UNIVERSIDADE FEDERAL DE MATO GROSSO
FACULDADE DE DIREITO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO PENAL E PROCESSUAL PENAL

KAMMYLLA PEREIRA RODRIGUES GARCIA

CRIMES CIBERNÉTICOS: ANÁLISE DO ESTELIONATO VIRTUAL NA MODALIDADE FRAUDE ELETRÔNICA COM O ADVENTO DA LEI N.º 14.155/21

Cuiabá – MT
2021

KAMMYLLA PEREIRA RODRIGUES GARCIA

CRIMES CIBERNÉTICOS: ANÁLISE DO ESTELIONATO VIRTUAL NA MODALIDADE FRAUDE ELETRÔNICA COM O ADVENTO DA LEI N.º 14.155/21

Trabalho de Conclusão apresentado à Universidade Federal de Mato Grosso – UFMT, como requisito final para obtenção de grau de Especialista em Direito Penal e Processual Penal.

Orientadora: Professora Mestre Keit Diogo Gomes

Cuiabá – MT
2021

KAMMYLLA PEREIRA RODRIGUES GARCIA

CRIMES CIBERNÉTICOS: ANÁLISE DO ESTELIONATO VIRTUAL NA MODALIDADE FRAUDE ELETRÔNICA COM O ADVENTO DA LEI N.º 14.155/21

Trabalho de Conclusão apresentado à Universidade Federal de Mato Grosso – UFMT, como requisito final para obtenção de grau de Especialista em Direito Penal e Processual Penal.

BANCA EXAMINADORA

Professora Mestre Keit Diogo Gomes

Professor Doutor Antônio Sergio Cordeiro Piedade

Aprovada em: 16/08/2021

DEDICATÓRIA

Dedico este trabalho a Deus pela resiliência e força imensurável que me concede em todos os momentos de minha vida. À minha família que tanto amo e é meu alicerce.

AGRADECIMENTOS

Agradeço primeiramente a Deus pela oportunidade, pelo aprendizado adquirido e pela resiliência diante de tantas dificuldades enfrentadas no caminho. Aos meus familiares por compartilhar mais uma vitória em minha vida. E a Universidade Federal de Mato Grosso que direta e indiretamente contribuiu para esta formação.

RESUMO

O crime cibernético de estelionato na modalidade fraude eletrônica, abordado oportunamente pela legislação jurídica brasileira no ano corrente, tornou-se uma realidade crescente, com registro de inúmeros boletins de ocorrência por vítimas no país, especificamente em Mato Grosso, onde mais que dobrou com advento da pandemia. Diante deste cenário, este estudo procurou analisar juridicamente o estelionato virtual e suas nuances, sob o aspecto da Lei n.º 14.155/21, norteando a internet e os crimes cibernéticos para melhor compreensão da especificidade do tema. Para a coleta e análise de dados, como método foi utilizada a pesquisa bibliográfica, com abordagem qualitativa e caráter descritivo, realizada em fontes primárias e secundárias. Os resultados obtidos apontam que foi necessária sua especificidade no ordenamento jurídico, trazendo mais segurança para a população e para a atuação das forças de segurança, tendo em vista a proteção da sociedade e do próprio Estado, além da punição do agente de tal prática ilícita no cyberespaço.

Palavras-chave: Crime Cibernético; fraude eletrônica; legislação brasileira.

ABSTRACT

The cybercrime of swindling in the electronic fraud modality, addressed timely by Brazilian legal legislation in the current year, it has become a growing reality, with record of numerous police reports by victims in the country, specifically in Mato Grosso, where it has more than doubled with the advent of the pandemic. Faced with this scenario, this study sought to legally analyze the virtual fraud and its nuances, under the aspect of Law 14.155/21, focusing on the internet and cyber crimes to better understand the specificity of the theme. For the collection and analysis of data, bibliographic research was used as a method, with a qualitative and descriptive approach, performed in primary and secondary sources. The results obtained indicate that its specificity was necessary in the legal system, bringing more safety for the population and for the action of the security forces, in order to protect society and the State itself, in addition to punishing the agent of such an illicit practice in cyberspace.

Keywords: Cybercrime; electronic fraud; Brazilian legislation.

SUMÁRIO

INTRODUÇÃO

O Brasil por ser um Estado democrático de direito é responsável em solucionar conflitos interpessoais e institucionais da sociedade. Esses conflitos advindos da sociedade moderna avançam em ritmo acelerado e um dos fatores são as melhorias tecnológicas por conta do crescimento da internet, que traz facilidade e agilidade na vida dos cidadãos.

Esse desenvolvimento tecnológico, exponencial, disposto a qualquer pessoa e em qualquer lugar, fez surgir na mesma proporção alguns delitos difíceis de serem punidos, utilizando-se o meio virtual como forma de execução.

Trata-se de formas de execução que até pouco tempo atrás não existiam, envolvendo novas técnicas, que por meio de ameaças virtuais, acarretam consequências reais.

Com a evolução da sociedade da informação, trazendo o surgimento de várias inovações tecnológicas e praticidade para a vida das pessoas, acarretou a facilidade das ações de pessoas maliciosas, que se aproveitam desse avanço para praticar os mais variados tipos de crimes.

Nessa senda, o estelionato virtual merece atenção especial, pois vitimiza milhares de pessoas diariamente, devido à facilidade com que o crime é executado, apresentando diversas formas de execução e a dificuldade que o Estado tem de punir seus autores, criando um ambiente favorável para seu crescimento e apresentando novas possibilidades para a continuidade da prática da criminalidade.

O tipo penal que trata o estelionato e outras fraudes encontra-se descrito no artigo 171, do Decreto-Lei nº 2.484, de 07 de dezembro de 1940 (Código Penal Brasileiro). Até pouco tempo, não havia no Brasil dispositivo legal referente ao estelionato praticado de modo virtual. No entanto, em 27 de maio do corrente ano, foi sancionada a Lei n.º 14.155, que altera o Código Penal Brasileiro, agravando as penas como invasão de dispositivo, furto qualificado e estelionato ocorrido em meio digital, conectado ou não à internet. A inovação legislativa veio em momento oportuno, tendo em vista o aumento de fraudes virtuais no Brasil, principalmente em decorrência da pandemia da Covid-19.

No entanto, mesmo com o advento da Lei n.º 14.155/21, há ainda outros fatores que dificultam a devida punição do criminoso que pratica esta modalidade delituosa, afinal, ele encontra em seu benefício a dificuldade em desvendar a autoria

e encontrar provas, não apenas pelo meio em que ocorre os atos executórios, mas também pelo aparato policial e judicial aquém do mínimo necessário, fatores que muitas vezes impedem o correto trâmite processual.

Diante desse cenário, faz-se necessário um real interesse em coibir este tipo de prática delituosa, para fins de proteger os cidadãos de ataques virtuais. Criminalizar o estelionato virtual foi uma iniciativa de extrema importância, objetivando a segurança das informações e a confiança na integridade das tecnologias, assegurando a dignidade da pessoa humana e a proteção da propriedade.

Sobretudo, fazem-se necessárias iniciativas públicas de ferramenta social, que promovam a inclusão digital, assegurada pela Lei 12.965/2014 – Marco Civil da Internet, como dever constitucional do Estado.

É primordial que sejam adotadas medidas de prevenção, por mecanismos de proteção com a finalidade de conscientizar a população sobre os perigos da internet, preparando para promover a autodefesa, orientando-se em como proceder para garantir a segurança de suas informações e a imprescindibilidade de salvaguarda dos dados pessoais.

Buscando melhor entendimento acerca do assunto, este trabalho monográfico tem por finalidade analisar juridicamente o estelionato virtual e suas nuances, sob o aspecto da Lei n.º 14.155/21, fazendo uma breve análise sobre a internet e os crimes cibernéticos para melhor compreensão da especificidade do tema.

A metodologia utilizada no desenvolvimento do trabalho consiste em pesquisa bibliográfica, com abordagem qualitativa e caráter descritivo, realizada em documentos, livros, artigos, dissertações e teses publicados em fontes abertas.

Nessa perspectiva, o estudo foi estruturado em capítulos:

O capítulo I trata da relação entre a internet e os crimes cibernéticos, por meio de conceitos e tipologias dos crimes como próprio e impróprio; e os crimes cibernéticos no ordenamento jurídico brasileiro;

O capítulo II faz uma abordagem sobre o estelionato virtual, com seus aspectos criminológicos, fraude eletrônica, e ainda, o perfil e o *modus operandi* do sujeito ativo de crime virtual;

O capítulo III, faz uma abordagem sobre o advento da Lei nº 14.155/2021, seus reflexos e sua aplicabilidade jurídica;

E por último, as considerações sobre o assunto em tela.

1 A INTERNET E OS CRIMES CIBERNÉTICOS

Inicialmente, antes de adentrar a especificidade do tema abordado, faz-se necessário o entendimento acerca da rede mundial de computadores, a internet. Para tanto, será exposta uma breve análise evolutiva, num cenário histórico que possibilite melhor coerência em sua ligação com os crimes cibernéticos.

A rede mundial de computadores foi criada para atender estratégias militares, numa corrida armamentista e espacial, no auge da Guerra Fria, estabelecida entre os Estados Unidos e União Soviética, quando os soviéticos lançaram, em outubro de 1957, o satélite *Sputnik* I, causando reação no Departamento de Defesa dos Estados Unidos, que criou uma agência militar de pesquisas em ciência e tecnologia, denominada *Advanced Research Projects Agency* (ARPA), cuja missão, inicialmente, era prevenir surpresas tecnológicas, como o satélite *Sputnik* I e servir como mecanismo para pesquisa e desenvolvimento de alto risco (CARVALHO, 2006, p. 8), descentralizando "[...] as informações sensíveis, de modo a preservá-las em caso de ataque nuclear pela extinta União Soviética (SIQUEIRA, 2008, p.127)".

Veja nessa mesma perspectiva, o ensinamento do criminalista Fabrízio Rosa (2005, p.31):

> A fagulha que acabaria por acender a revolução da conectividade ocorreu em 1957, quando a União Soviética pôs em órbita o primeiro satélite espacial, o Sputnik: quatro meses depois, o presidente americano Dwight Eisenhower anunciava a criação de uma agência federal norte-americana, nos moldes da NASA, conhecida como Advanced Research Projects Agency - ARPA, com a missão de pesquisar e desenvolver alta tecnologia para as forças armadas.

O Departamento de Defesa dos Estados Unidos, percebendo a necessidade de reunir informações do banco de dados de pesquisa do governo americano e dessa forma enviá-las para outras áreas de forma segura, criou a Rede da Agência para Projetos de Pesquisa Avançada – *Advanced Research Projects Agency Network* (ARPANET), um sistema de telecomunicações em que os computadores se comunicam, estando em locais diferentes, de modo que, ocorrendo um incidente de ataque aos Estados Unidos, mesmo após o ataque, as comunicações militares não seriam prejudicadas (INELLAS, 2009, p. 1).

Nesse sentido, conforme ensinamento do professor Gabriel César Zaccaria de Inellas (2009, p. 1):

> A partir dessa preocupação, o Departamento de Defesa dos Estados Unidos elaborou um Sistema de Telecomunicações, desenvolvido pela Agência de Projetos e Pesquisas Avançadas, a ARPA, criando assim uma rede denominada ARPAnet, que operaria através de inúmeras e pequenas redes locais, denominadas LAN (Local Area Network), que significa rede local responsável em ligar computadores num mesmo edifício, sendo instaladas em locais estratégicos por todo o País, os quais foram interligadas por meios de redes de telecomunicação geográficas, denominadas WAN (Wide Area Network), que significa rede de longo alcance, responsáveis pela conexão de computadores por todo o mundo, e assim, caso houvesse um ataque nuclear contra os Estados Unidos da América, as comunicações militares e governamentais não seriam interrompidas, podendo permanecer interligadas de forma contínua.

Em 29 de outubro de 1969, foi realizada a primeira comunicação entre a Universidade de Los Angeles (UCLA) e o Instituto de Pesquisa Stanford, sendo a primeira conexão entre computadores a centenas de quilômetros de distância (BRASIL, 2020, p.12).

Diante da amplitude do projeto, cabe destacar o seguinte posicionamento (BRASIL, 2020, p.14):

> [...] o objetivo do projeto era criar uma rede, cuja operação seria menos vulnerável a um ataque atômico e suas vias de comunicações menos interceptáveis. Porém, o potencial transformador desta criação, em pouco tempo, foi enxergado e seus designíos ampliados, exigindo uma padronização de protocolos e documentação detalhada[1].

Em sua tese de mestrado, o Msc. Bruce William Percílio Azevedo (2020, p. 5) reza que a rede mundial de computadores expandiu-se a partir de 1982, sendo inserida dentro do âmbito acadêmico dos Estados Unidos e posteriormente em outros países, quando passou a ser conhecida como Internet, e ainda:

> A partir de 1992, empresas e outras organizações começaram a investir na sua ampliação e difusão, juntamente com a invenção da World Wide Web (www) pelo Laboratório Europeu de Física de Partículas (CERN), dando origem a Internet "comercial", resultando desde então em seu emprego de forma maciça.

Considerando essa breve passagem histórica da criação da Internet, percebe-se sua amplitude diante do objetivo de sua criação, passando de uma iniciativa de estratégia militar para utilização de troca de mensagens entre universidades,

[1] BRASIL. Ministério da Justiça e Segurança Pública. Secretaria em Gestão e Ensino em Segurança Pública. **Curso Crimes Cibernéticos: Noções Básicas.** 2020.

associando ainda várias redes e serviços, tornando a proporção, que hoje tem, de infinitas possibilidades.

Dessa forma, analisando o atual contexto, vislumbra-se que “nenhuma outra tecnologia, ideologia ou ferramenta causou tamanha revolução cultural, econômica e social como a internet” (BARRETO; KUFA; SILVA, 2020, p. 27).

Com o advento da internet e sua expansão exponencial, com capacidade infindável de facilitar a vida das pessoas, “[...] se tornou uma ferramenta de extrema importância para o mundo globalizado, pois além de relacionar pessoas, transmitir informações é também um meio de comércio” (SANTOS; MARTINS; TYBUCSH, 2017, p.2).

No entendimento de Corrêa (2000, p. 8), a internet é vislumbrada como:

> Um sistema global de rede de computadores que possibilita a comunicação e a transferência de arquivos de uma máquina à outra qualquer, conectada na rede, possibilitando, assim, um intercâmbio de informações sem precedentes na história, de maneira rápida, eficiente e sem a limitação de fronteiras, culminando com a criação de novos mecanismos de relacionamento.

Conforme Pesquisa Nacional por Amostra de Domicílios Contínua, com o módulo temático sobre Tecnologia da Informação e Comunicação, nos aspectos de acesso à Internet e à televisão e posse de telefone móvel celular para uso pessoal, realizada no 4º trimestre de 2019, com pessoas a partir de 10 anos de idade, foi possível constatar que no Brasil, numa população de 183,3 milhões de pessoas de 10 anos ou mais de idade, 143,5 milhões utilizam a internet, ou seja, 78,3%. Percentual em crescimento nos últimos anos (com referência à população de 10 anos ou mais de idade, utilizando a internet no mesmo período), sendo: 64,7% em 2016, 69,8% em 2017 e 74,7% em 2018”[2].

Barreto, Kufa e Silva (2020, p. 29) apresentam um estudo realizado em 2018 pelo maior organismo mundial da área de telecomunicação, a *International Telecomunication Union* (ITU), estimando que no fim de 2018, 3,9 bilhões de pessoas estavam usando a internet, sendo 51,2% da população mundial, ou seja, mais da metade da população do planeta[3].

---

[2] IBGE. Disponível em: <https://biblioteca.ibge.gov.br/visualizacao/livros/liv101794_informativo.pdf>. Acesso em: 3 jul. 2021.

[3] Measuring the Information Society Report. Volume 1, p. 16. Disponível em: <https://tinyurl.com/y83bpgld>. Acesso em 07/07/2021.

Outro dado relevante quanto ao tema, para ter noção do alcance dessa tecnologia, trata-se da quantidade de usuários que utilizam redes sociais, que ultrapassa a população de alguns países. Em 2016, os usuários da rede social *Facebook* passavam de 1,59 bilhão de usuários, maior que a população da China, que somava 1,367 bilhão de cidadãos (BRASIL, p. 20).

Os dados expostos acima ratificam o alcance e a dependência diante dessa tecnologia, revelando a irreversibilidade e o crescimento da internet.

Contudo, por mais que a internet tenha sido um marco no desenvolvimento tecnológico, como meio de comunicação em massa mais difundido nos últimos anos, na mesma proporção, transformou-se em um potencial espaço para o cometimento de práticas delituosas, com uma expansão acelerada.

