CRIMES CIBERNÉTICOS: O Estelionato Virtual e a deficiência dos meios de combate

CYBER CRIMES: The Virtual Stelionate and the deficiency of the means of combat

Verônica dos Santos Cordeiro
Ricardo Silva
Jaqueline Ribeiro Cardoso

Resumo: O presente artigo perfaz uma abordagem analítica sobre os crimes cibernéticos, tratando especificamente sobre o estelionato virtual e a deficiência dos meios de combate por parte do Estado no que tange à esse tipo de crime. É evidente que a sociedade vive em um mundo no qual se depende cada vez mais da internet, dessa forma, mostra-se crescente os riscos decorrentes dos crimes cibernéticos. O estelionato virtual é um crime cibernético que vem acumulando várias vítimas ao decorrer dos anos, o que consequentemente gera para o poder judiciário um elevado número de ocorrências. Existem diversas maneiras de se cometer o crime de estelionato virtual, mas para isso, o criminoso precisa utilizar-se de uma rede de internet para a prática. A metodologia utilizada foi a teórico-bibliográfica, desenvolvida através de doutrinas e artigos jurídicos publicados em revistas impressas ou eletrônicas. Utilizou-se também a pesquisa documental, desenvolvida através de jurisprudências e da legislação brasileira.

Palavras-chave: Internet. Crimes Cibernéticos. Estelionato Virtual. Delegacias.

Abstract: This article makes an analytical approach to cyber crimes, dealing specifically with virtual larceny and the deficiency of means of combat by the State regarding this type of crime. It is evident that society lives in a world in which it is increasingly dependent on the internet, therefore, the risks arising from cybercrime are increasing. Virtual embezzlement is a cyber crime that has accumulated several victims over the years, which consequently generates a high number of occurrences for the judiciary. There are several ways to commit the crime of virtual embezzlement, but for that, the criminal needs to use an internet network to practice. The methodology used was theoretical-bibliographic, developed through doctrines and legal articles published in printed or electronic magazines. Documental research is also used, developed through jurisprudence and Brazilian legislation.

Keywords: Internet. Cyber Crimes. Virtual Scam. Police Stations.

1 INTRODUÇÃO

Os crimes cibernéticos ou cybercrimes surgiram com a evolução do computador e da internet, o que, lamentavelmente tem se tornado um enorme desafio para o Estado, no que tange ao combate desses crimes. Nesse trabalho, buscou-se identificar as principais modalidades dos crimes virtuais, bem como apresentar alguns avanços legislativos quanto à tipificação deles, assim como suas respectivas punibilidades. No decorrer do trabalho, será analisado que no Brasil não há delegacias suficientes para a punição desses crimes que se dá no âmbito virtual, devido a isso, os crimes cibernéticos no Brasil crescem cada vez mais, levando os criminosos à praticarem condutas ilícitas por meio da Internet, propiciando dano a outrem, como por exemplo o estelionato virtual, objeto do presente trabalho.

Pretende-se analisar os crimes virtuais abordando o tratamentos legais e a deficiência dos meios de combate por parte do Estado. Ademais, buscará evidenciar o avanço tecnológico e o advento da internet na vida em sociedade, bem como explana as mudanças trazidas por essas tecnologias, especialmente no âmbito penal. A justificativa para o tema se desenvolve no argumento de que a compreensão a respeito dos crimes virtuais auxilia na reflexão de maneiras de combater, minimizar ou até prevenir.

A temática surgiu a partir dos efeitos alarmantes causados por esse fenômeno, pois, aumentou-se consideravelmente o número de crimes virtuais ocorridos no país.

Diante do exposto, o tema problema reside em analisar a seguinte questão: Com o aumento do uso de tecnologias, os mecanismos de controle e combate ao estelionato virtual, promovidos pelo Estado, são eficazes? Para tanto utilizou-se como referencial teórico as contribuições de diversos autores, tais como Celso Delmanto, José Carlos de Araújo Almeida Filho, Simão Prado Lima, entre outros.

Para a sua confecção, a pesquisa foi desenvolvida em quatro capítulos. O primeiro capítulo aborda os crimes cibernético, fazendo um breve histórico do surgimento da internet e dos crimes virtuais. Ainda é apresentado o conceito e espécies de crimes virtuais. Por fim, é tratado a respeito da influência da internet na vida privada, bem como os riscos que esta tecnologia traz à privacidade. O segundo capítulo apresenta o estelionato virtual, um crime cibernético, cometido por meio da rede de computadores, cujo tratamento se encontra tipificado no art.171 do Código Penal, sendo, porém, praticado por meio eletrônico. Em sequência, serão abordadas as importantes legislações nacionais que proporcionaram

significativas alterações no Código Penal Brasileiro no sentindo de tipificar os crimes praticados no ambiente virtual e adequar alguns artigos já existentes para a realidade cibernética.

O quarto capítulo busca explanar a deficiência dos mecanismos de controle e combate ao estelionato virtual por parte do Estado, como a dificuldade de obtenção de provas desses delitos, diante do anonimato possibilitado pelo ambiente virtual, bem como a deficiência de aparatos investigativos capazes de identificar os agentes criminosos, e, a falta de delegacias especializadas. A metodologia utilizada foi a teórico-bibliográfica, desenvolvida através de doutrinas e artigos jurídicos publicados em revistas impressas ou eletrônicas. Utilizou-se também a pesquisa documental, desenvolvida através de jurisprudências e da legislação brasileira.

