANTOS, Ramon João Marcos dos. **O estelionato praticado por meio da internet**: uma visão acerca dos crimes virtuais. Disponível em: <https://repositorio.animaeducacao.com.br/bitstream/ANIMA/18080/1/TCC%201.12.21%20dep%C3%B3sito%20final.pdf>.

SOUZA, Luiza Ananda Queiroz de; CERVINSKI, Yasmin. É possível a prevenção e combate aos temidos crimes virtuais? **Anuário de Pesquisa e Extensão da UNOESC**, São Miguel do Oeste, 2021.