Jesus e Milagre (2016, p.1 e 2) descrevem com excelência o processo de globalização vivenciado no momento atual, caracterizado por uma economia global e informacional, que iniciou na segunda metade do século XX, rompendo as barreiras econômicas e dessa forma integrando a sociedade. E em decorrência dessa globalização, surgiu a sociedade da informação que vive em constante transformação e por meio da tecnologia propulsiona mudanças sociais, chegando a ditar comportamentos e costumes. Trata-se de uma sociedade inevitável, sedenta de conhecimento e informação, e no atual estágio social, a dominância informacional é poder, é riqueza. E levando em conta que a internet é rica, onde há riqueza, há crime.

Pode-se definir este momento vivenciado pela sociedade da informação, de “Aldeia Global”, notável expressão criada pelo estudioso canadense Marshal McLuhan[4], que denominava uma ideia em que a evolução tecnológica permitiria uma comunicação direta e sem barreiras, estando diretamente relacionada com o conceito de globalização.

Referido conceito também foi citado nas obras de Barreto, Kufa, Silva (2020, p. 30), dando ênfase a essa teia de informações, cujo alcance e dependência tornaram-se importantes em nossas vidas.

---

[4] Educador, intelectual, filósofo e teórico da comunicação canadense. Vislumbrou a internet quase trinta anos antes de sua criação, sendo um dos pioneiros nos estudos sobre as transformações sociais provocadas pela revolução tecnológica do computador e das telecomunicações. Conhecido por cunhar a expressão “Aldeia Global” e por sua máxima de que “O meio é a mensagem”. WIKIPEDIA. Disponível em: <https:// https://pt.wikipedia.org/wiki/Marshall_McLuhan#cite_note-38>. Acesso em: 1 jul. 2021.

Do mesmo modo, Jesus e Milagre (2016, p. 1) discorrem sobre a aldeia global, destacando o surgimento da sociedade da informação, também conhecida por sociedade do conhecimento ou da nova economia, enfatizando que “a informação é riqueza, poder e o motor para o desenvolvimento e bem-estar social”, aprimorando assim, o padrão de vida.

Não obstante, conforme expressão de Eric Schimidt[5]: “a internet é a primeira coisa que a humanidade criou e não entende, a maior experiência de anarquia que jamais tivemos” (NERY; BITTENCOURT; AZAMBUJA, 2013).

E por ser “uma grande praça pública, o maior espaço coletivo do planeta” (CASSANTI, 2014, p.3), “aliada a um surgimento não planejado, não escalonado e que não primava pela segurança da informação, facilitou, entre outros elementos, o desenvolvimento da criminalidade na rede e através da rede” (BARRETO; KUFA; SILVA, 2020, p.27), cultivando a ideia de que o ambiente virtual é terra sem lei, sem fronteiras, abrindo oportunidades para prática de crimes, de forma rápida, prática e corriqueira, objetivando poder e lucro.

Nesse contexto, ressalta-se o posicionamento de Damásio de Jesus e José Antônio Milagre (2016, p. 16):

> [...] a sociedade da informação (ou para muitos, pós-industrial) tem, sim, seus riscos. Pode ser chamada de sociedade dos riscos. Riscos que podem ser aceitos e riscos que devem ser mitigados. E um deles está associado à criminalidade digital. Ao considerarmos que nem todo o cidadão decidiu ingressar mas lançado foi no universo digital, constitui-se presa fácil nas mãos de especialistas em crimes cibernéticos [...].

Portanto, ainda que internet tenha surgido para facilitar e aumentar a comunicabilidade entre as pessoas, ela igualmente pode ser usada como meio para aqueles que vêem nela a oportunidade para prática de transgressões penais. (ALBUQUERQUE, 2006, p.20)

Nesse diapasão, segue o entendimento de Fabrízio Rosa (2005, p. 3):

> Com a expansão do uso de computadores e com a difusão da internet, tem-se notado, ultimamente, que o homem está se utilizando dessas facilidades para cometer atos ilícitos, potencializando, cada vez mais, esses abusos

[5] Eric Schmidt, bilionário americano, pesquisador visitante em inovação no Massachusetts Institute of Technology, foi CEO da empresa Google de 2001 a 2011, conselheiro da Alphabet, empresa controladora do Google, até junho de 2019, permanecendo como consultor técnico até fevereiro de 2020. Também foi CEO da Novell e diretor de tecnologia da Sun Microsystems. FORBES. Disponível em: <https://www.forbes.com/profile/eric-schmidt/?sh=7c277d17138e>. Acesso em: 7 jul. 2021.

> cometidos na rede. Como todos os recursos de disponibilidade do ser humano, a informática e a telecomunicação não são utilizadas apenas para agregar valor. O abuso (desvalor), cometido por via, ou com assistência dos meios eletrônicos não tem fronteiras.

Indubitavelmente a internet proporciona a seus usuários incontáveis benefícios, no entanto, como todo benefício traz consigo uma consequência, em decorrência desse desenvolvimento tecnológico, surgiram os crimes cibernéticos (LOPES, CONTRIM, 2014, p. 11).

As considerações abordadas evidenciam a propagação desenfreada de condutas ilícitas pela internet, provavelmente por oferecer um mundo sem fronteiras, com infinitas possibilidades e em processo contínuo de evolução, tornando propício a prática de crimes no espaço virtual, também chamado de ciberespaço, possibilitando ainda o anonimato.

1.1 Conceito e características do crime cibernético

Os ilícitos praticados por meio da internet ainda não possuem uma denominação consensual na doutrina, e conforme entendimento de Kunrath (2017, p. 45), eles podem assumir várias denominações, como “cybercrime, crime digital, crime informático, crime informático digital, cibercrime, crimes eletrônicos, delitos de computador, delitos computacionais, crime de computação, etc”.

Para Jorge e Wendt (2012, p. 10), podem ser denominados por “crimes digitais, crimes eletrônicos, cibercrimes, crimes cibernéticos [...]”, entre outras nomenclaturas.

Barreto, Kufa e Silva (2020, p. 50-51) reportam que essa questão de tentar achar uma nomenclatura apropriada para albergar esses tipos de delitos são tortuosas e que os Estados Unidos da América também sofrem com esse tipo de problema, mesmo sendo um país que está à frente na repressão de delitos cometidos pelas redes de dados. E ainda apontam conforme entendimento referenciado por Clough (2010, p. 9) as expressões utilizadas:

> [...] *computer crime, computer-related crime, crime by computer*, ou depois, com a maior disseminação da tecnologia, os termos: *higt-tecnology crime, information age-crime*. Com o advento da internet surgiram: *cybercrime, virtual crime, internet crime, net crime*, além de outras variantes mais genéricas, como: *digital crime, electronic crime, e-crime, hight-tech crime* ou *technology-enable crime*.

Conforme Clough (apud BARRETO; KUFA; SILVA, 2020, p. 51), nenhuma expressão é perfeita, por não alcançar o absoluto sentido da conceituação desta nova categoria de crime, sofrendo com uma ou mais deficiências. Dessa forma:

> As expressões que contêm o vocábulo “computador” podem não incorporar as infrações cometidas contra as redes de dados; o termo “cibercrime” pode ter como foco exclusivo a internet; “crimes de alta tecnologia” podem ser entendidos como referências, tão somente, aos delitos envolvendo avançadas e recentes searas da tecnologia, como a nanotecnologia ou a bioengenharia.

BARRETO, KUFA e SILVA (2020, p. 54 e 55), no esteio de Clough (2010, p. 9), adotaram a terminologia “cibercrime”, por melhor albergar os delitos dessa natureza e por “[...] ser a mais utilizada na doutrina internacional, por ressaltar a importância dos computadores em rede e, especialmente por ser o termo utilizado na Convenção de Budapeste [...]”.

Ressalta-se ainda posicionamento de Vladimir Aras (2001, p. 1), o qual reza que “cibercrimes” e “crimes telemáticos” são denominações mais apropriadas para identificar esses tipos de infrações:

> Delitos computacionais, crimes de informática, crimes de computador, crimes eletrônicos, crimes telemáticos, crimes informacionais, ciberdelitos, cibercrimes... Não há um consenso quanto ao nomen juris genérico dos delitos que ofendem interesses relativos ao uso, à propriedade, à segurança ou à funcionalidade de computadores e equipamentos periféricos (hardwares), redes de computadores e programas de computador (estes denominados softwares). Dentre essas designações, as mais comumente utilizadas têm sido as de crimes informáticos ou crimes de informática, sendo que as expressões "crimes telemáticos" ou "cibercrimes" são mais apropriadas para identificar infrações que atinjam redes de computadores ou a própria Internet ou que sejam praticados por essas vias. Estes são crimes à distância stricto sensu.

Por fim, Fabrízio Roza (2007, p. 53) pontua que são “denominações distintas, mas que, no fundo, acabam por significar basicamente a mesma coisa”, portanto, ainda que a nomenclatura “cibercrime” seja a mais difundida internacionalmente, as outras são utilizadas como sinônimos e no presente trabalho será utilizada a nomenclatura “crimes cibernéticos”.

Na doutrina há diversos conceitos acerca do tema em tela, e assim as definições se complementam.

No entendimento de Costa (1997 apud Kunrath, 2017, p. 47 e 48), esse tipo

de crime compõe dois elementos, quais sejam, “contra os dados que estejam preparados às operações do computador e, também, através do computador utilizando-se ‘software’ e ‘hardware’, para perpetrá-los”, definindo o crime pelo bem jurídico protegido:

> É a conduta que atenta contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar. Isto posto, depreende-se que o crime de informática é todo aquele procedimento que atenta contra os dados, que o faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão.

E seguindo essa linha de pensamento, conclui com o seguinte exemplo:

> [...] aquele que ateia fogo em sala que estiverem computadores com dados, com o objetivo de destruí-los, não comete crime de informática, do mesmo modo, aquele que, utilizando-se de computador, emana ordem a outros equipamentos e cause, por exemplo, a morte de alguém. Estará cometendo homicídio e, não crime de informática.

Para Rocha (2000, p. 318): “Crimes virtuais são aqueles que têm por instrumento ou por objeto de processamento eletrônico de dados, apresentando-se em múltiplas modalidades de execução e de lesão de bens jurídicos”.

O conceito apontado pela Organização para a Cooperação Econômica e Desenvolvimento da ONU (apud ROSSINI, 2004, p. 109) reza que o crime de informática abarca qualquer conduta que seja ilegal, não ética, não autorizada, envolvendo processamento de dados e/ou transmissão de dados.

Conforme Rossini (2004, p. 110), os “delitos informáticos”, compreendem crimes e contravenções penais, abrangendo condutas praticadas na Internet, bem como aquelas em que haja relação com sistemas informáticos, sendo tanto o meio, quanto o fim, de modo a abarcar delitos em que o computador seria uma mera ferramenta, sem estar conectado à internet ou a qualquer outro ambiente telemático. Assim, expende o seguinte:

> O conceito de “delito informático” poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade. (ROSSINI, 2004, p. 67)

Segundo Ferreira (2005, p. 261), os crimes virtuais são:

> 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.

É certo que se trata de crimes que se propagaram com o advento da rede mundial de computadores, cuja atividade criminosa é promovida no âmbito digital e se caracteriza analiticamente de forma tripartida, sendo um ato típico, antijurídico e culpável.

São crimes “em que a tecnologia foi utilizada como ferramenta-meio ou alvo-fim da atividade criminosa no meio ambiente computacional da sociedade complexa da informação e comunicação” (PINHEIRO; GROCHOCKI, 2016, p. 555).

Trata-se de um fenômeno característico das transformações tecnológicas, vivenciadas atualmente pela sociedade e que acabam influenciando no Direito Penal, caracterizando seu conceito como fato típico e antijurídico, em que seu cometimento ocorre pela tecnologia da informação, ou contra esta. Assim, a informática pode ser o bem ofendido ou o meio para a ofensa a bens que já são protegidos pelo Direito Penal. Porém, como crime-meio, vem se desenvolvendo como crime-fim. “Fato é que a maior parte dos crimes eletrônicos está relacionada a delitos em que o meio para a realização da conduta é virtual, mas o crime em si não” (JESUS; MILAGRE, 2016, p. 48-50).

Fichtelberg (2008, p. 265 apud BARRETO; KUFA; SILVA, 2020, p. 54) narra que os cibercrimes na concepção dos criminologistas são divididos em duas categorias: aqueles que utilizam computadores para a prática de crimes convencionais e outros que, antes de inventarem os computadores e a internet, não existiam, caracterizando como delitos específicos.

“[...] Em essência, o cibercrime envolve o uso de aparelhos eletrônicos para acessar, controlar, manipular ou utilizar os dados para fins ilegais” (MCQUADE III, 2006, P. 15 apud BARRETO; KUFA; SILVA, 2020, p. 55).

Face ao exposto, os autores mencionados sintetizam a definição de cibercrime em delitos tradicionais, que no atual momento encontra-se em nova roupagem, alcance e lesividade potencializada, com novas infrações que não existiriam se não houvesse computadores e redes de computadores para sua

concretização (cibercrimes propriamente ditos) (BARRETO; KUFA; SILVA, 2020, p. 56).

Nesse diapasão, fazendo referência a Briat (1985), discorrem Jesus e Milagres (2016, p. 53):

> [...] diga-se, a distinção entre crimes informáticos em que a informática é o meio para a prática de velhos crimes ou agressão a bem jurídico protegido pelo Direito Penal, e crimes informáticos em que a informática (inviolabilidade dos dados) é o bem jurídico protegido, propriamente dito.

A partir desse enfoque, pode-se classificar os crimes cibernéticos em próprios e impróprios, mesmo havendo várias outras classificações doutrinárias com o fito de defini-los, e conforme Carneiro (2012), trata-se da classificação que está mais próxima da realidade dos fatos.

E em decorrência de ser largamente utilizada pela doutrina no âmbito penal, parece ser mais acertada a escolha do *nomen juris:* “próprios e impróprios”, mesmo sendo apontada a existência de outras nomenclaturas, como delitos informáticos puros e impuros (BARRETO; KUFA; SILVA, 2020, p. 56), crimes informáticos comuns e específicos (ALBUQUERQUE, 2006, p. 40 apud BARRETO; KUFA; SILVA, 2020, p. 56), entre outras.

1.1.1 Crimes cibernéticos próprios

São aqueles praticados propriamente em razão de bens jurídicos afeitos à tecnologia da informação (BARRETO; KUFA; SILVA, 2020, p. 56), ou seja, “[...] o bem jurídico ofendido é a tecnologia da informação em si” (JESUS; MILAGRE, 2016, p.56).

Marco Túlio Viana (2003, apud CARNEIRO, 2012) classifica como crimes em que a execução e consumação ocorrem por meio do computador, só podendo ser praticados no meio virtual, tendo em vista que o bem jurídico tutelado é a informática, especificamente a inviolabilidade das informações automatizadas, ou seja, os dados.

Como exemplo, tem-se: “[...] o acesso indevido a banco de dados, os ataques de negação de serviço contra sites, o sequestro de informações, a apropriação indevida de dados [...]” (PATURY; SALGADO, 2016, p. 4), “[...] vírus que invadem os

sistemas para destruir informações, roubar informações ou até mesmo danificar o aparelho, seja ele smartphones, computadores ou tablets” (LACERDA; SILVA, 2021, p.15).

Em julgado da 3ª Turma Criminal do Tribunal de Justiça do Distrito Federal (TJ-DF 20160110635069 DF 0009088-86.2016.8.07.0016), publicada em 11/02/2020, em sede de Apelação Criminal (que inadmitiu Recurso Especial), restou comprovada a invasão de dispositivo informático pelo recorrente, que instalou aplicativo espião no notebook de sua namorada, fins de obter informações não autorizadas.

Por meio da perícia realizada no notebook, foram constatados três softwares espiões: *Kgb Keylogger Spy, Refog Keylogger e Netspy Pro*, sendo possível monitorar o envio de dados capturados remotamente, monitoramento das teclas digitadas pelos usuários, capturas de telas do dispositivo, utilização de salas de bate papo, acesso a sites e redes sociais, bem como aplicativo de mensagens e senhas utilizadas.

Entendeu o Tribunal que a conduta do recorrente em instalar software espião configura invasão de dispositivo informático, tipificado no art. 154-A do Código Penal, considerando que pela literalidade do referido dispositivo “a ausência de violação de dispositivo de segurança impede a configuração típica apenas da conduta de invadir”.