2 CRIMES CIBERNÉTICOS

Quando de seu surgimento, em 1969, nos Estados Unidos, a internet que se conhece hoje, recebia na época, o nome de Arpanet (Advanced Research Projects Agency). De lá pra cá, começou a evolução da internet em si, surgindo várias transformações tecnológicas em todo o mundo. Não se pode negar que nas últimas décadas, com a presença da internet, o mecanismo de comunicação entre as pessoas foi facilitado de forma absurda, surgindo assim, novas formas de interação social. Fato é que a internet ao revolucionar as formas de comunicação, trouxe para o mundo uma geração de pessoas que têm o conhecimento, a informação e a interação com outras pessoas bem na palma de suas mãos. Trata-se da eclosão de uma nova espécie de sociedade que, por sinal, bastante diferenciada das outras.

A sociedade contemporânea utiliza-se praticamente de inúmeros tipos de aplicativos para suprir várias necessidades, como por exemplo, aplicativos de redes sociais, de relacionamentos, de edição de fotos, de comidas, de compras, de oração, entre outros. Uma vez feito o cadastro nesses aplicativos, os dados da pessoa ficam armazenados. Isso é possível tendo em vista o uso de *big data* (um grande conjunto de dados que contemplam fontes e dados que podem ser processados, gerando resultados para as empresas) (ROQUE, 2007).

Assim, graças à atual tecnologia da informação, a transmissão de dados é cada vez mais ágil; computadores e satélites auxiliam no processo de envio e recebimento de mensagens, permitindo que várias pessoas conversem entre si, de vários lugares do país e até fora dele. Nesse tocante, a internet não só revolucionou as formas de comunicação, como

também as relações de trabalho, de consumo e de diversão da sociedade, quebrando barreiras e atravessando fronteiras.

No entanto, com o crescimento das interações realizadas por meio eletrônico, houve também o aumento dos chamados crimes cibernéticos. Com isso, a única alternativa que lhes resta é recorrem ao judiciário, na busca de uma possível reparação pelos danos sofridos.

Para um maior entendimento sobre o assunto, Simão Prado Lima (2014) assevera que crimes cibernéticos são "os crimes praticados com o uso do computador ou crimes praticados pela internet". Mas, sua definição é um tanto quanto extensa, pois, o criminoso, com um único equipamento, pode violar a segurança e alcançar informações sigilosas de redes completas de computadores, tanto de empresas privadas como também de órgãos públicos para alcançar seu objetivo criminoso.

Dentre as diversas classificações doutrinárias para estes tipos de crimes, Ivette Senise Ferreira os classificam como:

> Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial (FERREIRA, 2005, p. 261).

Pode-se afirmar que os crimes cibernéticos são todas as condutas "típicas, antijurídicas e culpáveis praticadas contra ou com a utilização dos sistemas da informática" (SCHMIDT, 2014). Ademais, para o autor Sérgio Marcos Roque (2007, p. 25) o crime cibernético é "toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material".

A digitalização dos métodos de comunicação trouxe muitos transtornos provocados por uma nova onda de crimes cibernéticos. Somente neste ano foram registrados inúmeros casos de retenções de informações de empresas e hospitais por todo mundo.

No Brasil, por exemplo, o Hospital do Câncer de Barretos, e outros administrados pela Fundação Pio XII, tiveram as fichas de seus pacientes sequestradas e o resgate exigido girou em torno de mil reais por computador em *bitcoins* (dinheiro virtual). O Hospital teve seu sistema desativado por três dias, fazendo com que os funcionários trabalhassem de forma manual, o que gerou atrasos e prejuízos a muitos pacientes.

De acordo com Marcelo Soares (2000) embora as formas de praticar crimes na internet estejam evoluindo, o País já possui um longo histórico de condutas informáticas danosas.

Outro exemplo dessa infeliz estatística é o do ex-prefeito Paulo Maluf, o qual, nas eleições de 2003, foi o primeiro político a sofrer sabotagem digital.

Os hackers, que são pessoas de elevado conhecimento em informática e que invadem sistemas de computadores sem autorização, para acessar informações de caráter confidencial, invadiram o site do político espalhou e-mails a todos os eleitores cadastrados, divulgando mensagens de cunho difamatório.

Sobre a prática de crimes cibernéticos, há alguns crimes que são praticados com mais frequência, tem-se como exemplo o delito de calúnia, disposta no art. 138 do Código Penal, que é inventar histórias inverídicas sobre alguém; A Difamação, disposta no art. 139, que traduz em difamar ou imputar a alguém fato ofensivo à sua reputação; A Divulgação de segredo, ou seja, divulgar, sem justa causa, conteúdo de documento particular ou de correspondência confidencial disposta no art. 153, do Código Penal.

Outra prática que se expande e gera bastante transtorno, muito comum em época de eleições, é a prática de divulgar notícias falsas, as denominadas *fake news,* que tem gerado uma preocupação no sentido de influenciar indevidamente o processo eleitoral e a confiança dos cidadãos no sistema democrático.

Nesse contexto, a Lei 4.737/65 - Lei que institui o Código Eleitoral, dispõe em seu artigo 323 a pena de detenção de dois meses a um ano, ou pagamento de 120 a 150 dias-multa, para quem divulgar, na propaganda, fatos inverídicos em relação a partidos ou candidatos.

O conceito de *fake news* indica notícias falsas com aparência de notícias jornalísticas que são divulgadas pela internet ou outras mídias. A deliberada divulgação de conteúdos falsos configura ato ilícito civil. Assim, é preciso analisar o tratamento jurídico dado às notícias falsas, e ainda, reconhecer os parâmetros de identificação destas, principalmente de modo a respeitar os princípios da liberdade de imprensa e de opinião.

Nesse sentido, o artigo 5º, inciso IV da CR/88, dispõe sobre a liberdade de manifestação do pensamento, sendo vedado o anonimato. Outro exemplo emblemático são as campanhas contra a vacinação que, periodicamente viralizam e, recentemente, têm resultado no retorno de algumas doenças antes consideradas erradicadas, como sarampo, caxumba, coqueluche, catapora, poliomielite, entre outras.

Ademais, tem-se que o procedimento para a identificação de notícia falsa é complexo e, deve-se considerar a fonte e, até mesmo, outras histórias da mesma fonte, se são igualmente falsas; investigar as fontes de apoio, apurar se o autor é pessoa conhecida e idônea, ou se não há indicação de quem é o autor da manchete. Desse modo, conclui-se que, caberá, à

população através das instituições estabelecidas, reprimir e punir a criação e disseminação de *fake news*, porém preservando as garantias da liberdade de imprensa e a livre manifestação do pensamento.

Como salientado, o uso da internet já está consolidado na sociedade contemporânea, sendo por muitas vezes, a principal ferramenta de trabalho, de lazer e de estudo de diversas pessoas. Em razão disso, pode-se deduzir que, se a mesma vier a extinguir, provavelmente iria causar um caos na sociedade, pois, o usuário já se acostumou com a facilidade de, com apenas alguns cliques, resolver grande parte de suas tarefas, sem ter que sair do conforto de seu lar. Todavia, se for descuidado, poderá causar danos irreparáveis a si e a seus familiares.

Por isso, essa ferramenta deve ser utilizada com muita atenção, uma vez que nem todos que estão por trás de uma tela eletrônica, são dotados de boa-fé, utilizando-se muitas vezes, deste meio para praticar crimes como violação de segurança, roubo de dados pessoais, roubo de informações sigilosas, assédio e, até *bullying*, sendo esse último, um meio de intimidar, aterrorizar e praticar atos vingativos ou cruéis, causando dor e angústia a alguém por meio da internet, podendo se dar de forma física ou psicológica.

3 ESTELIONATO VIRTUAL

O estelionato virtual é um crime cibernético, ou seja, cometido por meio da rede de computadores, que vem gerando para o poder judiciário um elevado número de ocorrências relatando esse tipo de crime. Trata-se do delito de estelionato tipificado no art.171 do Código Penal, porém praticado por meio eletrônico.

Pode-se afirmar, de uma forma inicial, que o estelionato virtual, crime frequente ocorrido na internet, é conceituado por José Carlos de Araújo Almeida Filho e Aldemario Araújo Castro como:

> Uma forma crescente de enganar pessoas de boa- fé. Mas, ainda que praticado via internet, não ganha nova natureza e não se constitui em um novo tipo penal. No fundo nunca deixou de ser ato tendente a obter vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro artifício ou meio fraudulento (ALMEIDA FILHO; CASTRO, 2005, p.183).

Existe apenas uma diferença entre o estelionato comum e aquele praticado na internet e essa diferença é encontrada no modus operandi, uma vez que, o criminoso utiliza-se da internet para obter vantagens e realizar golpes contra os usuários. Ele obtém primeiramente a confiança destes para conseguir seus dados pessoais, com o intuito de desviar seus recursos,

ou fazer com que os mesmos cheguem ao ponto de transferir determinado valor para esse criminoso (FREITAS; CARVALHO, 2021). Desse modo, a internet tem sido utilizada, em boa parte dos casos, como meio para prática de crimes comuns, já existentes, como o estelionato - embora haja condutas criminosas que se originam exclusivamente do meio digital

3.1 O delito de estelionato e a legislação brasileira

Trata-se de crime contra o patrimônio onde a legislação penal visa proteger a inviolabilidade patrimonial orientada pela prática de atos que visam enganar a vítima e beneficiar o agente. Vários são os crimes regulados pelo Código Penal Brasileiro (CP), esse código consiste em impedir que certos direitos da sociedade sejam prejudicados, ou seja, o código penal surgiu para regular as ações dos indivíduos e preservar os direitos da sociedade. Sendo assim, no referido dispositivo legal, o crime de estelionato está disposto no artigo 171. Conforme esse artigo, qualquer indivíduo que cometer os atos nele dispostos, estará cometendo um crime.

O estelionato é um crime que dispõe de certas características de atuação, tendo como intuito auferir uma certa vantagem sobre a outra pessoa. Nos ensinamentos de Hungria (2002) de forma ocasional, a criminalidade anda a passos lentos, longe do uso da violência, propriamente dita, passando-se a ser ressaltada de modo silencioso e inteligente. Em complemento a esse entendimento, de acordo com Noronha (1999), no cenário atual, para atingir o patrimônio pessoal de alguém, tal crime não ocorre com emprego de violência, o estelionatário praticado na atualidade age de forma sorrateira, sem alarde, havendo em muitos casos, o consentimento da própria vítima.

O crime de estelionato está previsto nesse artigo 171 do CP de 1940, e, recentemente, sofreu uma importante alteração pela Lei n° 14.155, de 27 de maio de 2021, que acrescentou e alterou alguns parágrafos no supramencionado dispositivo legal.