Segue o entendimento do Tribunal:

> APELAÇÃO CRIMINAL. INVASÃO DE DISPOSITIVO INFORMÁTICO. FORMA QUALIFICADA. TIPICIDADE CONFIGURADA. CONDENAÇÃO MANTIDA. DOSIMETRIA. CONSEQUENCIAS DO CRIME. ANÁLISE ESCORREITA. QUANTUM. READEQUAÇÃO. PENA PECUNIÁRIA. EXCLUSÃO. IMPOSSIBILIDADE. REDUÇÃO. PROPORCIONALIDADE COM A PENA CORPORAL. SUBSTITUIÇÃO. POSSIBILIDADE.
> I - A expressão "dispositivo informático" não se refere apenas aos equipamentos físicos (hardware), mas também os sistemas, dispositivos que funcionam por computação em nuvem, facebook, instagram, e-mail e outros.
> II - O crime previsto no art. 154-A do CP possui dois núcleos de conduta típica não cumulativos: (i) invadir dispositivo informático alheio, com o fim de obter, adulterar ou destruir dados ou informações sem autorização do titular e (ii) instalar vulnerabilidades, visando obter vantagem ilícita. Pela literalidade do dispositivo, a ausência de violação de dispositivo de segurança impede a configuração típica apenas da conduta de invadir.
> III - Pratica a conduta tipificada no art. 154-A, §3º, do CP aquele que, sem o conhecimento de sua então namorada, instala programa espião no notebook dela, com o fim de monitorar as conversas e atividades e, diante dessa vulnerabilidade, consegue violar os dispositivos de segurança e, com isso, ter acesso ao conteúdo das comunicações eletrônicas privadas e

> outras informações pessoais, inclusive diversas senhas.
> IV - A constatação de que a conduta do réu causou transtornos de ordem psicológica que excederam a normalidade do tipo justifica a avaliação desfavorável das consequências do crime.
> V - Ausente determinação legal acerca do quantum de aumento da pena-base, a par da análise desfavorável de circunstância judicial, a jurisprudência entende adequada a fração de 1/8 (um oitavo) sobre o intervalo entre os limites mínimo e máximo abstratamente cominados no tipo legal.
> VI - A pena de multa é sanção que integra o preceito secundário do tipo penal sob exame e de aplicação cogente. Deve, ainda, ser estabelecido observando os mesmos parâmetros utilizados para fixação da pena corporal.
> VII - Em se tratando de crime cometido no contexto das relações domésticas, mas sem o emprego de violência ou grave ameaça, admite-se a substituição da pena privativa de liberdade por restritiva de direitos, desde que presentes os requisitos do art. 44 do CP.
> VIII - Recurso conhecido e parcialmente provido[6].

Nota-se que o caso supramencionado caracteriza crime cibernético próprio, pela invasão de dispositivo informático, violando informações automatizadas, em que o sistema informático foi o objeto e o meio para executar o crime, ou seja, a ação só ocorre no meio virtual.

Cabe ressaltar que nesses tipos de crimes é necessário o mínimo de conhecimento técnico.

1.1.2 Crimes cibernéticos impróprios

São crimes em que a tecnologia da informação é o meio para agredir bens jurídicos já protegidos pelo Código Penal Brasileiro, já que certas condutas realizadas encontram tipificação em alguns dos tipos penais, sendo suficiente a legislação criminal (JESUS; MILAGRE, 2016, p.56).

Para esses delitos, a tecnologia da informação é a ferramenta para lesionar bens jurídicos tradicionais, quais sejam, honra, patrimônio, costumes, liberdade, etc (BARRETO; KUFA; SILVA, 2020, p. 56).

Com a mesma linha de raciocínio, segue Pinto (2017, p. 16), descrevendo que a conduta encontra-se devidamente tipificada no ordenamento jurídico, com bens já tutelados pelas normas penais, desse modo, o computador e a internet são

---

[6] TJ-DF Apelação Criminal 20160110635069 DF 0009088-86.2016.07.0016, Relatora: NILSONI DE FREITAS CUSTORDIO, 3ª Turma Criminal, Data de Publicação: DJE 11/02/2020. Disponível em: <https://pje2i.tjdft.jus.br/consultapublica/ConsultaPublica/DetalheProcessoConsultaPublica/listView.seam?ca=9da5e2affb6a3bbfb8bf52711cc803c05fd187ddfe216ebe>. Acesso em: 14 jul. 2021.

apenas um meio alternativo de executar o delito.

Trata-se de crime comum, executado pelo meio eletrônico.

São exemplos de crimes cibernéticos impróprios, já tipificados em nossa legislação penal em vigor: calúnia, difamação, injúria, ameaça, divulgação de segredo, furto, dano, estelionato, violação ao direito autoral, escárnio por motivo de religião, assédio sexual, favorecimento da prostituição, escrito ou objeto obsceno, atentado contra a segurança de serviço público, incitação ao crime, apologia de crime ou criminoso, formação de quadrilha ou bando, falsa identidade, inserção de dados falsos em sistema de informações, adulteração de dados em sistema de informações, falso testemunho (WENDT, 2011, p. 81 e 82), induzimento, instigação ou auxílio a suicídio, automutilação realizada por meio de redes de computadores, divulgação de cena de estupro ou de cena de estupro de vulnerável, divulgação de cena de sexo ou de pornografia por qualquer meio de comunicação de massa ou sistema de informática ou telemática (LACERDA; SILVA, 2021, p.15), entre outros.

Wendt (2011) ainda referencia outros exemplos, constantes na legislação especial ou esparsa, citando os seguintes atos normativos: jogo de azar, constante na Lei de Contravenções Penais; crime contra a segurança nacional – Lei nº 7170/83; crimes de preconceito ou discriminação – Lei nº 7716/89; pedofilia – decorrente de alterações no Estatuto da Criança e do Adolescente, que foram introduzidas pela Lei nº 10.829/08; crime contra a propriedade industrial – Lei nº 9.279/96; interceptação de comunicações de informática – Lei nº 9.296/96; lavagem de dinheiro – Lei nº 9.613/98; licitações – Lei nº 8.666/93.

No que tange a exemplo prático de crime cibernético impróprio, a 8ª Câmara de Direito Criminal do Tribunal de Justiça do Estado de São Paulo julgou a Apelação Criminal n. 0002953-45.2018.8.26.0635, publicada em 05/05/2020, referente a roubo qualificado, em que a vítima foi atraída por anúncio que viu na internet, no site OLX, em que era anunciada a venda de uma televisão de 47 polegadas. Ela entrou em contato por ligação telefônica com o suposto vendedor, mostrando interesse na compra, momento em que alegou que já havia uma pessoa interessada. No entanto, o suposto vendedor retornou a ligação marcando um local para que fosse concretizado o negócio.

Chegando ao local indicado, a vítima foi abordada com a sua sogra por dois homens, mediante grave ameaça com uso de arma de fogo, dizendo-lhes que era “golpe da OLX”, subtraindo o dinheiro que a vítima havia sacado para efetuar aquela

compra, levando também a chave do veículo.

A polícia foi acionada, dois homens com as características passadas aos policiais foram abordados e reconhecidos pela vítima e pela testemunha, que também procedeu o reconhecimento nas dependências policiais, ratificando em Juízo.

Diante dos fatos, segue manifestação do Tribunal:

> APELAÇÃO roubo qualificado, consumado. “Golpe da OLX”. Vítima atraída para o local do roubo mediante anúncio de venda de TV. Pagamento em dinheiro. Abordagem naquele local com a expressão “golpe da OLX”, a demonstrar que eram aqueles que a haviam atraído para a armadilha. Abordagem dos apelantes logo após, com reconhecimento formal, art. 266, CPP, no IP e com ratificação em Juízo. Desnecessária em Juízo a formalidade do art. 226, CPP, haja vista ser ratificação de prova do IP, o que foi resultou positivo. Testemunha presencial que reconheceu também ambos. Qualificadoras demonstradas de concurso de agentes e uso de arma. Em havendo interesse na aferição da arma, cabe ao interessado sua apresentação para perícia, art. 156, CPP. Apelantes que afirmando terem estado em posto de gasolina, que iriam se encontrar ou já tinham se encontrado (contradição entre eles) com moças, nada produziram de prova quanto a isso art. 156, CPP. Não é a não recuperação do dinheiro que invalida os reconhecimentos. Materialidade presente, provada a autoria, mantido o decreto condenatório. Art. 59, CP penas bem fixadas, fundamentadas, pelo inusitado do crime premeditado, armado para esse fim com abuso de meios de internet. Necessidade de manutenção. Qualificadora com exacerbação adequada. Regime prisional de acordo, inclusive pela falta de primariedade. NEGADO PROVIMENTO AOS RECURSOS[7].

Em continuidade, houve também manifestação quanto à pena, em discurso que ressaltou a problemática do uso da tecnologia da informação por pessoas mal intencionadas:

> Na fase do artigo 59, do Código Penal, a pena foi fundamentada, reconhecida intensidade do dolo *ab initio*, ou seja, foi premeditado o crime, com toque de sutil inovação tecnológica para o antigo fim de roubo. A Comunidade que acredita nos meios de comunicação virtual para efetuar negócios é seriamente atingida com essa quebra de confiança, tudo a justificar a elevação inicial.

O julgado referenciado é apenas um exemplo de crime cibernético impróprio. Como citado anteriormente, há vários, sendo esse tipo de crime o de maior

---

[7] TJ-SP – APR: 00029534520188260635 SP, Relator: Ruy Alberto Leme Cavalheiro, Data de Julgamento: 21/06/2018, 3ª Câmara de Direito Criminal, Data de Publicação: 05/05/2020. Disponível em: <https://tj-sp.jusbrasil.com.br/jurisprudencia/842621957/apelacao-criminal-apr-29534520188260635-sp-0002953-4520188260635/inteiro-teor-842621977>. Acesso em: 15/07/2021.

incidência no meio virtual, caracterizando-se pelo uso do computador ou outra tecnologia (mesmo sem conhecimento técnico), como meio ou facilitador para efetivação de crime comum.

1.2 Considerações acerca dos crimes cibernéticos no ordenamento jurídico brasileiro

Com o surgimento da sociedade da informação oriunda do desenvolvimento da tecnologia, o Direito passou a reconhecer a relevância das condutas em ambientes de informática, percebendo que havia outros valores penalmente relevantes, considerando-a merecedora de tutela, iniciando embates referentes às normas protetoras dos cidadãos em decorrência das tecnologias e a má intenção em seu uso (JESUS; MILAGRE, 2016).

Discorrem Damásio de Jesus e José Antônio Milagre que algumas figuras delitivas foram surgindo, embora não tenha sido fácil a aprovação de legislações que tipificassem os crimes cibernéticos, levando em conta que a ação do direito é devida, fins de preservar bens mais relevantes e imprescindíveis das relações sociais, ocorrendo intervenção mínima na vida dos cidadãos.

Em meio aos debates sobre criminalizar certas condutas na rede, surgiram posicionamentos que colocaram em pauta o Direito Penal, e conforme entendimento dos autores supracitados, a intervenção mínima como princípio consagrado do Direito Penal foi desconsiderada, passando a considerar a proteção e segurança da sociedade digital, acentuando a tutela penal dos direitos difusos e não necessariamente a proteção de bens jurídicos individuais, o que para muitos autores é o foco do Direito Penal.

Mesmo diante de reflexões e debates acerca do assunto, não se pode negar a existência de novas práticas para crimes antigos, que já têm tipificação em nosso ordenamento jurídico. Da mesma forma, surgiram novos delitos atentatórios a bens jurídicos não tipificados.

E diante de toda essa problemática, ao que indica, o caminho não será trilhado no sentido de criação de leis específicas, mas sim de alterações no Código Penal e de Processo Penal.

Contudo, ainda que o Decreto-Lei n. 2.848/40 – Código Penal Brasileiro faça referência a alguns delitos cibernéticos, até o momento é omisso quanto ao meio

virtual, como bem protegido pelo Direito Penal.

É certo que ainda há muitos desafios pela frente, e nesse sentido, são necessárias medidas que se adequem a cada caso específico, pois as lacunas existentes favorecem os criminosos.

Para tanto, será discutido, embora não exaustivamente, considerações acerca de alguns dispositivos legais constantes em nosso ordenamento.

De início, importa-se destacar o direito à privacidade, disposto na Constituição Federal de 1988, em seu art. 5º, X: “[...] são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação” (BRASIL, 1988).

Nesse sentido, Gilmar Mendes, Ministro do Supremo Tribunal Federal (STF), (2007, p. 307) enfatiza que:

> O direito à privacidade, em sentido mais estrito, conduz à pretensão do indivíduo de não ser foco da observação por terceiros, de não ter os seus assuntos, informações pessoais e características particulares expostas a terceiros ou ao público em geral.

Embora o Código Penal Brasileiro seja de 1940 e por vezes acaba não conseguindo atender às atuais demandas sociais, traz desde sua criação, mesmo que de forma indireta, ilícitos inerentes ao sistema cibernético (PATURY; SALGADO, 2016).

Os autores retratam ainda que, em nosso Código Penal, não havia dispositivos que tratavam sobre crimes cibernéticos próprios, emergindo algumas legislações, fins de regulamentar, alterar ou complementar o Código Penal Brasileiro.

De forma sucinta segue abaixo algumas legislações mencionadas por Patury e Salgado (2016):

- Lei 8.069/90 (Estatuto da Criança e do Adolescente), que pela Lei 11.829/08 passou por alguns ajustes, tipificando a pedofilia digital;

- Lei 9.504/97, oriunda da necessidade de proteger o processo de digitalização do sistema eleitoral brasileiro;

- Lei 9.609/98, que trata da proteção da propriedade intelectual e comercialização de programas de computador;

- Lei 9.983/2000, que trouxe alterações à legislação penal, acrescentando

ilícitos específicos ocorridos nos sistemas informáticos;

- Lei 9.964/2000, que tipificou como conduta ilícita os crimes contra a ordem tributária, efetuada também por meio dos sistemas automatizados.

Importante salientar outras legislações subsequentes às citadas anteriormente, como a Lei 12.735/12, oriunda do Projeto de Lei n. 84/99 apresentado em 24 de fevereiro de 1999, que tramitou durante 13 anos até sua aprovação, desfigurando-se de dezoito artigos para apenas quatro (JESUS e MILAGRE, 2016, p. 72 e 73), tendo como ponto principal a criação de delegacias especializadas no combate aos crimes cibernéticos.

O projeto tinha como proposta a punição dos crimes praticados no meio virtual. Ficou popularmente conhecida por “Lei Azeredo” (por ter como relator tanto na Câmara quanto no Senado Federal, o político Eduardo Azeredo) e também por “AI-5 Digital”, por haver no projeto pontos considerados polêmicos, que violavam direitos fundamentais dos clientes da internet (SEGUNDO, 2016, p. 28 e 29).

Igualmente, em 2012, foi sancionada a Lei n. 12.737, após o caso midiático da atriz Carolina Dieckman, que supostamente teve suas fotos íntimas divulgadas na internet. E assim, houve a tipificação da “invasão de dispositivo informático, a interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública e a falsificação de cartão de crédito ou débito” (JESUS; MILAGRE, 2016, p. 75).

Com o advento da lei, foram acrescentados dois artigos e alterados outros dois no Código Penal. No entanto, os tipos penais se valeram de conceitos imprecisos, não adequando tipicamente eventual conduta à norma, bem como não conseguiu exaurir todas as espécies de crimes cibernéticos próprios e impróprios, além de apresentar desproporção na sanção prevista em relação aos delitos tradicionais (BARRETO; KUFA; SILVA, 2020, p. 130 e 131).

A referida lei criou as figuras previstas no art. 154-A e 154-B do Código Penal, que passaram por modificações recentes pela Lei 14.155/21, que será discutida adiante.

Na percepção de Jesus e Milagre (2016, p. 75), as Leis 12.735 e 12.737, ambas sancionadas em 2012, foram “impulsionadas por um casuísmo, populismo penal”, que por terem sido aprovadas apressadamente, sem haver muitas discussões sobre o assunto, poderiam gerar margens a enquadramentos errôneos e atitudes violadoras de direitos e garantias dos cidadãos.

Em 23 de abril de 2014, foi sancionada a Lei n. 12.965 – Marco Civil da Internet, garantindo direitos e deveres aos atores da Internet brasileira, e por isso, passou a ser considerada como “Constituição da Internet”. Oriunda de um projeto por “construção colaborativa”, que ficou acessível em consulta pública, recebendo mais de duas mil contribuições entre os meses de novembro de 2009 e junho de 2010 (JESUS; MILAGRE, 2016, p. 182).

Foi proposta devido à resistência social quanto à Lei Azeredo, possuindo três pilares fundamentais: “a liberdade de expressão, a proteção da privacidade e o estabelecimento da neutralidade da rede”, impondo ainda obrigações de responsabilidade civil aos usuários e provedores (PINTO, 2017, p. 39).

O Marco Civil da Internet iniciou de forma inovadora, tendo em vista o engajamento e grande articulação política, além da interação da sociedade que contribuiu sobremaneira para sua sistematização.

E não é à toa que é considerada a “Constituição da Internet”, afinal, traz em seu bojo normas que buscam assegurar a liberdade, a privacidade e a neutralidade da rede, com intuito de tornar a internet um ambiente seguro e também igualitário, por abarcar não somente os usuários, mas também empresas e provedores de internet.

Em 2015, foi sancionada a Lei n. 13.185, instituindo o programa de combate à intimidação sistemática, denominada *“bulling”*, propondo combater o “cyberbulling” (intimidação sistemática na rede mundial de computadores) (BRASIL, 2015).

A Lei nº 13.718 de 24 de setembro de 2018, introduziu na lei penal o art. 218-C, que criminaliza a divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia, por meio de comunicação de massa ou sistema de informática ou telemática, entre outros meios (BRASIL, 2018).