Dentre essas mudanças, foram incluídos os § 2°-A e § 2°-B, que dispõem sobre a fraude eletrônica, trazendo a seguinte redação:

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento
> § 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, 1940).

Sobre o delito de estelionato, Guilherme de Souza Nucci ensina que:

> Existem diversas maneiras de se cometer o crime de estelionato, sendo a sua forma genérica a que está disposta no *caput* do artigo, que é quando o indivíduo obtém determinada vantagem sobre outra pessoa ao induzi-la a erro, ou, fazer que permaneça nele. A vítima deve contribuir com o criminoso, porém sem notar que está colocando a risco o seu patrimônio. O autor do crime pode provocar a situação de engano ou simplesmente fazer que a vítima permaneça em erro, usando de artifícios, meios ardilosos ou qualquer outra forma de fraude. (NUCCI, 2017, p. 794).

Depreende-se do tipo em questão que o crime ocorre mediante fraude (emprego de artifício, ardil, apto a enganar alguém); vantagem ilícita e prejuízo alheio. Assim, o bem jurídico protegido por esse crime é a inviolabilidade patrimonial da vítima. Ou seja, "para que seja estelionato é preciso o emprego do artifício ardil, induzir a vítima em erro, obtenção da vantagem ilícita, prejuízo alheio. Assim se faz que com duplo resultado, vantagem ilícita e prejuízo alheio, conexo com a fraude e o erro que provocou" (DELMANTO, 2002, p. 396).

O sujeito ativo do delito pode ser qualquer pessoa, tratando-se de um crime comum, já o sujeito passivo será a pessoa que foi enganada. Vale destacar que se a vítima for incapaz, o crime cometido pelo agente, não será o do art. 171, CP, mas do art. 173, CP que fala de abuso de incapazes:

> Art. 173 - Abusar, em proveito próprio ou alheio, de necessidade, paixão ou inexperiência de menor, ou da alienação ou debilidade mental de outrem, induzindo qualquer deles à prática de ato suscetível de produzir efeito jurídico, em prejuízo próprio ou de terceiro:
> Pena - reclusão, de dois a seis anos, e multa (BRASIL, 1940).

Portanto, o dolo no crime de estelionato é a vontade consciente do agente em: induzir ou manter alguém em erro; utilizar-se de meio fraudulento para tal; e obter vantagem ilícita às custas do prejuízo alheio.

Por fim importante ressaltar que antes da entrada em vigor do 'pacote anticrime', o crime de estelionato, como mencionado, era classificado como crime de ação penal pública incondicionada. Agora, sua classificação é de crime de ação penal pública condicionada a representação da vítima. Ou seja, é uma ação penal pública, mas exige representação porque

há uma ofensa direta à vítima e à sua intimidade. Por isso, o legislador optou por condicioná-la à representação da vítima ou de seu representante legal, Prevista no art. 24, CPP, in verbis:

> Art. 24. Nos crimes de ação pública, esta será promovida por denúncia do Ministério Público, mas dependerá, quando a lei o exigir, de requisição do Ministro da Justiça, ou de representação do ofendido ou de quem tiver qualidade para representá-lo (BRASIL, 1941).

Ademais, o crime de estelionato virtual pode ser praticado contra qualquer pessoa, no entanto, tem-se visto muito, a eminência dessa prática contra pessoas idosas. Dessa forma, entre outros agravantes que aumentam a pena, com previsão no art. 171 do CP, há um critério rigoroso quando o crime de estelionato acometido contra pessoas que de certa forma estejam perdendo sua plena capacidade, como no caso dos idosos. Essa foi mais uma alteração feita pela

> Lei 14.155/2021, referindo-se ao estelionato contra idoso ou vulnerável. Veja-se:
> Art. 171 (...)
> (...)
> § 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, 1940).

Assim, como limite às aplicações de punições pelo Estado, o direito penal é o meio de reprovação ao fato social contrário à norma e em atendimento ao anseio por justiça ao ofendido.

Nessa linha, a autora Debora Nigri (1992) defende que o atual Código Penal brasileiro não está apto quando o assunto é crimes informáticos, ainda que na época quem dirá nos dias atuais que o avanço se encontra bem à frente das perspectivas do passado. Para a autora, o Código penal, sendo da década de 1940, está muito atrás dos avanços tecnológicos, pois nessa época, não se falava em crimes virtuais.

Em disposição contrária Gagliardi (1999) entende que o computador é apenas um meio pelo qual o sujeito efetua o delito, sendo a máquina apenas longa manus, que nada mais é do que uma receptora de comandos. Para o autor, o sujeito se utiliza necessariamente do computador para cometer o crime, sendo esse o sistema informático do sujeito passivo, no qual o computador como sistema tecnológico é usado com objeto e meio de execução do crime.

Nesse contexto, destaca-se que a justiça brasileira tem lutado intensamente para não só prevenir, como também reprimir essa nova modalidade de delito, fato que pode ser

evidenciado através dos dados estatísticos que demonstram o aumento gradativo das demandas judiciais relacionadas à essa temática.