Com a Lei n. 13.964, de 24 de dezembro de 2019, instituindo o pacto anticrime no Brasil, foi alterada a natureza jurídica da ação penal no delito de estelionato, passando a exigir a representação da vítima, como condição de procedibilidade, tornando-a, assim, ação pública condicionada à representação, excetuando se a vítima for a Administração Pública, direta ou indireta; criança ou adolescente; pessoa com deficiência mental; ou ainda maior de 70 (setenta) anos de idade ou incapaz (BRASIL, 2019).

Recentemente foi sancionada a Lei n. 14.155/21, objeto de estudo deste trabalho, trazendo alterações no Código Penal e no Código de Processo Penal

(Decreto-Lei n. 3.689, de 3 de outubro de 1941), tornando mais gravosos os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet e definindo a competência nas modalidades de estelionato (BRASIL, 2021).

Ressalta-se ainda a integração do Brasil frente à cooperação internacional em matéria digital e prevenção aos crimes cibernéticos, no que tange a Convenção de Budapeste de 2001, tratado internacional que entrou em vigor em 1º de julho de 2004, contemplando diversos aspectos e conceitos sobre os crimes cibernéticos, traduzindo em importante marco para a comunidade penal internacional, envolvendo mais de 60 países e reconhecendo a soberania dos Estados signatários.

Tendo o Brasil sido convidado pelo Conselho da Europa a integrar o conjunto de partes signatárias do tratado em 11/12/2019, somente em 22/07/2020 o texto do tratado foi encaminhado, por meio da Mensagem 412/2020, pela Presidência da República ao Congresso Nacional, fins de adesão do Estado brasileiro ao instrumento. E quase um ano depois, em 17/06/2021, a Câmara, pela Comissão de Relações Exteriores, iniciou o procedimento com a tramitação de urgência do Projeto de Decreto Legislativo 255, tendo atualmente como relator o senador Vitor Hugo. No entanto, o segundo protocolo da convenção, encontra-se em negociações (POLIDO, 2021).

Seria um fator positivo, se o Congresso Nacional considerasse o momento para efetivação da adesão do Brasil à Convenção de Budapeste, tendo em vista a importância da cooperação internacional no combate aos crimes cibernéticos, oportunizando maior participação e envolvimento do Brasil nas instituições de enfrentamento à criminalidade transnacional.

Embora haja no Brasil lei que disciplina o uso da internet e sua inviolabilidade, o uso da Internet para prática de crimes virtuais tem se tornado um campo fértil, seja para prática de crimes com valores ou para a subtração de informações pessoais. A cada dia surgem novos tipos de golpes e novos *modus operandi*, fazendo novas vítimas e dificultando o trabalho de investigação da polícia.

2 O ESTELIONATO VIRTUAL

O estelionato virtual configura entre os tipos de crimes mais recorrentes, que utilizam como meio o computador ou outros dispositivos eletrônicos e a internet nas práticas delituosas, caracterizando-se pela agressão a bens jurídicos protegidos pelo Código Penal Brasileiro (crimes cibernéticos impróprios).

Os crimes virtuais em quase todo o país são crescentes e desde 2020 a prática tem se intensificado, principalmente devido à pandemia da Covid-19[8], em que as pessoas passaram a utilizar com mais frequência as redes sociais e aplicativos de mensagens nos mais diversos atendimentos no mercado virtual, destacando que os criminosos utilizam de “engenharia social”[9] para aplicar os golpes, principalmente o estelionato virtual.

Em 2020, houve um aumento de 265% nos crimes praticados no ambiente virtual no Estado de São Paulo. No Rio de Janeiro, durante o período de isolamento, os casos de golpes na internet tiveram um aumento de 11,8% do total de crimes, segundo o Instituto de Segurança Pública (ISP). Em Minas Gerais, o número de crimes virtuais teve uma alta de 50% em 2020, segundo informações da polícia civil. (GOUSSINSKY, 2021).

A Internet proporciona ao criminoso uma sensação de anonimato e leva muitas vezes a prática de uma série de crimes, acreditando que jamais será descoberto, visto que o delinquente pode praticar sua atividade criminosa a partir de qualquer lugar do mundo, dificultando o rastreamento e a descoberta em tempo hábil de evitar transtornos e danos às vítimas, fato que pode mudar com o advento da Lei 14.155/2021 que torna mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet.

2.1 Aspectos Gerais do crime de estelionato

A palavra estelionato origina do latim *stellionatu*, que veio de *stellio*, que é um

[8] A Covid - 19 é uma doença infecciosa causada pelo novo coronavírus (SARS-CoV-2). Disponível em: https://www.paho.org/pt/covid19. Acesso em: 17 jul. 2021.

[9] Engenharia social é uma técnica empregada por criminosos virtuais para induzir usuários desavisados a enviar dados confidenciais, infectar seus computadores com malware ou abrir links para sites infectados. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-social-engineering. Acesso em: 17 jul. 2021.

tipo de camaleão com manchas na pele parecidas com estrelas, que em latim significa *stella* (NOGUEIRA, 2014). O camaleão troca de pele para que seja confundido com o ambiente, facilitando a captura de suas presas, ganhando fama de trapaceiro, similaridade com o estelionatário que se molda de acordo com o meio em que vive para atingir os objetivos de iludir as vítimas na obtenção de vantagem pretendida.

O significado descrito no dicionário de "estelionato" configura a "obtenção de vantagens em proveito próprio por fraude ou logro; burla [...]" (DICIO, 2021).

A conduta humana de enganar não é fruto da modernidade, trata-se de comportamento que remonta os primórdios da humanidade.

Há na Bíblia, um dos livros mais antigos da história da humanidade, registro de conduta ardilosa, constante no capítulo 27 de Gênesis, em que registra a história de Jacó, que enganou seu pai Isaque, passando-se por seu irmão mais velho Esaú, com intuito de receber a benção que estava destinada ao primogênito[10].

Como bem preceitua Rogério Greco (2012, p. 228): "Desde que surgiram as relações sociais, o homem se vale da fraude para dissimular seus verdadeiros sentimentos e intenções para, de alguma forma, ocultar ou falsear a verdade, a fim de obter vantagens que, em tese, lhe seriam indevidas".

O Estelionato está tipificado no Código Penal Brasileiro, no artigo 171, caput: "Obter, para si ou para outrem, vantagem ilícita em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento" (BRASIL, 1940).

O artifício é de natureza material, manifestando-se através de meio ou objeto que possibilite a concretização da fraude, podendo ser executado por disfarces, truques, efeitos especiais, etc. O ardil é de natureza material, porém com cunho intelectual, já que o criminoso utiliza-se de meios argumentativos para que possa enganar a vítima, usando de astúcia, sutileza e sagacidade. E outro meio fraudulento, abrange qualquer outra artimanha que possa enganar a vítima, e sua interpretação analógica fica a cargo do julgador.

A configuração do crime de estelionato exige que a conduta do agente seja composta do binômio: vantagem ilícita e prejuízo alheio.

Greco (2012, p. 98) conceitua o estelionato como: "Qualquer meio fraudulento

[10] Disponível em: <https://www.bibliaonline.com.br/acf/gn/27>. Acesso em: 19 jul. 2021.

utilizado pelo agente, seja mediante dissimulações, seja até mesmo uma reticência maliciosa, que faça a vítima incorrer em erro, já será suficiente para o raciocínio relativo ao delito de estelionato".

Entende ainda, que o crime de estelionato se configura "[...] quando o agente emprega qualquer meio fraudulento, induzindo alguém em erro ou mantendo-o nessa situação e conseguindo, assim, uma vantagem indevida para si ou para outrem, com lesão patrimonial alheia".

O bem jurídico tutelado é o patrimônio daquele que sofreu prejuízo com o comportamento fraudulento empregado. Referido bem jurídico encontra amparo constitucional, conforme preconiza o art. 5°, caput e incisos XXII e XXIII, da CF/88:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] XXII - é garantido o direito de propriedade; XXIII - a propriedade atenderá a sua função social; [...].

Conforme entendimento de Coelho (2015, p. 599), a tutela penal do patrimônio é abarcada pela Constituição Federal de 1988, conforme dispositivo já citado acima, sendo o patrimônio "[...] um conjunto de bens ou interesses de valor econômico, vinculados a um titular, pessoa física ou jurídica. [...] representado por bens materialmente considerados ou interesses, todos representativos de valor pecuniário".

O sujeito ativo pode ser tanto aquele que emprega a fraude, como também aquele que recebe a vantagem ilícita. No polo passivo, pode ser qualquer pessoa, que seja prejudicada patrimonialmente, enganada pela fraude perpetrada, mesmo que não seja prejudicada economicamente. Sendo possível como sujeito passivo do crime de estelionato, pessoa jurídica, na condição de prejudicada economicamente pelo golpe (GONÇALVES, 2018, P. 485).

Trata-se de um crime doloso, pois o emprego do dolo por meio da fraude, como elemento subjetivo é o componente substancial para a configuração do delito, que não admite a forma culposa. Admite, no entanto, a forma tentada.

As formas de execução do crime de estelionato são as mais diversas existentes, embora a atuação e o êxito do crime dependa da confiança que a vítima adquire em relação ao criminoso, que age dolosamente com emprego de artifício, ardil ou qualquer outro meio fraudulento, objetivando enganar a vítima.

2.2 Estelionato Virtual: fraude eletrônica

O uso da internet tornou-se um instrumento importante em todas as formas de interação da sociedade, seja pelas relações interpessoais, econômicas ou sociais. A riqueza de informações e a facilidade de acesso ao ambiente virtual, possibilita a utilização desses dados para a prática criminosa, principalmente o estelionato virtual na modalidade fraude eletrônica.

O crime de estelionato preconizado pelo art. 171 do Código Penal prevê o enquadramento de fraude eletrônica, “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”, com pena de quatro a oito anos e multa; considerando ainda, a relevância do resultado gravoso, aumenta-se de um terço a dois terços, se o crime é praticado mediante a utilização de servidor mantido fora do território nacional, dispositivo inserido com o advento da Lei n. 14.155/21.

A Lei nº 14.155/21, publicada recentemente, qualifica os ilícitos mediante fraude eletrônica, aumentando as penas em relação a tipologia do crime, promovendo segurança no âmbito jurídico aos profissionais na aplicação da sansão penal.

A referida lei traz alterações ao Código Penal (Decreto Lei nº 2.848/40) e ao Código de Processo Penal (Decreto Lei Nº 3.689/41), com disposições jurídicas recrudescendo a punição de crimes eletrônicos e informáticos, e ainda, hipótese de competência no âmbito criminal.

Costa, Fontes e Hoffmann (2021) explicam que no estelionato, “a fraude é usada como meio de obter o consentimento da vítima, que entrega voluntariamente o que o agente deseja” para consumar o crime.

Barreto e Wendt (2020, p. 202) versa que:

> [...] os criminosos tem se valido dos avanços tecnológicos para potencializar suas ações, especialmente no que diz respeito às fraudes cometidas em ambiente virtual. Muito embora exista legislação determinando aos entes federativos a estrutura de setores ou delegacias especializadas na repressão dos crimes de Internet, o que vemos ainda são estruturas deficientes na investigação criminal dessas infrações.

Um exemplo prático de crime impróprio de estelionato virtual, na modalidade fraude eletrônica, ocorreu em Mato Grosso, no mês de abril de 2021, quando foi presa uma suspeita que se apresentava como funcionária bancária e induzia a vítima a entregar o cartão a um falso motoboy. A suspeita entrava em contato com a vítima, por telefone, se apresentava como funcionária do banco e comunicava a tentativa de compras fraudulentas. Durante a conversa, a suspeita dizia que estava fazendo o bloqueio do cartão e induzia a vítima a fornecer dados pessoais e bancários da conta. Conforme o Delegado Ruy Guilherme Peral da Silva, da Delegacia de Repressão a Crimes Informáticos (DRCI) da Polícia Civil de Mato Grosso, os crimes virtuais e fraudes tem gerado prejuízo à população (MOLINA, 2021).

Outro tipo de fraude muito utilizada no Brasil é aplicada pelo golpe de *phishing*[11], realizado por meio de comunicações eletrônicas (e-mail ou telefone), em que o golpista finge ser um indivíduo ou organização de confiança, objetivando obter informações pessoais confidenciais (BELCIC, 2020).

Uma das formas de execuação é através de correio eletrônico fraudulento, em que os cibercriminosos enviam mensagens falsas em nome de instituições financeiras e empresas para iludir a vítima a ceder informações (ROHR, 2021).

Nessa senda, numa pesquisa realizada pela Kapersky no segundo trimestre de 2020, que gerou o relatório "*Spam and Pishing*", publicada em 07 de agosto do mesmo ano, foi constatado que os brasileiros foram um dos principais alvos de phishing do mundo durante os primeiros meses da pandemia. Cerca de um a cada oito usuários de internet do País (13%) acessaram de abril a junho de 2020, ao menos um link direcionando a páginas maliciosas. Referido índice está bem acima da média mundial (8,26%), colocando o Brasil como o quinto país com maior proporção de usuários atacados.

Entre os meses de março, abril e maio de 2020, os ataques contra aparelhos móveis mais que dobraram, em comparativo ao período de pré-pandemia. A média local de tentativas de ataque de phishing contra celulares era de 10 por minuto, no

[11] "Phishing é uma técnica de crime cibernético que usa fraude, truque ou engano para manipular as pessoas e obter informações confidenciais. [...] O cibercriminoso vai 'pescar' (em inglês, 'fishing') com uma atraente 'isca' para fisgar as vítimas do vasto 'oceano' dos usuários da internet. O ph em 'phishing' vem de 'phreaking de telefone' que surgiu em meados de 1900, no qual os 'phreaks', ou seja, entusiastas, faziam experimentos com as redes de telecomunicações para descobrir como elas funcionavam. Phreaking + fishing = phishing." (BELCIC, 2020).

mês de fevereiro de 2020, quando se deu a confirmação do primeiro caso de Covid-19 no Brasil, e nos três meses seguintes, o índice aumentou para mais de 23 tentativas por minuto. Segundo Fabio Assiolini, analista sênior de segurança da Kapersky, os cibercriminosos intensificaram o envio de *pishing,* principalmente via aplicativos de celulares, nos primeiros meses de confinamento, devido a pandemia de Covi-19 (RODRIGUES, 2020).

A virtualização tornou-se uma facilitadora na vida das pessoas, abrindo, porém, as portas para atuação de criminosos virtuais, já que não há uma ferramenta que assegure a proteção integral das informações solicitadas durante procedimentos no uso da internet.

Como já fora exposto, existe tipificação para o cometimento de crime mediante obtimento de vantagem ilícita que induz a vítima ao erro. Assim, o estelionato virtual é apenas a mudança de meio, empregada através do meio virtual, de utilização dos dados virtuais.

A fraude é o ato que potencializa a vítima ao engano, através da configuração dos elementos essenciais do tipo, já previstos no art. 171 do Código Penal, quais sejam: fraude, erro, vantagem ilícita e prejuízo alheio, bem como o dolo. Portanto, a fraude eletrônica também não se trata de nova modalidade de estelionato, o legislador com o advento da Lei n. 14.155/21 apenas delimitou o meio do cometimento da fraude, trazendo um grau maior de reprovabilidade, aumentando desse modo, a pena da conduta fraudulenta, se for cometida por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou qualquer outro meio fraudulento análogo.

2.3 Perfil e *modus operandi* do sujeito ativo de crime de estelionato virtual

O pensamento sobre o perfil criminoso cibernético, provavelmente criado através de inspiração em filmes e publicidade, era de pessoa “jovem, feia, mas muito estudiosa e com conhecimento extraordinário no ramo da informática” (BARRETO; BRASIL, 2016, p. 22). Conforme entendimento de Glenny (2008) in (BARRETO; BRASIL, 2016, p. 22) a maioria dos cibercriminosos são do sexo masculino (95%), com pouca habilidade de comunicação e adquirido conhecimentos da prática do

cracKing[12] entre os 13 e 15 anos, antes de ter a formação dos valores morais consolidades.

Entretanto, esse estereótipo não condiz com a atual realidade, em que qualquer pessoa, em qualquer faixa etária, por meio de uso da internet pode aprender técnicas conceituais e práticas para tornar um potencial criminoso.

Paesani (2010) citado por Barreto e Brasil (2016, p. 22) afirma que “o perfil dos criminosos cibernéticos se destaca pela autoconfiança e pelo sentimento de anonimato e impunidade, especialmente em razão do contato com a vítima ser normalmente à distância”. O autor relata ainda a mesma linha de raciocínio de Strano, especialista italiano da Polícia do Estado, o qual afirma que: “[...] Para essas pessoas, a tela do computador funciona como escudo de proteção que se projeta no mecanismo do pensamento; ou seja, a falta de percepção da ilegalidade do comportamento, dos riscos assumidos e do dano causado à vítima”.

Importante destinguir nesse contexto a figura dos “*hackers*” e dos “*crackers*”, já que muitos fazem confusão conceitual relacionada aos termos. Apesas das duas palavras serem muito parecidas e também servirem para designar indivíduos com habilidades e conhecimentos avançados em computadores, dispositivos móveis e na rede mundial, elas se diferem.

Ao contrário do que a maioria das pessoas acreditam, os *hackers* não agem com intuito de tirar proveito de alguma situação, eles tentam ao máximo diminuir os riscos de segurança em uma aplicação. Possuem a capacidade de criar funcionalidades e aplicações para computadores, dispositivos móveis e internet, modificando softwares, hardwares e aplicando seus conhecimentos para desenvolver soluções de segurança, criando ou adaptando novos sistemas. Já os *crackers*, possuem o mesmo conhecimento, no entanto, utilizam para praticar ações maléficas, de coletar informações, descobrir senhas de acesso a redes e quebrar códigos de segurança em benefício próprio, praticando delitos virtuais (ROSA, 2020).

Há também, a figura dos pichadores digitais, que alteram páginas da internet, substituindo o conteúdo por desenhos, vídeos ou música, como forma de protesto, geralmente com cunho político; cibervândalos que agem simplesmente com intuito

[12] CracKing é uma técnica usada para violar software de computador ou um sistema de segurança de computador com más intenções. Disponível em: <https://www.avast.com/pt-br/c-cracking>. Acesso em: 18 jul. 2021.

de causar danos a outra pessoa; ciberterrrorista, que usam seu conhecimento em prol de causas políticas extremas; *phreakers*, que utilizam técnicas de manipulação e conhecimento na área da telefonia (BARRETO; BRASIL, 2016); entre outras.

O cibercriminoso é aquele indivíduo cujo *modus operandi* (modo de operação) é praticado utilizando-se das tecnologias da informação com objetivo de cometer crimes e obter algum proveito pessoal.

Nesse contexto, o estelionato virtual, tem como *mudus operandi* a utilização de meios digitais para o cometimento de crime mediante obtimento de vantagem ilícita que induz a vítima ao erro.

Ressalta-se que o estelionatário atual não precisa necessariamente possuir conhecimento técnico, podendo ser qualquer pessoa com a finalidade e predisposição em cometer crimes.

E a Internet por ter se tornado campo fértil para cometimento de crimes virtuais, a cada dia surgem novos tipos de golpes e com novos *modus operandi*, fazendo novas vítimas e dificultando o trabalho de investigação da polícia.

3 ADVENTO DA LEI 14.155/21

Com as inovações tecnológicas que surgiram nos últimos anos e o crescimento exponencial do uso da rede mundial de computadores, trazendo facilidade para a vida das pessoas, surgiram também vulnerabilidades exploradas por pessoas mal intencionadas, com o propósito de práticas delituosas.

A variedade de delitos virtuais ocorridos ultimamente tem sido assombrosa, principalmente após a pandemia da Covid-19, que alterou os hábitos da humanidade, forçando a adaptação das relações interpessoais e sociais, trazendo situações nunca vista antes, com uma nova estrutura.

E em face de ações preventivas, buscando conter o vírus, houve isolamento e distanciamento social, copelindo a sociedade a uma ambientação ao mundo virtual, e particularmente a internet foi indispensável nesse processo, garantindo a comunicação, o acesso à informação, a movimentação no comércio eletrônico, acesso à prestação de serviços públicos, vídeoaulas, teletrabalho, telemedicina e maior interação através de redes socias. Contudo, decorreu um aumento sem precedentes na quantidade de crimes cibernéticos.

Em pesquisa experimental sobre o uso da Internet no Brasil durante a

pandemia do Novo Coronavírus - Painel TIC Covid-19, realizado pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), pelo Departamentodo do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), ligado ao Comitê Gestor da Internet no Brasil (CGI.br), os resultados apontaram para uma intensificação do uso das tecnologias de informação e comunicação nesse período, com a ampliação da proporção de usuários realizando atividades de comunicação, acesso à informação, serviços, cultura e comércio eletrônico[13].

O Painel TIC COVID-19 identificou um aumento expressivo na realização de atividades na internet. A pesquisa apontou estimativa de usuários de internet, em cada atividade, sendo que: 49% realizaram atividades de trabalho pela internet; 72% buscaram informações relacionadas à saúde; 43% pagaram por serviços de filmes ou séries; 66% compraram produtos ou serviços pelo comércio eletrônico, proporção que era de 44% em 2018; 46% usaram aplicativos de mensagens instantâneas para mediar compra de produtos ou serviços, que era de 26% em 2018;

Diante de dessas estimativas, é possível perceber o quanto o uso da internet se tornou imperioso na vida das pessoas, aumentando o risco de vulnerabilidades a crimes virtuais.

Em Mato Grosso, a Superintendência do Observatório da Violência da Secretaria de Estado de Segurança Pública (Sesp-MT), divulgou dados correspondentes ao total de Boletins de Ocorrências com práticas de estelionato registrados em todo o estado no período de janeiro a junho, estimando um comparativo entre os anos de 2019 e 2020. Desse modo, contabilizou-se durante esse período 4.305 registros em 2020, número superior a 2019 que foram 3.707 registros. Somente em Cuiabá, foram 1.760 registros em 2020 em comparativo a 2019, que foram 1.338 registros[14].

Segundo os dados, os principais *modus operandi* dos criminosos, na modalidade estelionato, em Mato Grosso, no período compreendido entre janeiro a junho de 2020 foram:

---

[13] PAINEL TIC COVID-19. Pesquisa sobre o uso da Internet no Brasil durante a pandemia do Novo Coronavírus, 1ª EDIÇÃO: Atividades na Internet, Culturae Comércio Eletrônico, 2020. Disponível em: <https://cetic.br/media/docs/publicacoes/2/20200817133735/painel_tic_covid19_1edicao_livro%20eletr%C3%B4nico.pdf>. Acesso em: 16/07/2021.

[14] Disponível em: <http://www.sesp.mt.gov.br/-/15219266-golpes-por-whatsapp-lideram-crimes-de-estelionato-em-mato-grosso>. Acesso em: 16/07/2021.

- Clonagem de WhatsApp (23.9%);
- Uso indevido de dados pessoais (15,7%);
- Boleto falso (10.7%);
- Golpe por sites de comércio eletrônico (8,4%);
- Venda simulada/produto não entregue (7,4%);
- Golpe por redes sociais Facebook/Instagram (6,6%);
- Cartão clonado (6.6%);
- Outros - cobrança aluguel, golpes pessoais (5,7%);
- Compra/ transação bancária não autorizada (4,2%);
- Empréstimo falso (2,4%),
- Cheque falso/adulterado (2,1%);
- Site falso (1,9%);
- Golpe pelo whatsapp (1,9%);
- Golpe das panelas (produto com qualidade inferior) (1,3%);
- Golpe por contato telefônico - funcionário bancário (0.8%);
- Golpe do falso sequestro (0,4%), dentre outros.

Os dados referenciados só demonstram uma parte da demanda desse tipo de crime. Sem falar que há uma parcela de ocorrências que não são devidamentes comunicadas às autoridades.

Possivelmente, os índices reais desse tipo de criminalidade são maiores que aqueles oficialmente registrados e documentados pelos órgãos competentes, por vários motivos, como: o desconforto que a vítima sabe que irá passar no decorrer do trâmite processual, a dificuldade que enfrentará diante de conhecidos e curiosos tendo conhecimento da ocorrência do crime, medo de denunciar devido o delito ter sido praticado por alguém de seu âmbito familiar (QUEIROZ, 2015) ou do círculo de amizade, além da vergonha, descrença nas autoridades, medo devido a ameaças, crença de impunidade dos criminosos, dentre outros.

Diante desse cenário de crescimento da criminalidade cibernética, intensificada pela pandemia do Novo Coronavírus, tornando imperioso o uso da internet nas mais variadas atividades do dia a dia, expondo as pessoas a situações de risco, eis que surge a Lei 14.155/21.

A referida Lei Ordinária é novíssima. Entrou em vigor em 28 de maio de 2021, promovendo algumas alterações no Código Penal e Código de Processo

Penal, encrudecendo as penas para os crimes de violação de dispositivos informáticos (art. 154-A do CP), furto (art. 155 do CP) e estelionato (art. 171 do CP) cometidos pela internet ou de forma eletrônica, determinando também, competência para julgamento de algumas modalidades de estelionato no domicílio da vítima e em caso de pluralidade de vítimas, firmando competência por prevenção (BRASIL, 2021).

Oriunda do Projeto de Lei n. 4.554/2020, de autoria do senador Izalci Lucas, foi apresentada em 07/12/2020 e tramitou em regime de urgência, transformando em Lei Ordinária 14.155/2021, em 27/05/2021, entrando em vigor na data de sua publicação, em 28/05/2021 (CÂMARA DOS DEPUTADOS, 2021).

Perante a necessidade de adaptar as relações jurídicas ao cenário social vivenciado no momento, fins de mitigar as ações criminosas, sendo indispensável a adaptação do arcabouço penal em face dessas novas necessidades, o senador Izalci Lucas dispôs a seguinte justificativa no PL 4.554/2020:

> O Jornal Folha de São Paulo de 26/08/2020 noticia que a pandemia fez aumentar drasticamente o número de fraudes cometidas de forma eletrônica, gerando perdas de aproximadamente R$ 1 bilhão. Segundo a mesma fonte, a alta foi de 70% e os montantes envolvidos já se apresentam como empecilho à redução de juros ao consumidor, vez que se elevaram os riscos envolvidos. Esse tipo de crime tem atingindo, inclusive, os beneficiários do auxílio emergencial. Estima-se que 600 mil fraudes foram praticadas somente no pagamento do benefício. São inúmeros os canais de imprensa que vem noticiando a explosão de ocorrências em que criminosos estão lucrando durante a pandemia. Observa-se que tem havido um aumento crescente de crimes dessa natureza nos últimos anos, mas que o número disparou durante a pandemia. A situação agrava-se ainda mais quando os servidores de rede utilizados para o crime estão situados fora do país. O Banco Central emitiu alerta sobre fraudes durante a pandemia, quando os golpes via WhatsApp ultrapassaram 11 milhões de casos. Bandidos usam inclusive aplicativos de informação sobre o Coronavirus para enganar os cidadãos de bem. Nosso país alcançou o terceiro lugar no ranking mundial em registros de fraudes eletrônicas. Os criminosos, em função da branda legislação brasileira, estão escolhendo o Brasil como terreno fértil para seguirem impunes. O Jornal O Globo de 14 de julho informa inclusive que os cibercriminosos brasileiros estão expandindo suas atividades aplicando fraudes nos Estados Unidos, Europa e China. Líderes em segurança contra fraudes lamentam todo o esforço para combater esse tipo de crime enquanto a legislação considerar essa prática como um crime menor, cujas penas são muitas vezes substituídas por penas “alternativas”. O volume de fraudes já começa a afetar a economia do país, gerando perda do poder aquisitivo e também perdas emocionais por parte das vítimas. Diante do exposto, é medida urgente que aprovemos meios mais rigorosos para punir esse tipo de crime que assola o país. (PEREIRA, 2021).

As modificações trazidas pela nova lei são interessantes e já estão sendo motivos de debates no âmbito jurídico. É certo, que com o advento da lei foram

sanadas algumas falhas com a alteração de forma significativa do crime de invasão de dispositivo informático e os procedimentos a ele equivalentes, iserindo também novas tratativas aos crimes de furto e estelionato, condutas já tipificadas criminalmente.

Para melhor compreensão, serão abordadas nos próximos tópicos as alterações na legislação Penal e Processual Penal Brasileira com o advento da Lei 14.155/21.

3.1 Crime de violação de dispositivo informático

As alterações iniciais promovidas pela Lei 14.155/21 recaíram sobre o artigo 154-A do Código Penal Brasileiro, este que foi incluído no CPB pela Lei nº 12.737, de 2012, conhecida popularmente por “Lei Carolina Dieckman”, responsável pela tipicação criminal de delitos informáticos no Brasil (BRASIL, 2012).

Visando melhor compreensão das mudanças inseridas no art. 154-A, será apresentado abaixo quadro comparativo com a redação anterior à Lei n. 14.155/21 e a atual. Posteriormente será realizada a sua análise:

Redação anterior à Lei n. 14.155/21	Redação atual
Art. 154-A. Invadir dispositivo informático **alheio**, conectado ou não à rede de computadores, **mediante violação indevida de mecanismo de segurança** e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do **titular do dispositivo** ou instalar vulnerabilidades para obter vantagem ilícita:.	Art. 154-A. 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:
Pena - **detenção**, **de 3 (três) meses a 1 (um) ano**, e multa	Pena – **reclusão**, **de 1 (um) a 4 (quatro) anos**, e multa.
§ 2º Aumenta-se a pena de **um sexto a um terço** se da invasão resulta prejuízo	§ 2º Aumenta-se a pena de **1/3 (um terço) a 2/3 (dois terços)** se da invasão

econômico.	resulta prejuízo econômico.
§ 3º [...] Pena - reclusão, de **6 (seis) meses a 2 (dois) anos**, e multa, se a conduta não constitui crime mais grave.	§ 3º [...] Pena – reclusão, de **2 (dois) a 5 (cinco) anos**, e multa.

Em análise às mudanças advindas da Lei 14.155/21, pode-se notar que constava na redação anterior como tipo penal o termo “invadir dispositivo informático alheio” e no atual consta “invadir dispositivo informativo de uso alheio”.

Assim, o tipo penal tornou-se mais abrangente, deixando de exigir que o dispositivo informático seja de propriedade do usuário. O sujeito passivo do delito não precisa ser necessariamente o proprietário do dispositivo, podendo inclusive configurar crime se o proprietário do dispositivo o invadir caso esteja sob o uso de outra pessoa.

São dispositivos informáticos, conforme Gilaberte (2021): “smartphones, computadores, discos rígidos externos, pen drives, aparelhos de GPS, smart TVs, consoles de videogames etc”. Nota-se que não é alcançado pelo conceito, “aplicativos isoladamente considerados, plataformas digitais e afins”.

No entanto, partindo do exemplo hipotético, em que uma pessoa consiga acessar arquivos armazenados na nuvem[15] por outra pessoa, ainda que não invada o dispositivo pertencente ao titular[16] desses arquivos, sistematicamente irá atingir o servidor da empresa que presta o serviço. O que leva a crer que esses *softwares* trabalham com dados que são armazenados em servidores, cujos dispositivos informáticos são de uso alheio (GILABERTE, 2021).

Nesse mesmo entendimento, há julgado da Terceira Turma Criminal do Tribunal de Justiça do Distrito Federal: “[...] I - A expressão "dispositivo informático" não se refere apenas aos equipamentos físicos (hardware), mas também os

[15] Armazenamento em nuvem consiste no ato de armazenar um ou mais arquivos em um HD fora da sua máquina, através da internet, contando com um servidor que fará a comunicação dos dispositivos pessoais com os centros de dados. Os centros de dados são os locais físicos, que a princípio, possuem um alto nível de segurança digital, física e estão espalhados pelo mundo. Dessa forma, quando um usuário acessa um serviço de armazenamento em nuvem através de seus dispositivos, ele está acessando os servidores diponibilizados pelas empresas. (COSTA, Matheus Bigogno. **O que é armazenamento em nuvem e como funciona**. CanalTech, 2020. Disponível em: <https://canaltech.com.br/internet/armazenamento-em-nuvem-o-que-e/>. Acesso em: 17/07/2021).

[16] Nota-se que o autor faz referência ao titular do dispositivo, cabendo esclarecer que a expressão “titular do dispositivo” foi modificada por “usuário do dispositivo”, pela Lei n. 14.155/21, no caput do art. 154-A.

sistemas, dispositivos que funcionam por computação em nuvem, facebook, instagram, e-mail e outros [...].” (TJ-DF 20160110635069 DF 0009088-86.2016.8.07.0016, publicada em 11/02/2020), já citado anteriormente no item 1.1.1 Crimes cibernéticos próprios.

O crime tem como sujeito ativo, qualquer pessoa, excetuando aquela que tenha autorização para acessar os dados constantes do dispositivo. A vítima (sujeito passivo) pode ser qualquer pessoa, física ou jurídica (CAVALCANTE, 2021).

Na redação original, ocorria a conduta com a “violação indevida de mecanismo de segurança”, sendo carcaterizado o delito quando o agente, por exemplo, “burlasse senhas de acesso, criptografia, firewalls ou qualquer outra forma de proteção do conteúdo armazenado no dispositivo” (GILABERTE; MONTEZ, 2021).

A nova redação suprimiu essa exigência, dessa forma, o simples acesso à máquina pela rede, sem violação de qualquer dispositivo de segurança poderá enquadrar na tipificação.

Um exemplo dessa situação, é se certo indivíduo, na hora do almoço, acessasse sem a devida autorização o computador de seu colega de trabalho, que não tem proteção de senha ou qualquer outro mecanismo de segurança, e dessa forma, obtivesse acesso a dados privativos. Nota-se que mesmo sem haver mecanismo de segurança, a privacidade está sendo violada e por tal motivo merece a reprimenda penal (CAVALCANTE, 2021).