De acordo com uma pesquisa feita ao site UOL, o promotor de Justiça Mauro Ellovitch, do Ministério Público de Minas Gerais (MPMG), relatou que entre os crimes virtuais existentes, o perfil falso no WhatsApp é o golpe mais recorrente no Estado, segundo o magistrado, de janeiro a setembro de 2021, foram 32,9 mil registros de estelionato por meio do aplicativo (MPMG, 2022)

Além disso, em recente pesquisa feita ao jornal O Globo, de acordo com os dados constantes no 16º Anuário do Fórum Brasileiro de Segurança Pública (FBSP), a quantidade de crimes de estelionato virtual cresceu. Passando de 426,8 mil casos em 2018 para 1,26 milhão no ano de 2021, atingindo uma taxa de 583 casos por 100 mil habitantes, é um aumento de 180% em quatro anos (CAETANO, 2022).

Nessa perspectiva, importante se faz destacar também que cada vez mais, inovadoras, são as técnicas utilizadas por criminosos para a práticas desses crimes, por isso a importância da ação por parte do Estado, juntamente com o judiciário, através de seu ordenamento jurídico, e sua real capacidade de repressão diante da prática de ilícitos civis e penais.

Destarte, com o objetivo é garantir a segurança dos usuários da rede, que devem ter seus dados pessoais protegidos contra invasores, cabe trazer à baila, a Lei nº 12.965/14, editada em 23 de Abril de 2014, que cuidou de determinar princípios, garantias, direitos e deveres para o uso da internet no Brasil. Essa Lei Federal foi intitulada como Marco Civil da Internet, sendo aprovada após longos debates sobre a necessidade de se regular o uso da internet no Brasil. Além disso, seu art. 3º, prevê os princípios inerentes ao uso da internet no Brasil, veja-se:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> IV - preservação e garantia da neutralidade de rede;
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei (BRASIL, 2014).

Uma das principais finalidades da referida lei é garantir a privacidade de dados dos usuários da internet, e para isso é necessário que se estabeleça um sistema de segurança no acesso das informações. Outra lei que merece destaque é a Lei nº 12.737/12 (Lei dos crimes cibernéticos), mais conhecida como Lei Carolina Dieckmann. Essa lei reflete um acontecimento vivido pela atriz Carolina Dieckmann. Em 2012, um hacker invadiu o computador pessoal da atriz, possibilitando a ele ter acesso a várias fotos de caráter íntimo. Como a atriz se recusou a pagar R$ 10 (dez) mil reais para não ter suas fotos publicadas - as mesmas acabaram sendo divulgadas na internet, levando à uma discussão sobre a criminalização desse tipo de prática.

A lei altera a legislação penal, acrescentando o artigo 154-A, ao Código Penal Brasileiro, tratando do crime de invasão de dispositivo informático, dispondo que: "Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita" (BRASIL, 2012).

A pena do crime de invasão de dispositivos é a de reclusão, de 1 (um) a 4 (quatro) anos, e multa, aumentando-se a pena de um terço a dois terços se a invasão resultar em prejuízo econômico. A pena aplicável era de detenção de três meses a um ano e multa, no entanto, a nova redação foi incluída pela Lei n° 14.155/2021. Diante disso, a inclusão da equiparação de cartão de crédito ou débito como documento particular "não gera a menor dúvida sobre responsabilização penal nos casos de clonagens de cartões, falsificação de numeração, entre outras alterações" (ANANIAS; WANDERLEY, 2014, p. 45).

Outro artigo acrescentado ao código Penal por força da Lei nº 12.737/12, é o art. 154-B, esclarecendo que: "Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime for cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos" (BRASIL, 2012).

Nos termos desse artigo, a ação penal procederá mediante representação, ou seja, o Ministério Público (MP) só poderá oferecer denúncia a requerimento do ofendido, salvo nos casos em que o crime for cometido contra a administração pública (direta ou indireta), incluindo nesse rol, qualquer poder do governo Municipal, Estadual ou da União, bem como empresas e concessionárias de serviços públicos. Ainda, cumpre trazer a Lei Geral de Proteção de Dados (LGPD) - Lei nº 13.709/2018 (lei que dispõe sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado). Essa lei tem

como fundamentos: O respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Fato é que, uma vez expostos na internet, aqueles usuários que não têm a devida cautela com seus dados pessoais inseridos na rede, correm mais riscos de serem vítimas de crimes cometidos no ambiente virtual, pois, essas informações uma vez disponibilizadas em sites sem nenhuma segurança necessária, ficam suscetíveis de serem utilizadas por criminosos.

Nessa perspectiva, vale citar aqui o Projeto de Lei nº 3376/20 que insere o estelionato virtual no Código Penal. Pelo texto em tramitação na Câmara dos Deputados, essa modalidade terá pena de reclusão, de 2 a 10 anos, e multa – o dobro daquela prevista para o estelionato. Assim, o estelionato virtual será caracterizado, conforme o texto, se o crime for cometido mediante invasão, adulteração ou clonagem de aplicativo de mensagens instantâneas e de chamadas de voz para telefones celulares ou com o emprego da internet, de dispositivo de comunicação ou de sistema informatizado. Nessa visão, entende-se o processo penal como instrumento de justiça para a pacificação social, e, para que assim seja, o Estado deve estabelecer normas jurídicas condizentes com a realidade, garantindo a inviolabilidade dos bens jurídicos dos indivíduos de boa-fé.