Importante esclarecer que o bem jurídico protegido nesse crime é a privacidade, no que refere a intimidade e a vida privada, tutelado pela Constituição Federal de 1988, em seu art. 5º, X.

A nova lei manteve no em seu texto, a finalidade de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita, no entanto, a autorização deve ser do usuário e não mais do titular do dispositivo.

E ainda, houve aumento da pena, alterando de 3 (três) meses a 1(um) ano, e multa para 1 (um) a 4 (quatro) anos, e multa. Deixando dessa forma, de ser um crime de menor potencial ofensivo, sujeito à competência do Juizado Especial Criminal, disposta no art. 61 da Lei nº 9.099/95 (que trata de crimes com pena não superior a dois anos) (BRASIL, 1995), deixando também, de admitir o procedimento apuratório através do Termo Circunstanciado de Ocorrência (TCO). Com a entrada em vigor do novo comando normativo, a autoridade policial deverá instaurar o

Inquérito Policial.

Contudo, ainda é cabível suspensão condicional do processo (art. 89 da Lei nº 9.099/95) e acordo de não persecução penal (art. 28-A do CPP).

E em caso de condenação, mesmo que a pena não seja aplicada em seu limite máximo, terá a possibilidade da conversão da pena privativa de liberdade em restritiva de direitos, tendo em vista que o crime não é praticado com violência ou grave ameaça, conforme disposto no art. 44, I, do Código Penal (BRASIL, 1940).

O crime é considerado comum; doloso (por exigir a intenção do agente); formal (já que é desnecessária a obtenção de qualquer dos resultados almejados pelo sujeito ativo para que se consuma, sendo indiferente estar ou não o dispositivo conectado à rede de computadores) e admite a tentativa (PROCOPIO, 2021).

Houve majoração da pena no parágrafo segundo, logo, a antiga redação que previa o aumento da pena, de um sexto a um terço, se da invasão resultasse prejuízo econômico, com o novo texto, o aumento de pena passou a ser de 1/3 (um terço) a 2/3 (dois terços) se decorrer a mesma situção. Por tratar de alteração mais gravosa, o referido dispositivo se aplicará somente aos crimes que for cometido após o início de sua vigência.

O parágrafo terceiro qualifica a pena, se com a invasão o agente obter “conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido” (BRASIL, 1940).

Nesse sentido, a pena do parágrafo terceiro que era de reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constituísse crime mais grave, passou a ser de reclusão, de 2 (dois) a 5 (cinco) anos, e multa. Também aplicando a delitos ocorridos após o início de sua vigência, por ser mais gravosa.

A ação penal continua sendo, em regra, a pública condicionada. Há excepcionalidade, 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 (art. 154-B do CP).

3.2 Furto mediante fraude cometido por meio de dispositivo eletrônico ou informático

A Lei nº 14.155/2021 incluiu ao crime de furto, previsto no art. 155 do Código

Penal Brasileiro, o §4º-B, criando figura do furto qualificado mediante fraude eletrônica, e §4º-C, com duas causas de aumento de pena relacionadas ao §4º-B, conforme segue:

> § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.
> § 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso:
> I – 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;
> II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável.(BRASIL, 2021)

Para Rogério Sanches (2021), em razão dos prejuízos provocados e da maior dificuldade de apuração revelada nos casos de subtrações fraudulentas, o legislador inseriu no art. 155 do CPB, uma qualificadora específica para as situações em que o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático.

No §4ª-B o legislador trouxe nova figura qualificada, com patamar de quatro a oito anos se a fraude é cometida por meio de dispositivo eletrônico ou informático. Nessa previsão, basta que a fraude seja eletrônica, não sendo necessária violação a mecanismo de segurança, utilização de programa malicioso ou que o mecanismo esteja conectado à internet.

Entende-se por dispositivo eletrônico ou informático, qualquer aparelho com capacidade de armazenar e processar automaticamente informações/programas, como computador, notebook, tablet, smartphone (CUNHA, 2021).

Para Gilaberte (2021): “dispositivo eletrônico é um conceito mais abrangente, contemplando aparelhos e mecanismos que não são necessariamente informáticos, como calculadoras eletrônicas, aparelhos de fax, cartões bancários dotados de chip e outros”.

Cabe ressaltar que a qualificadora do § 4º-B não se confunde com o estelionato, em que o agente induz alguém em erro para que entregue voluntariamente o bem. No caso do § 4º-B o bem é retirado pelo agente sem que a vítima o perceba, através de manobra ardilosa, visando afastar a vigilância da vítima e possibilitar a subtração, mantendo o pressuposto do inc. II do § 4º do CP (CUNHA, 2021).

No §4º-C foram adicionadas majorantes para o furto qualificado mediante

fraude por meio eletrônico, cuja previsão encontra-se no artigo 155, § 4º-B. A causa de aumento de pena poderá variar conforme critério da relevância do resultado gravoso.

A expressão: “considerada a relevância do resultado gravoso”, deixa a cargo de o julgador definir o grau de aumento da pena e se há relevância suficiente para aplicar o referido aumento.

Conforme o inciso I, do §4º-C, a pena será aumentada de 1/3 (um terço) a 2/3 (dois terços) se o crime for praticado por meio de servidor mantido fora do território nacional. Cabe pontuar que se trata “de servidor mantido” fora do Brasil e não de “autor do delito” que esteja fora do Brasil.

O inciso II do §4º-C aumenta a pena de 1/3 (um terço) até o dobro, nos casos em que o crime é praticado contra idoso ou vulnerável.

Nesse sentido, é considerada idosa a pessoa com idade igual ou superior a 60 anos, conforme encontra-se tipificado no art. 1º da Lei nº 10.741/2003, que dispõe sobre o Estatuto do Idoso (BRASIL, 2003).

O inciso II não trouxe um conceito específico de vulnerável, para tanto, o Código Penal, no art. 217-A, caput e § 1º, considera vulneráveis: pessoa menor de 14 anos e a pessoa que, em razão de enfermidade ou deficiência mental, não tem o necessário discernimento para a prática de determinados atos (BRASIL, 1940)

Conforme entendimento de Rogério Sanches Cunha (2021):

> [...] a majoração da pena pressupõe a ciência das circunstâncias referidas no § 4º-C. O autor da subtração deve ter conhecimento de que sua conduta se vale de conexão internacional. Ou deve saber que a vítima é idosa ou vulnerável, o que nem sempre ocorrerá, em razão das circunstâncias dos crimes cibernéticos, nos quais muitas vezes o criminoso não tem nenhum contato – nem mesmo remoto – com sua vítima.

Levando em consideração o argumento de Rogério Sanches, pode-se afirmar que o elemento subjetivo para o aumento da pena é o dolo. Sendo necessário que o agente saiba que está utilizando servidor mantido fora do Brasil, ou que tenha ciência de que a vítima é idosa ou pessoa vulnerável.

Embora a promulgação da Lei 14.155/21 seja recente, já há julgados em nosso ordenamento, quanto à tipificação do art. 155, § 4ª, II. Recentemente foi julgado pelo Superior Tribunal de Justiça, em decisão monocrática, Habeas Corpus (STJ – HC: 566139 RJ 2020/0063479-3, relator Ministro João Otávio de Noronha,

publicada em 28/06/2021), constando o seguinte teor:

> **DENÚNCIA OFERECIDA PELA PRÁTICA DOS DELITOS PREVISTOS NO ART. 2.º, §3º, DA LEI Nº 12.850/2013, C/C ART. 155, §4º, INCS. II e IV, DO CÓDIGO PENAL, C/C ART. 1º, CAPUT e §4º, DA LEI Nº 9.613/1998 (174 VEZES), N/F DO ART. 71 DO CÓDIGO PENAL, TODOS EM CONCURSO MATERIAL (ART. 69 DO CÓDIGO PENAL). DEFESA TÉCNICA QUE ALEGAR QUE A PRISÃO DO ORA PACIENTE ESTRIBOU-SE EM ARGUMENTOS FRÁGEIS, BEM COMO DEIXOU DE ANALISAR DE FORMA EFETIVA A POSSIBILIDADE DE ADEQUAÇÃO DE MEDIDAS CAUTELARES, ALÉM DE SER O MESMO PRIMÁRIO E PORTADOR DE BONS ANTECEDENTES**. Prisão preventiva que foi adequadamente fundamentada, pois extraída dos autos a periculosidade do ora Paciente, evidenciada pela gravidade das condutas praticadas por ele e pela Organização Criminosa, na qual exercia a função de CODER (incumbido pelo desenvolvimento dos programas espiões capazes de captar dados). Fatos que são antigos, mas que até a data de hoje causam prejuízos às vítimas, protraindo-se no tempo. A alegação de ter residência fixa, ocupação lícita e bons antecedentes, por si sós, não conduz obrigatoriamente à revogação da prisão preventiva. Antecedentes do Superior Tribunal de Justiça. O caso concreto é de necessidade da manutenção da prisão do Paciente, ante a presença de indícios de autoria e materialidade. Medida cautelar alternativa que são insuficientes para manutenção da ordem pública, uma vez que os atos podem ser praticados de dentro de casa. Decreto prisional bem fundamentado, em consonância com o art. 93, inc. IX, da CRFB/88, vez que necessário, adequado e proporcional. Presença dos requisitos do art. 312 do Código de Processo Penal, quais sejam: periculum libertatis e fumus comissi delictis. Decreto prisional bem fundamentado, em consonância com o art. 93, inc. IX, da CRFB/88. **PEDIDO DEDUZIDO em habeas corpus que se JULGA IMPROCEDENTE. ORDEM QUE DEVE SER DENEGADA.**

E ainda, salientou as características dos crimes informáticos, revelando a preocupação do legislador dada a importância da promulgação da Lei n. 14.155, fazendo referências ao furto informático e a necessidade do autor do crime não permanecer em liberdade, devido ao *modus operandi*, que possibilita reitação delitiva:

> Importa lembrar que os crimes informáticos têm características únicas, cuja execução e alcance diferem daqueles ocorridos no mundo tangível material, pois, como lembra Spencer Toth Sydow, são "praticados por meio facilitador e com alta capacidade lesiva", em circunstâncias que "encoraja[m] a ação d[o] delinquente" (Crimes informáticos e suas vítimas. 2. ed., versão eletrônica. São Paulo: Saraiva, 2015). A recente promulgação da Lei n. 14.155, de 27/5/2021, revela a preocupação do legislador com o crescente aumento dos crimes informáticos, particularmente no período de pandemia do novo coronavírus, tendo sido inserida nova qualificadora no § 4º-B do art. 155 do CP, [...]. O incremento da cibercriminalidade exige das autoridades judiciárias a adoção de medidas adequadas para coibir a reiteração delituosa, tendo em vista os mecanismos utilizados pelos hackers para a prática de furtos eletrônicos e a provável ineficácia das medidas cautelares diversas da prisão para acautelar o meio social e econômico. De fato, o modus operandi dos crimes cibernéticos torna, por exemplo, insuficiente a

> prisão domiciliar ou a monitoração eletrônica para prevenção do risco de reiteração. Nesse aspecto, como destacado no julgamento do HC n. 34.715/PA, no qual a Quinta Turma denegou a ordem de habeas corpus em favor de acusados de delitos informáticos, "não há como não reconhecer que, uma vez em liberdade, os pacientes não terão absolutamente nenhuma dificuldade em acessar à internet através de qualquer computador e utilizar o programa desenvolvido por eles próprios ou, em último caso, confeccionar outro, pois são eles pessoas de profundo conhecimento técnico, tristemente utilizado a serviço do ilícito, em tese (HC n. 34.715/PA relator Ministro Arnaldo Esteves Lima, Quinta Turma, DJ de 18/10/2004). Em caso análogo, o Ministro Gilmar Mendes, do Supremo Tribunal Federal, denegou a ordem postulada no HC n. 199.823/MA, consignando a legitimidade dos "decretos prisionais consubstanciados no modus operandi do delito e na possibilidade concreta de reiteração delitiva" (HC n. 199.823/MA, DJe de 26/4/2021).

Nota-se com o julgado supramencionado, manifesta preocupação também do judiciário quanto à incidência dos crimes cibernéticos, e nesse caso em especial, o furto mediante fraude cometido por meio de dispositivo eletrônico ou informático, tendo em vista a possibilidade de o agente incorrer em reiteração delitiva, já que pelo modo de operação, o criminoso pode atuar em qualquer local, ainda que esteja, por exemplo, em prisão domiciliar. Daí a importância da pena de reclusão constante no dispositivo.

3.3 Alterações no crime de estelionato

A incidência de crimes de fraudes eletrônicas aumentou consideravelmente desde o início da pandemia de Covid-19, com medidas restritivas de imposição de distanciamento social, em que muitos hábitos e atividades passaram a ser realizadas remotamente, e tendo em vista que as relações sociais influenciam diretamente no surgimento de novos comportamentos criminosos, tornaram-se epidêmicas também as fraudes eletrônicas.

O legislador levando em consideração esse cenário, percebeu a necessidade de criar mecanismos penais de repressão e com a promulgação da Lei 14.155/21, foram acrescentados dois parágrafos ao dispositivo do art.171 do Código Penal Brasileiro, o § 2º-A e o §2º-B, tratando de nova modalidade qualificadora, além de modificar o §4º com nova causa de aumento de pena, aumentando a fração no caso de estelionato majorado contra idoso e incluindo o vulnerável.

3.3.1 Estelionato na modalidade fraude eletrônica - §2º-A

O § 2º-A, encontra-se disposto na Lei 14.155/21 com a seguinte redação:

> § 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.

O dispositivo em comento cria a figura da fraude eletrônica, que se trata de um novo tipo penal, bem como uma nova qualificadora. Contudo, diferente do furto tipicado no art. 155, § 4º-B, CPB, o estelionato nessa situação, não faz menção específica a dispositivo eletrônico ou informático.

A invasão se configura na possibilidade da subtração, sem que a vítima num primeiro momento perceba, sendo mais grave a conduta de quem obtém vantagem utilizando “informações fornecidas pela vítima ou por terceiro induzido em erro, por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo”.

Ainda que a qualificadora do estelionato, não tenha indicado de forma expressa que a fraude seja cometida por meio de dispositivo eletrônico ou informático, pode considerar que seja praticada dessa forma, visto que, as redes sociais, telefone, e-mail ou outro meio análogo são manejados justamente por dispositivos eletrônicos ou informáticos (COSTA; FONTES; HOFFMANN, 2021).

O estelionato na modalidade fraude eletrônica possui em seu escopo possibilidades mais amplas, e conforme Costa, Fontes e Hoffman (2021), também não exige que o engodo seja praticado pela internet, ou ainda que haja violação de mecanismo de segurança, ou utilização de programa malicioso.

Trata-se de delito de duplo resultado, exigido no tipo penal o binômio vantagem indevida e prejuízo alheio, os quais necessariamente são consequência da adoção do meio fraudulento.

Rogério Sanches (2021) descreve que nesses casos de estelionato a conduta é agravada por quem obtém vantagem utilizando informações fornecidas pela vítima ou por terceiro induzido em erro, conforme consta em sua tipificação, dando exemplos em cada situação:

- Redes sociais: através de anúncios promovidos em redes sociais como Fa-

cebook e Instagram. Geralmente são anúncios fraudulentos com manobras ardilosas, fins de atrair pessoas que forneçam seus dados;

- Contatos telefônicos: atavés de envio de mensagem, muito comum pelo aplicativo *WhatsApp*, em que o estelionatário se identifica como amigo ou familiar da vítima e lhe pede depósito bancário devido a uma emergência. Nessa situação, a vítima sem dar-se conta, efetua o depósito na conta do criminoso;
- Envio de correio eletrônico fraudulento: pode ocorrer quando a vítima recebe um e-mail, no entanto, fraudulento, que muitas vezes imita os caracteres de empresas ou organizações conhecidas, disponibilizando link em que a vítima acessa e ao inserir dados de cartão de crédito ou efetuar pagamentos de compras simuladas, proporciona a vantagem ao estelionatário;
- Por qualquer outro meio fraudulento análogo: de forma analógica pode ser inserido quaisquer outras práticas fraudulentas cometidas por meios eletrônicos ou informáticos. Como exemplo, tem-se páginas na internet em que a vítima não é diretamente abordada pelo estelionatário, mas induzida em erro por fatores diversos, tais quais, simulação de um estabelecimento comercial regularmente constituído; cópia de outra página conceituada, entre outras situações.

No estelionato mediante fraude eletrônica, a atuação do agente com o objetivo de obter vantagem indevida, se dá por meio de informações da vítima que ele obteve da própria vítima, ou de um terceiro que foi induzido em erro.

Nesse sentido, a vítima fornece informações que possibilita a prática do crime, integrando diretamente o ardil preparado pelo estelionatário para obter a vantagem indevida (CUNHA, 2021).

Para melhor entendimento, assim exemplifica, Rogério Sanches:

> [...] Pretendendo adquirir um televisor, um indivíduo faz uma pesquisa na *internet* e encontra a página de uma conhecida rede varejista na qual o produto está sendo anunciado por um preço muito abaixo das concorrentes. Insere seus dados pessoais e bancários sem saber que, na verdade, se trata de uma página clonada, que apenas copia os caracteres da famosa rede varejista, para induzir as pessoas em erro. Efetuado o pagamento, o dinheiro é creditado ao autor da fraude, que evidentemente não pretende entregar o produto anunciado. Nesse exemplo, [...], a vítima tem participação direta, pois, induzida por um anúncio enganoso, fornece os dados para que o autor da fraude possa obter a vantagem. Trata-se, portanto, de estelionato.

Por isso não se confunde com o furto mediante fraude digital. No estelionato, o valor sai da conta da vítima, tendo ela consciência. A própria pessoa transfere o valor. O exemplo citado por Rogério Sanches demonstra como a vítima tem ciência que está fazendo o pagamento ou transferência, no entanto ela foi enganada, induzida ao erro pelo estelionatário.

De acordo com o que dispõe o §2º-A, a pena é de 4 (quatro) a 8 (oito) anos, e devido ao caráter qualificador, não admite o benefício de medidas despenalizadoras da Lei nº 9.099/95 (Lei dos Juizados Especiais - LJE), nem suspensão condicional do processo (art. 89 da LJE), possibilitando no entanto, a admissibilidade de acordo de não persecução criminal (artigo 28-A do Código de Processo Penal).

3.3.2 Forma majorada da fraude eletrônica - § 2º-B

A Lei n. 14.155/21, assim prescreveu o § 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”.

Essa qualificadora existe quando o estelionato é cometido por meio de redes sociais, contatos telefônicos, envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo, previstos no § 2º-A.

Consta inserido no dispositivo uma causa de aumento de pena de um a dois terços. Essa fração deve ser usada, em conformidade ao critério da relevância do resultado gravoso, como já previsto pela lei. Observa-se que o legislador repetiu a expressão “relevância do resultado gravoso”, também utilizada como critério de aumento de pena do furto mediante fraude, prescrito no art. 155, § 4º-C, do CP.

A forma majorada incide sobre a forma qualificada do § 2º-A, se o crime for praticado mediante a utilização de servidor mantido fora do Brasil.

Cabe ratificar que advém de servidor mantido fora do território nacional e não necessariamente de autor do delito que esteja fora do território nacional.

Sua gravidade possivelmente fundamenta-se na representação da ameça à soberania nacional e na problemática da repressão do delito, tendo em vista a dificuldade do trabalho de investigação em identificar e responsabilizar penalmente os envolvidos.

3.4 Estelionato mediante fraude eletrônica contra idoso ou vulnerável - § 4º

Mesmo antes da promulgação da Lei n. 14.155/21, já havia previsão do § 4º do art. 171 do Código Penal Brasileiro, porém, no antigo texto a pena era aumentada em dobro se a vítima fosse idosa. Com o novo texto, advindo da Lei 14.155/21, permanece o aumento da pena para vítima idosa, inserindo o vulnerável, considerada a relevância do resultado gravoso.

Para melhor entendimento sobre a mudança na causa de aumento de pena, constante no dispositivo em comento, segue abaixo quadro demonstrativo com o dispositivo antes da Lei 14.155/21 e com a redação atual:

Redação anterior à Lei n. 14.155/21	Redação atual
Estelionato contra idoso § 4º Aplica-se a pena em dobro se o crime for cometido contra idoso.	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.

O critério de escolha para o aumento da pena nesse dispositivo deve ser a relevância do resultado gravoso.

Nesse caso, o legislador trouxe uma *lexis mitior* em relação ao idoso, já que antes a pena era aumentada em dobro e agora de 1/3 (um terço) ao dobro.

No entendimento de Procópio (2021), caso o crime cometido anterior não tenha resultado gravoso de grande importância, a nova lei poderá retroagir, fins de beneficiar o acusado ou condenado.

Nesse sentido, caso alguém seja condenado por estelionato contra idoso, independente se na modalidade fraude eletrônica, ou não, poderá pedir aplicação retroativa do § 4º.

No caso da inserção do vulnerável no dispositivo, por ausência de previsão anterior, a majorante só poder incidir (no caso de vulnerável), para os crimes cometidos após o início de vigência da lei, por constituir *novatio legis in pejus*.

Impende destacar, que em relação ao vulnerável tem-se uma *lex gravior*, já que não existia essa causa de aumento para o vulnerável.

Tal como no caso do furto mediante fraude eletrônica, o legislador não definiu

o que é o vulnerável. Dessa forma, ratifica-se que se trata o que dispõe o Código Penal, em seu art. 217-A, caput e § 1º: “considera vulneráveis pessoa menor de 14 anos e a pessoa que, em razão de enfermidade ou deficiência mental, não tem o necessário discernimento para a prática de determinados atos” (BRASIL, 1940).

3.5 Da Competência pelo domicílio da vítima ou por prevenção no crime de estelionato

A Lei nº 14.155/2021 inseriu o § 4º ao art. 70 do Código de Processo Penal, conforme redação abaixo:

> Art. 70 [...] § 4º Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção.

A partir da promulgação da Lei n. 14.155/21, via de regra, o § 4º do art. 70, do CPP, em casos em que ocorra estelionato mediante depósito ou transferência de valores de forma eletrônica, a competência para processar e julgar será do domicílio da vítima.

Percebe-se com esse dispositivo, uma novidade, já que é a primeira vez que uma lei altera o Código de Processo Penal Brasileiro para determinar a competência pelo domicílio da vítima, ainda que não seja o domicílio da conta da vítima.

Referida alteração pode abarcar diversos motivos. Possivelmente o legislador fez essa mudança por conta dos bancos virtuais, que não possuem agências físicas, sendo as contas simplesmente virtuais, e também pelo fato de algumas pessoas ter o domicílio em um local e a conta em outro local.

Essas alterações já geraram muitas críticas, pois colidem com Súmulas do Supremo Tribunal Federal (STF) e do Superior Tribunal de Justiça (STJ).

De acordo com a Súmua 521 do STF: “O foro competente para o processo e julgamento dos crimes de estelioanto, sob a modalidade de emissão dolosa de cheque sem provisão de fundos, é o do local onde se deu a recusa do pagamento

pelo sacado”[17].

Na Súmula 244 do STJ: “Compete ao foro do local da recusa processar e julgar o crime de estelioanto mediante cheque sem provisão de fundos[18]”.

As duas Súmulas decritas acima, foram superadas pelas alterações do § 4º do art. 70 (GOMES, 2021).

No entanto, a Súmula 48 do STJ: “Compete ao juízo do local da obtenção da vantagem processar e julgar crime de estelionato cometido mediante falsificação de cheque”, não foi superada, continua atuante, sendo aplicada, já que o art. 70, § 4º não faz referência a cheque falsificado (GOMES, 2021)

Conforme a redação do art. 70, em casos que haja várias vítimas do estelionatário, e que seja em comarcas diversas, a competência firmar-se-á pela prevenção (art. 83 do CPP).

Assim dispõe o art. 83 do CPP:

> DA COMPETÊNCIA POR PREVENÇÃO
> Art. 83. Verificar-se-á a competência por prevenção toda vez que, concorrendo dois ou mais juízes igualmente competentes ou com jurisdição cumulativa, um deles tiver antecedido aos outros na prática de algum ato do processo ou de medida a este relativa, ainda que anterior ao oferecimento da denúncia ou da queixa.

Impende salientar, que o disposto no § 4º ao art. 70 do CPP serve para alterar a competência para as ações penais já em curso, quando da entrada em vigor da nova lei.

---

[17] Supremo Truibunal Federal (STF). **Súmula 521 STF**, Sessão Plenária de 03/12/1969. Data de Publicação do enunciado: DJ de 12-12-1969. Disponível em: <http://www.stf.jus.br/portal/jurisprudencia/menuSumarioSumulas.asp?sumula=2725>. Acesso em: 18/07/2021.

[18] LEGJUR. **Súmula 244 STJ.** Disponível em:<https://www.legjur.com/sumula/busca?tri=stj>. Acesso em: 18/07/2021.

CONCLUSÃO

É inegável a otimização da ciência, das relações, da comunicação, do ensino-aprendizagem, dentre outros, com as inovações tecnológicas. Por outro lado, é evidente que criminosos têm deturpado o fim para o qual a internet foi criada.

Diante disso, é imprescindível o acompanhamento do ordenamento jurídico na evolução, com a lei penal tendo implementações, revogações ou modificações sempre que for necessário para proteger a sociedade e o Estado, ainda que para muitos juristas a ação do direito seja devida como intervenção mínima na vida dos cidadãos.

Um ponto positivo da alteração da Lei n.º 14.155/21, foi a modificação da competência para a apuração do crime de estelionato. A apuração passa agora a ser regida pelo local de domicílio da vítima, de modo a aproximá-la da autoridade incumbida pela investigação, bem como favorecer a obtenção de provas do crime, e por fim, o encaminhamento do que foi investigado à justiça.

Ainda há a carência de ferramentas eficientes na investigação dessas práticas delituosas para o alcance de seus criminosos, apesar de já ser prevista, como mostrado neste estudo, a responsabilização do estelionatário virtual, na modalidade fraude eletrônica. O amparo legal foi uma brecha fechada para o crime, porém ainda há muito que ser feito.

É preciso aprimorar e capacitar as instituições investigativas, possibilitando infraestrutura necessária para o trabalho de investigação de crimes cibernéticos.

Com o advento da Lei n. 12.735/12, conhecida por Lei Azeredo, foi determinado que os órgãos da polícia judiciária criassem setores e equipes especializadas no combate a crimes cibernéticos. Desse modo, há no Brasil delegacias especializadas nesse sentido, gerando maior efetividade na individualização da autoria e materialidade do delito. No entanto, se torna imprescindível, que sejam identificados os crimes que realmente fazem parte do rol dos crimes cibernéticos, fins de não sobrecarregar a unidade investigativa. E ainda, é preciso que haja uma melhor estrutura para que a investigação ocorra da melhor forma possível, já que as atuais estão muito aquém do mínimo necessário.

Em Mato Grosso há a Delegacia de Repressão a Crimes Informáticos (DRCI), que atua em combate aos crimes praticados por meio virtual.

Facilitaria o processo investigativo, se as instituições estaduais e federais se

comunicassem, havendo interação entre os sistemas corporativos estaduais e nacionais, em busca de dados constantes em cada instituição.

Da mesma forma, seria imprescindível a interação entre os órgãos de segurança pública, Ministério Público, Poder Judiciário e entidades representativas da sociedade, bem como de organizações internacionais.

E tendo em vista a globalização da internet, em que o crime cibernético não tem fronteiras, possuindo um caráter transnacional, a cooperação internacional para o combate aos crimes cibernéticos é extremamente importante. O processo de negociação para que o Brasil seja signatário da Convenção de Budapeste deve ser finalizado, para que o Brasil possa abrir as portas para uma maior participação da comunidade internacional em matéria penal.

Em outro viés, é de suma importância a participação do Estado na conscientização populacional para a prevenção de crimes como os de estelionato virtual.

Fazem-se necessárias iniciativas públicas de ferramenta social, que possa promover a inclusão digital, e, portanto, também social, assegurada pela Lei 12.965/2014 – Marco Civil da Internet, como dever constitucional do Estado, compreendendo a democratização da tecnologia para todos os cidadãos, prevista no Capítulo IV – DA ATUAÇÃO DO PODER PÚBLICO, artigos 24 a 28.

Cabe a fomentação de políticas de efetivação do acesso inclusivo, sendo necessária a integralização por parte do Estado de instrumentos que promova inclusão social, requerendo integração entre os setores públicos e privados. Cumprindo aos operadores das diversas searas incluídas no processo, o dever de harmonizar o liame entre esses setores, tendo em vista a justiça social e proclamação dos direitos inerentes a todos os cidadãos.

E por fim, também é importante a conscientização dos cidadãos quanto a questões básicas de prevenção, como procurar ter um antivírus, evitar acessar sites suspeitos, links estranhos recebidos ou redes desconhecidas que pedem acesso por senhas de redes sociais, dando preferência aos canais oficiais de comunicação, principalmente os que requisitam dados pessoais e caso seja vítima de algum golpe, procurar imediatamente ajuda das autoridades policiais, visando não apenas a punição, mas a tentativa de reparação ou recuperação do dano.

REFERÊNCIAS

ALBUQUERQUE, Roberto Chacon. **Criminalidade informática**. São Paulo: Juarez de Oliveira, 2006.

ARAS, Vladimir. Crimes de informática: Uma nova criminalidade. **Jus Navigandi**, ISSN 1518-4862, Teresina, ano 6, n. 51, out. 2001. Disponível em: <http://jus.com.br/artigos/2250>. Acesso em: 10 jul. 2021.

AZEVEDO, Bruce William Percílio. **Modelo de referência para o desenvolvimento de aplicações de inteligência de ameaças cibernéticas e sua aplicabilidade para o compartilhamento de dados**. Brasília: UNB, 2020. Disponível em <http://repositorio.unb.br/10482/39792/1/2020_BruceWilliamPercílioAzevedo.pdf>. Acesso em: 2 jul. 2021.

BARRETO, Alessandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. **Cibercrimes e seus reflexos no direito brasileiro**. JusPodivm, Salvador, 2020.

BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética à Luz do Marco Civil da Internet.** Rio de Janeiro: Ed. Brasport, 2016.

BARRETO, Erick Teixeira. Crimes cibernéticos sob a égide da Lei 12.737/2012. **Âmbito Jurídico**, 2017. Disponível em: <https://ambitojuridico.com.br/edicoes/revista-159/crimes-ciberneticos-sob-a-egide-da-lei-12-737-2012/>. Acesso em: 16 jul. 2021.

BELCIC, Ivan. O guia essencial sobre phishing: Como funciona e como se proteger. **Avast**, 2020. Disponível em: <https://www.avast.com/pt-br/c-phishing>. Acesso em: 10 ago. 2021.

BRASIL, **Constituição da República Federativa do Brasil**. Brasília: Senado Federal, 1988. Disponível em: Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 12 jul. 2021.

_____ . Decreto-Lei nº 2.848, de 07 de dezembro de 1940. **Código Penal**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>. Acesso em: 12 jul. 2021.

_____ . Lei nº 10.741/2003 de 1º de outubro de 2003. **Estatuto do Idoso**. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2003/l10.741.htm>. Acesso em 17 jul. 2021.

_____ . **Lei nº 12.965 de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília – DF, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 19 mai. 2021.

_____ . **Lei nº 13.185, de 06 de novembro de 2015**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13185.htm>.
Acesso em 16 jul. 2021.

_____ . **Lei nº 13.718, de 24 de setembro de 2018**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13718.htm>.
Acesso em 16 jul. 2021.

_____ . **Lei nº 13.964, de 24 de dezembro de 2019**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm>.
Acesso em 17 jul. 2021.

_____ . **Lei nº 14.155, de 27 de maio de 2021**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm>.
Acesso em 10 jul. 2021.

_____ . Ministério da Justiça e Segurança Pública. Secretaria em Gestão e Ensino em Segurança Pública. **Curso Crimes Cibernéticos: Noções Básicas.** Brasília - DF, 2020.

_____ . **PL 4554/2020**. Câmara dos Deputados 56ª Legislatura - 3ª Sessão Legislativa Ordinária, Brasília, 2021. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2266148>. Acesso em: 17 jul. 2021.

BOTTINI, Pierpaolo Cruz. Reflexões sobre a AP 470 e a lavagem de dinheiro. **Consultor Jurídico,** 2013. Disponível em: https://www.conjur.com.br/2013-jul-16/direito-defesa-reflexoes-ap-470-lavagem-dinheiro. Acesso em: 15 jul. 2021.

CARNEIRO, Adeneele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. **Revista Âmbito Jurídico**, São Paulo, 2012. Disponível em: <https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/>. Acesso em 12 jul. 2021.

CARVALHO, Marcelo Sávio Revoredo Menezes de. **A Trajetória Da Internet No Brasil: Do surgimento das redes de computadores à instituição dos mecanismos de governança**. Publicado pela UFRJ, 2006. Disponível em <https://www.cos.ufrj.br/uploadfile/1430748034.pdf>. Acesso em: 7 jul. 2021.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. Rio de Janeiro: Brasport, 2014.

CASTRO, Carla Rodrigues Araújo. **Crimes de informática e seus aspectos processuais**. 2ª ed. Rio de Janeiro: Editora Lumen Juris, 2003.

CAVALCANTE, Márcio André Lopes. Lei 14.155/2021: promove alterações nos crimes de violação de dispositivo informático, furto e estelionato. **Dizer o Direito**, 2021. Disponível em: <https://www.dizerodireito.com.br/2021/05/lei-141552021-promove-alteracoes-nos.html>. Acesso em: 16 jul. 2021.

CLASSIFICAÇÃO dos crimes. Direito Penal. **DireitoNet**. Disponível em: <https://www.direitonet.com.br/resumos/exibir/370/Classificacao-dos-crimes>. Acesso em: 18 jul. 2021.