4 A DEFICIÊNCIA DOS MECANISMOS DE CONTROLE E COMBATE AO ESTELIONATO VIRTUAL POR PARTE DO ESTADO

Como destacado, não se pode negar que o crescimento da internet acelerou de forma a facilitar muitos processos na vida pessoal e profissional das pessoas, mas, como toda regra tem sua exceção, assim como ela age de maneira positiva, também age de maneira negativa, favorecendo o cometimento de vários crimes virtuais, principalmente o crime de estelionato virtual, objeto de estudo do presente artigo. Diante da quantidade de casos de crimes virtuais em evidência na mídia, pode-se dizer que está cada vez mais difícil mensurar a quantidade desses números, tendo em vista que esses crimes podem variar desde uso indevido de informações, para aplicação de golpes até invasão de sistemas por meio de redes sociais para criar perfis falsos.

Para se ter uma ideia, a prática dos crimes virtuais, tornou-se mais frequente com o isolamento social, em decorrência da pandemia do Covid-19, esses delitos aumentaram abundantemente no ano de 2020 e, no Brasil, estima-se que por minuto ocorrem cerca 23 condutas criminosas pelo meio virtual (INELLAS, 2020).

Ocorre que esse tipo de golpe tem se tornado tão frequente, que muitas vezes, as vítimas acabam por não tomarem as devidas providências, ou seja não procuraram os órgãos responsáveis, gerando como consequência, casos não registrados, o que influencia no levantamento dos índices, tornando-os mais difíceis de serem rastreados. Isso dificulta, até mesmo que o legislador acompanhe tamanhos avanços desses crimes.

De acordo com os peritos criminais dos Institutos de Criminalística, existem algumas ações para o combate e prevenção desses crimes que se traduzem na implantação de tecnologias de segurança da informação, para executar exames periciais e o monitoramento mediante mandado judicial em redes com suspeitas de práticas fraudulentas e, com isso, direcionar estratégias de instituições tanto nacionais quanto internacionais.

Cada agente que comete algum tipo de crime virtual tem uma maneira de agir, no caso do crime de estelionato virtual, cabendo também para outros tipos de crimes virtuais, ao ser uma vítima, a pessoa deve coletar o máximo de evidências possíveis relacionadas ao crime praticado em questão, e se dirigir imediatamente a uma delegacia especializada, para que seja registrado um boletim de ocorrência, caso ela deve procurar a delegacia mais próxima. Ressalta-se que, esse tipo de crime está tomando tamanha proporção, que, alguns estados já contam com delegacias especializadas, para que os processos possam ser agilizados.

No entanto, existem alguns municípios de atuação como Belo Horizonte, que conta com apenas uma delegacia especializada de investigações de crimes cibernético, localizada na Avenida Francisco Sales, 780, Bairro Floresta, esquina da Avenida dos Andradas (altura do nº 1270) - Belo Horizonte -MG. Destaca-se, que uma delegacia especializada nesse tipo de crime, para atender uma cidade que conta com aproximadamente 2,5 milhões de habitantes, não se mostra quão suficiente, pois o delegado precisa ter conhecimento generalista e cuidar de todos os tipos de casos e crimes virtuais, o que acaba por levar a um acumulo de processos e demora na resolução dos crimes e consequentemente a devida punição do agente.

Na opinião da doutrina, para que se possa combater os chamados hackers e golpistas, é preciso preparar a força policial e buscar cooperação dentro e fora do Brasil. De fato, existem poucos combatentes contra os crimes virtuais (NUNES, 2019), por isso, os criminosos aproveitam para invadir sistemas e praticar esses delitos, ou seja, geralmente, os criminosos

agem sem deixar suspeitas, associado ao ambiente virtual que, os permitem agir de forma anônima e silenciosa.

Uma das dificuldades principais enfrentadas pelo Estado é a falta de obtenção de provas para que se tenha uma devida punição dos delitos praticados (CARVALHO, 2021).

Em complemento Goulart (2019) explana que atualmente o direito brasileiro em certos delitos virtuais acaba aplicando a analogia do direito penal visto que é utilizado como parâmetro o crime semelhante existente no ordenamento jurídico. Contudo, é necessário que haja profissionais especializados para tentar combater os delitos virtuais buscando provar a atuação dos criminosos, com isso devem ser utilizados os meios de provas existentes no direito penal.

De acordo com os ensinamentos de Dias (2014) tem-se uma solução para identificar o criminoso que pratica crimes virtuais, seria a utilização da biometria ou de qualquer outro meio que se utilize de característica personalíssima da pessoa, com o intuito de identificar o usuário. Então com a biometria teria uma probabilidade mínima de erro de identificação do agente criminoso. O autor ainda traz outra solução que seria “a responsabilização do acusado somente se houvesse uma prisão em flagrante com o equipamento ligado”. (DIAS, 2014, p. 49). Portanto, de acordo com o autor, tem-se na biometria uma eficácia para os meios de identificação dos criminosos visto que com a prisão em flagrante poderá uma responsabilizar o acusado pelo crime cometido.

Além disso, de acordo com o mesmo autor, a falta de profissionais capacitados nesse ramo para o combate aos crimes virtuais é outra dificuldade enfrentada no país, em razão disso é necessário que esses profissionais, bem como os órgãos destinados a esse combate, se atualizem para realizar seu trabalho de forma desejável. Outra dificuldade enfrentada pelo Brasil é o atraso na criação de leis que evoluam juntamente com a sociedade. São dificuldades como essas que possibilitam o aumento significativo desses crimes (DIAS, 2014).

Nesse sentido, para o professor de direito na Bahia e presidente no Brasil da SaferNet, Tavares (2021) "sem o aparelhamento do Estado, a lei não terá aplicabilidade". Para o professor, falta estrutura e equipamento para a investigação de crimes virtuais, o que consequentemente gera lentidão na apuração de provas e aumento de inquéritos. Ele aponta ainda que “muitas vezes, o mesmo caso é investigado por mais de uma delegacia, devido à falta de coordenação, diz o advogado. "Além disso, ele tece a crítica de que de todos os 27 estados do Brasil, apenas 6 têm delegacias especializadas na repressão a crimes cibernéticos", quais sejam: São Paulo, Rio de Janeiro, Minas Gerais, Espírito Santo, Distrito Federal e Paraná. Para ele "esse número precisa pelo menos triplicar para dar conta do fluxo de casos".

Ainda, de acordo com Silveira (2019) existe uma escassez de profissionais dessa área, isso ocorre pelo fato dos crimes e ameaças nesse setor crescerem e evoluírem rapidamente no decorrer dos anos. Devido a isso, é de extrema relevância que surjam mais profissionais especializados nessa área, para conseguir acompanhar o rápido desenvolvimento desses crimes, e, também, que seja disponibilizado a esses combatentes todos os meios disponíveis e eficazes para um melhor desempenho de seu trabalho.

Assim, a dificuldade na identificação de autoria dos crimes cibernéticos, inclusive do estelionato virtual está na dificuldade na obtenção de provas.

Muito embora, haja uma facilidade no rastreamento do meio pelo qual o crime foi praticado, vale destacar que há a dificuldade maior, encontra-se na associação do meio eletrônico, como por exemplo, o computador, ao sujeito do crime.

Viu-se que para a doutrina, utilização da biometria e a prisão em flagrante com o computador operante seriam soluções propostas a fim de solucionar tal problema. Ademais, considerando a efemeridade e volatilidade dos dados que servirão como prova do crime digital praticado, o instituto da produção antecipada de provas ganha importância, diante da possibilidade de perecimento das provas (DIAS, 2014, p. 50). Segundo Dias (2014) a facilitação da identificação da autoria do criminoso será importante na produção de provas gerando uma eficácia no combate aos crimes cibernéticos.

Uma das possíveis mudanças para serem utilizadas pelos órgãos competentes para impor medidas na eficácia dos combates aos crimes virtuais seria uma reestruturação no que tange aos conhecimentos de informática, para que se possa conhecer melhor a tecnologia avançada para combater a prática de crimes virtuais, assim permitindo uma melhor eficácia contra os crimes virtuais.

5 CONSIDERAÇÕES FINAIS

A presente pesquisa abordou acerca dos crimes virtuais, das bases legais e da eficácia dos possíveis meios de combate aos crimes cibernéticos. Tal qual aos crimes comuns, os crimes virtuais se aperfeiçoam com o tempo abrangendo práticas delituosas que só aumentam, de acordo com o avanço da tecnologia.

A tecnologia pode ser utilizada tanto para o bem quanto para o mal, quando é utilizada para o mal, tal utilização traz sérias consequências para a humanidade, principalmente pela facilidade do acesso à internet que se tem nos dias atuais. Por essa razão, qualquer forma de regulamentação no sentido de estabelecer proteção à sociedade, torna-se bem-vinda.

Ficou constatado que o estelionato virtual apresenta a realidade dos crimes cibernéticos existentes na sociedade contemporânea. Assim, nas situações em que forem comprovados a prática desses delitos, os sujeitos devem ser responsabilizados.

Ainda, ficou demonstrado que a Constituição Federal de 1988 garante a livre manifestação, mas veda o anonimato, sendo essa uma das características principais dos crimes virtuais.

Verificou-se que a jurisdição brasileira tem lutado intensamente para não só prevenir, como também reprimir esses delitos. Foram destacados os principais mecanismos de controle e combate dos crimes cibernéticos no Brasil, como a Lei Federal intitulada como Marco Civil da Internet, que determina princípios, garantias, direitos e deveres para o uso da internet no Brasil; a Lei dos crimes cibernéticos, popularmente conhecida como Lei Carolina Dieckmann, vindo essa lei, alterar a legislação penal, acrescentando o artigo 154-A, ao Código Penal Brasileiro, tratando do crime de invasão de dispositivo informático e trazendo a penalidade aplicada a esse crime. Viu-se também, a Lei Geral de Proteção de Dados, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais por pessoa natural ou por pessoa jurídica de direito público ou privado. Não obstante, ficou entendido que o crime de estelionato previsto no artigo 171 do CP, sofreu uma recente e importante alteração - a Lei n° 14.155/2021, acrescentou e alterou alguns parágrafos no supramencionado dispositivo legal, que dispõem sobre a fraude eletrônica.

Assim, diante das pesquisas legislativas realizadas, no que concerne aos crimes cibernéticos não há no momento, a necessidade da criação de uma nova lei que regulamente esses crimes, visto que já foi criada uma lei especifica para punir esses criminosos, porém há uma necessidade de criação de mais delegacias especializadas e treinadas para identificar e punir esses agentes, pois, como destacado, dentre os 27 estados existentes no Brasil, apenas 6 contam com delegacias especializadas na repressão a crimes cibernéticos. No entanto, existem alguns municípios como Belo Horizonte, que contam com apenas uma delegacia especializada de investigações de crimes cibernético.

A doutrina brasileira não tem dúvidas sobre a dificuldade de se estabelecer um critério seguro e eficaz quando se está diante de crimes praticados no ambiente virtual. Constatou-se com isso que os meios utilizados pelo legislador são eficazes apenas quando à tipificação. Assim, foi possível verificar que não há uma eficácia no combate aos crimes cibernéticos por parte do Estado, pois devido a facilidade de os criminosos utilizarem meios eletrônicos de qualquer parte do mundo, ainda mais onde há uma grande gama de circulação de pessoas, torna-se difícil conseguir provas para a identificação e punição desses criminosos.

Conclui-se que a investigação dos crimes cibernéticos no Brasil não produz resultados eficazes, visto que há uma insuficiência nos recursos tecnológicos utilizados pelo Estado, que se traduz na insuficiência, no despreparo e conhecimento tecnológico para identificar os que praticam crimes virtuais. Enquanto não se tem um efetivo combate a esse tipo de crime, é importante que a população não descuide, ou seja, não deve acreditar em promessas milagrosas, preços abaixo do mercado, garantia rápida de lucros, entre outros. Quanto mais informações disponíveis, maiores as chances de resolução de problemas, pois o desafio dos crimes virtuais ainda é poder identificar de forma célere, de onde partiu a conduta criminosa.

REFERÊNCIAS

ALMEIDA FILHO, José Carlos de Araújo; CASTRO, Aldemario Araújo. **Manual de informática jurídica e direito da informática.** São Paulo: Forense, 2005.

BRASIL. **Decreto-Lei nº 2.848, de 07 de dezembro de 1940.** Institui o Código Penal. **Diário Oficial da União**, Brasília, 07 de outubro de 1940.

BRASIL. **Lei nº 4.737, de 15 de julho de 1965.** Institui o Código Eleitoral. Disponível em: https://www.tse.jus.br/legislacao/codigo-eleitoral/codigo-eleitoral-1/codigo-eleitoral-lei-nb0-4.737-de-15-de-julho-de-1965. Acesso em: 28 de ago. 2022.

BRASIL. **Lei Federal nº 12.737, de 30 de Novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 29 de ago. 2022.

BRASIL. **Lei nº 12.965, de 23 de Abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 29 de ago. 2022

DELMANTO, Celso. Código penal comentado. Rio de Janeiro: Ed., Renovar, 2002.

FERREIRA, Ivette Senise. **Direito & Internet:** Aspectos Jurídicos Relevantes. 2 ed. São Paulo: Quartier Latin, 2005.

FREITAS, Bismarck Thiago de; CARVALHO, Bruno Leandro de. **Crimes cibernéticos.** Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/13962/1/versofinaldoartigoemPDF_BrunoLeandro_20210610184333.pdf. Acesso em: 09 nov. 2022.

DIAS, Jéssica Olivia Dias, PAIVA, Maria de Fátima Sampaio. **Crimes Virtuais e a dificuldade para combatê-los**. 2017. Disponível em: https://flucianofeijao.com.br/novo/wpcontent/uploads/2018/11/artigo_crimes_virtuais_e_as_dificuldades_pa ra_combate_los.pdf. Acesso em: 23 nov. 2022.

DIAS, Camila Barreto Andrade. **Crimes Virtuais:** as inovações jurídicas decorrentes da evolução tecnológica que atingem a produção de provas no processo penal. Disponível em: http://repositorio.uniceub.br/bitstream/235/5977/1/20888860.pdf. Acesso em: 01 nov. 2022.

INELLAS, Gabriel Cesar Zaccaria. Crimes na internet. 2. ed., atual. e ampl. São Paulo: Juarez de Oliveira, 2009. p. 5. Acesso em: 19 out. 2022

LIMA, Simão Prado. **Crimes virtuais:** uma análise da eficácia da legislação brasileira e o desafio do direito penal na atualidade. Disponível em: <https://ambitojuridico.com.br/cadernos/direito-penal/crimes-virtuais-uma-analise-da-eficacia-da-legislacao-brasileira-e-o-desafio-do-direito-penal-na-atualidade/>. Acesso em: 30 de ago. 2022.

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

SCHMIDT, Guilherme. **Crimes cibernéticos**. Jusbrasil, 2014. Disponível em: < http://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos>. Acesso em: 30 de ago. 2022.

SILVEIRA, Artur Barbosa da. **Os crimes cibernéticos e a Lei nº 12.737/2012. 2015.** Disponível em: https://conteudojuridico.com.br/consulta/Artigos/43117/os-crimes-ciberneticos-e-a-lei-no-12-737-2012.

SOARES, Marcelo. **Maluf sofre sabotagem digital em e-mail.** Folha de São Paulo. Disponível em< https://www1.folha.uol.com.br/fsp/brasil/f241020025.htm. Acesso em: 30 de ago. 2022.

NASCIMENTO, Samir de Paula. Cibercrime: Conceitos, modalidades e aspectos jurídicos-penais. 2019.

NUNES, Wagner. Carência de profissionais em cyber segurança facilita crimes na internet. 2019. Disponível em: https://www.terra.com.br/noticias/dino/carencia-de-profissionais-em-cyber-seguranca-facilita-crimes-na-internet,b76978ec3e1077ca0b000ab9094abfa5qmm40vsm.html.

WANDERLEY, Lucas Felix. **Delito Informático e a Lei 12.737/12 (Lei Carolina Dieckmann).** Prof. Me. Ricardo Guilherme Corrêa da Silva, 2014.