COELHO, Yuri Carneiro. **Curso de Direito Penal Didático**. Vol. único, 2ª ed. – São Paulo: Atlas, 2015.

CORRÊA, Gustavo Testa. **Aspectos jurídicos da Internet**. São Paulo: Saraiva, 2000.

COSTA, Adriano Sousa; FONTES, Eduardo; HOFFMANN, Henrique. Lei 14.155/21 incrementa punição de crimes eletrônicos e informáticos. **Revista Consultor**

Jurídico, 2021. Disponível em: <https://www.conjur.com.br/2021-mai-28/opiniao-lei-1415521-incrementa-punicao-crimes-eletronicos-informaticos>. Acesso em: 17 jul. 2021.

CUNHA, Rogério Sanches. Lei 14.155/21 e os crimes de fraude digital: primeiras impressões e reflexos no CP e no CPP. **Meu Site Jurídico**, 2021. Disponível em: <https://meusitejuridico.editorajuspodivm.com.br/2021/07/09/novo-aumento-de-pena-nos-crimes-contra-honra/>. Acesso em: 17/07/2021.

DA REDAÇÃO. Hacker que praticava golpes digitais é preso em Cuiabá com carros de luxo e ouro; prejuízo é estimado em R$ 2 milhões. **O Documento**. Policial. Disponível em: <https://odocumento.com.br/hacker-que-praticava-golpes-digitais-e-preso-em-cuiaba-com-carros-de-luxo-e-ouro-prejuizo-e-estimado-em-r-2-milhoes/>. Acesso em: 15 jul. 2021.

DICIO. Dicionário Online de Português. **Todas as palavras de A a Z**. Disponível em: <https://www.dicio.com.br/estelionato/>. Acesso em: 18 jul. 2021.

DISTRITO FEDERAL. Tribunal de Justiça. **Apelação criminal nº 20160110635069** - DF (0009088-86.2016.07.0016). Relator: NILSONI DE FREITAS CUSTORDIO, 3ª Turma Criminal, Data de Publicação: DJE 11/02/2020. Disponível em: <https://pje2i.tjdft.jus.br/consultapublica/ConsultaPublica/DetalheProcessoConsultaPublica/listView.seam?ca=9da5e2affb6a3bbfb8bf52711cc803c05fd187ddfe216ebe>. Acesso em: 14 jul. 2021.

DOS SANTOS, Liara Ruff; MARTINS, Luana Bertasso; TYBUCSH, Francielle Benini Agne. Os crimes cibernéticos e o direito a segurança jurídica: uma análise da legislação vigente no cenário brasileiro contemporâneo. **Anais do 4º Congresso Internacional de Direito e Contemporaneidade: mídias e direitos da sociedade em rede.** Edição 2017. Universidade Federal de Santa Maria. Disponível em: <http://www.ufsm.br/cursos/posgraduacao/santa-maria/ppgd/wp-content/uploads/sites/563/2019/09/7-7.pdf>. Acesso em: 08 jul. 2021.

ENGENHARIA social – Definição. **KaspersKy**. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-social-engineering. Acesso em: 16 jul. 2021.

FERREIRA, Ivete Senise. **Os crimes de informática**. In: BARRA, Rubens Prestes, ANDREUCCI, Ricardo Antunes. Estudos jurídicos em homenagem a Manoel Pedro Pimentel. São Paulo: RT, 1992.

_____ . **Direito & Internet: Aspectos Jurídicos Relevantes**. 2 ed. São Paulo: QuartierLatin, 2005.

FOLHA informativa sobre COVID-19. **Organização Pan-Americana da Saúde – OPAS**. Disponível em: <https://www.paho.org/pt/covid19>. Acesso em: 17 jul. 2021.

GARCIA, Rodrigo Antonio Coxe; CARUZO, Willian Ronie; ZAMQUIM JUNIOR, José Wamberto. Crimes cibernéticos. Instituto Matonense Municipal de Ensino Superior. **Revista Matis Online**. Disponível em: <https://immes.edu.br/wp-content/uploads/2020/10/2017-Crimes-Cibern%C3%A9ticos.pdf>. Acesso em: 19 jul. 2021.

GILABERTE, Bruno; MONTEZ, Marcus. A Lei nº 14.155/2021 em análise: invasão de dispositivo informático, furto eletrônico, fraude eletrônica e competência. **JusBrasil**, 2021. Disponível em:< https://profbrunogilaberte.jusbrasil.com.br/artigos/1229253925/a-lei-n-14155-2021-em-analise-invasao-de-dispositivo-informatico-furto-eletronico-fraude-eletronica-e-competencia>. Acesso em: 15 jul. 2021.

GOMES, Adão Mendes. A competência para o julgamento do estelionato após a Lei 14.155/2021. **JusBrasil**, 2021. Disponível em: < https://adaomg.jusbrasil.com.br/artigos/1220722415/a-competencia-para-o-julgamento-do-estelionato-apos-a-lei-14155-2021>. Acesso em: 17 jul. 2021.

GONÇALVES, Victor Eduardo Rios. **Direito penal esquematizado: parte especial do Código Penal**. - 8. ed. – São Paulo: Saraiva Educação, 2018. (Coleção Esquematizada/Coordenador Pedro Lenza).

GOUSSINSKY, Eugenio. Crimes digitais tem forte alta em vários estados; saiba como prevenir. Tecnologia e Ciência. **R7**, 2021. Disponível em: <https://noticias.r7.com/tecnologia-e-ciencia/crimes-digitais-tem-forte-alta-em-varios-estados-saiba-como-prevenir-05052021>. Acesso em: 5 mai. 2021.

GRECO, Rogério. **Resumos Gráficos de Direito Penal, Parte Especial** – vol III. 7ª. ed - Niterói, RJ: Impetus, 2012.

IBGE. Acesso à Internet e à televisão e posse de telefone móvel celular para uso pessoal 2019. **Pesquisa Nacional por Amostra de Domicílios Contínua** – PNAD Contínua, 2021. Disponível em: <https://biblioteca.ibge.gov.br/visualizacao/livros/liv101794_informativo.pdf>. Acesso em: 3 jul. 2021.

INELLAS, Gabriel César Zaccaria de. **Crimes na Internet**. 2º ed., atualizada e ampliada. São Paulo: Editora Juarez de Oliveira, 2009.

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

KUNRATH, Josefa Cristina Tomaz Martins **A expansão da criminalidade no ciberespaço: desafios de uma política criminal de prevenção ao cibercrime**. Dissertação (Mestrado) — Faculdade de Direito, Universidade Federal da Bahia, Salvador, 2014. Disponível em: <http://www.progesp.ufba.br/sites/progesp.ufba.br/files/dissertacao-final-josefa-cristina-tomaz-martins-kunrath-2014.pdf>. Acesso em: 10 jul. 2021.

LACERDA, Anna Carolina Alves Moreira de; SILVA, Amanda Pedroso. Cibercrime: Evolução do crime e a banalização dos crimes virtuais. **II Congresso Internacinal de Direito e Inteligência Artificial – Direito Penal e Cibercrimes**: Skema Business School, Belo Horizonte – MG, 2021. Disponível em: <https://conpedi.org.br/wp-content/uploads/2021/07/Livro-10-Direito-Penal-e-Cibercrimes.pdf>. Acesso em: 14 jul. 2021.

LOPES, Jéssica Rodrigues; COTRIM, Ana Carolina Tomiciolli. Mecanismos de cooperação internacional de repressão e combate dos crimes cibernéticos. **Revista Ideia**. 2014, v.5, n.1. Disponível em: <https://www.revistaidea.oldsiteesamc.york.digital/index.php/idea/article/view/134/105>. Acesso em: 5 jul. 2021.

MAIORIA dos crimes de estelionato em MT é aplicado pelo WhatsApp. **G1 Mato Grosso**. 2020. Disponível em: <https://g1.globo.com/mt/mato-

grosso/noticia/2020/08/24/maioria-dos-crimes-de-estelionato-em-mt-sao-aplicados-pelo-whatsapp.ghtml>. Acesso em: 19 jul. 2021.

MEASURING the Information Society Report. Volume 1, p. 16. Itu: 2018. Disponível em: <https://tinyurl.com/y83bpgld>. Acesso em: 3 jul. 2021.

MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 1ª ed., São Paulo: Saraiva, 2007.

MOLINA, Camila. Polícia prende mulher que aplicou golpes contra vítima idosas em Cuiabá e cidades vizinhas. **Crimes informáticos**. Polícia Civil - MT, 2021. Disponível em: <http://www.mt.gov.br/-/16955397-policia-civil-prende-mulher-que-aplicou-golpes-contra-vitimas-idosas-em-cuiaba-e-cidades-vizinhas>. Acesso em: 14 jul. 2021.

NERY, Claudio Lima; BITTENCOURT, Manoela de; AZAMBUJA, Mariana Menna Barreto. A proteção de dados pessoais e a Internet - The Personal Data Protection And The Internet. **Revista Páginas de Direito**. Porto Alegre, ano 13, nº 1097, 04 de dezembro de 2013. Disponível em: <https://www.paginasdedireito.com.br/index.php/artigos/258-artigos-dez-2013/6364-a-protecao-de-dados-pessoais-e-a-internet-the-personal-data-protection-and-the-internet>. Acesso em: 25 jun. 2021.

NOGUEIRA, Sérgio. PALAVRAS que vêm do latim. **G1, Globo.com**, 2014. Disponível em: <http://g1.globo.com/educacao/blog/dicas-de-portugues/post/palavras-que-vem-do-latim.html>. Acesso em: 16 jul. 2021.

O MEIO é a mensagem. **WIKIPEDIA**. Disponível em: <https:// https://pt.wikipedia.org/wiki/Marshall_McLuhan#cite_note-38>. Acesso em: 1 jul. 2021.

O QUE É CracKing? É hacKing, mas do mal. **Avast Academy**. Disponível em: <https://www.avast.com/pt-br/c-cracking>. Acesso em: 18 jul. 2021.

PAESANI, Liliana Minardi. O papel do direito contra o crime cibernético. In: **Âmbito Juridico**, Rio Grande, XIII, n. 79, ago. 2010. Disponível em: <https://ambitojuridico.com.br/edicoes/revista-79/o-papel-do-direito-contra-o-crime-

cibernetico/>. Acesso em: 18 jul. 2021.

PAINEL TIC COVID-19. **Pesquisa sobre o uso da Internet no Brasil durante a pandemia do Novo Coronavírus, 1ª EDIÇÃO: Atividades na Internet, Culturae Comércio Eletrônico,** 2020. Disponível em: <https://cetic.br/media/docs/publicacoes/2/20200817133735/painel_tic_covid19_1edicao_livro%20eletr%C3%B4nico.pdf>. Acesso em: 16 jul. 2021.

PATURY, Fabricio Rabelo; SALGADO, Fernanda Veloso. **A Política Criminal do Núcleo de Combate aos Crimes Cibernéticos do Ministério Público do Estado da Bahia no enfrentamento aos ilícitos cometidos no âmbito digital.** MPBA, Bahia, 2016. Disponível em: <https://www.mpba.mp.br/system/files_force/biblioteca/criminal/artigos/diversos/a_politica_criminal_do_nucleo_de_combate_aos_crimes_ciberneticos_do_ministerio_publico_do_estado_da_bahia._-_fabricio_rabelo_patury_e_fernanda_veloso_salgado.pdf?download=0>. Acesso em: 12 jul. 2021.

PEREIRA, Jeferson Botelho. Aspectos jurídicos da novíssima Lei nº 14.155, de 27 de maio de 2021. **Revista Jus Navegandi**, 2021. Disponível em: < https://jus.com.br/artigos/90857/aspectos-juridicos-da-novissima-lei-n-14-155-de-27-de-maio-de-2021>. Acesso em: 15 jul. 2021.

PINHEIRO, Patrícia Peck; GROCHOCKI, Luiz Rodrigo. **Noções de Direito Cibernético**. In: VELHO, Jesus Antônio. Tratado de computação forense. Campinas - SP: Millennium, 2016.

PINTO, Anderson de Sousa. Crimes Cibernéticos: Aplicando o Direito Real no Mundo Virtual. **XXVI Congresso Nacional do CONPEDI** (Conselho Nacional de Pesquisa e Pós-Graduação em Direito) - Direito, inovação, propriedade intelectual e concorrência, São Luís – MA, 2017. Disponível em: <http://site.conpedi.org.br/publicacoes/27ixgmd9/96v57uv0/LH3Z2LQHNIN75H7U.pdf>. Acesso em: 10 jul. 2021.

POLIDO, Fabrício Bertini Pasquot. Por que o Brasil deve urgentemente aderir à Convenção de Budapeste. **Revista Consultor Jurídico**, 2021. Disponível em:

<https://www.conjur.com.br/2021-jul-05/polido-brasil-urgentemente-aderir-convencao-budapeste#_ftn2>. Acesso em: 16 jul. 2021.

PROCOPIO, Michael. Lei 14.155/2021: a fraude eletrônica e outras alterações no Código Penal. **Estratégia Concursos**, 2021. Disponível em: <https://www.estrategiaconcursos.com.br/blog/lei-14-155-2021-a-fraude-eletronica-e-outras-alteracoes-no-codigo-penal/>. Acesso em: 16 jul. 2021.

QUEIROZ, Maria Izabel de. As cifras negras e a impunidade. **JusBrasil**, 2015. Disponível em: <https://mariaisabelqueiroz.jusbrasil.com.br/artigos/245894559/as-cifras-negras-e-a-impunidade>. Acesso em: 17 jul. 2021.

REAL Time Net Worth. **FORBES**. Disponível em: <https://www.forbes.com/profile/eric-schmidt/?sh=7c277d17138e>. Acesso em: 7 jul. 2021.

ROCHA, Manuel Lopes. **Crimes da Informática**. Remy Gama Filho. Editora: CopyMarket.com, 2000.

RODRIGUES, Renato. Brasileiros estão entre os mais atacados por golpes durante a pandemia. **Kapersky**, 2020. Disponível em: < https://www.kaspersky.com.br/blog/brasil-phishing-covid-golpe/15902/>. Acesso em: 02 ago. 2021.

ROHR, Altieres. Golpes pela internet têm penas ampliadas para até 8 anos de prisão; entenda a nova lei. Economia, 2021. **G1**. Disponível em: <https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2021/05/28/golpes-pela-internet-tem-penas-ampliadas-para-ate-8-anos-de-prisao-entenda-a-nova-lei.ghtml>. Acesso em: 19 jul. 2021.

ROSA, Fabrízio. **Crimes de Informática**. 2º ed. Campinas: Bookseller, 2005.

ROSA, Joseane. Diferença entre hacker e cracker: Entenda o conceito das palavras. **Educa Mais Brasil**, 2020. Disponível em: <https://www.educamaisbrasil.com.br/educacao/dicas/diferenca-entre-hacker-e-cracker>. Acesso em: 02 ago. 2021.

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

SÃO PAULO. Tribunal de Justiça. **APR: nº 00029534520188260635** SP. Relator: Ruy Alberto Leme Cavalheiro, Data de Julgamento: 21/06/2018, 3ª Câmara de Direito Criminal, Data de Publicação: 05/05/2020. Disponível em: <https://tj-sp.jusbrasil.com.br/jurisprudencia/842621957/apelacao-criminal-apr-29534520188260635-sp-0002953-4520188260635/inteiro-teor-842621977>. Acesso em: 15 jul. 2021.

SEGUNDO, Luiz Carlos Coelho Correa. **CRIMES CIBERNÉTICOS: Análise das leis 12.735 e 12.737 no que tange a sua real necessidade de existência.** Monografia (Curso de Direito) - Faculdade do Estado do Maranhão, São Luís – MA, 2016. Disponível em: <https://www.facem.edu.br/aluno/arquivos/monografias/luis_carlos.pdf>. Acesso em: 14 jul. 2021.

SILVA, Remy Gama. **Crimes da Informática**. CopyMarket.com, 2000.

SIQUEIRA, Ethevaldo. **Para compreender o mundo digital.** São Paulo: Globo, 2008.

SUPERIOR TRIBUNAL DE JUSTIÇA – **HC: 566139 RJ 2020/0063479-3**, Relator: Ministro João Otávio de Noronha, Data de Publicação: DJE 28/06/2021. Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/1238284821/habeas-corpus-hc-566139-rj-2020-0063479-3/decisao-monocratica-1238284837>. Acesso em: 18 jul. 2021.

TEIXEIRA, Hérica. **Golpes por WhatsApp lideram crimes de estelionato em Mato Grosso**. SESP-MT, 2020. Disponível em: Disponível em: <http://www.sesp.mt.gov.br/-/15219266-golpes-por-whatsapp-lideram-crimes-de-estelionato-em-mato-grosso>. Acesso em: 16 jul. 2021

VIANA, Túlio Lima. **Do acesso não autorizado a sistemas computacionais: fundamentos de Direito Penal Informático**. Dissertação. Mestrado em Direito, área de concentração em Ciências Penais. Universidade Federal de Minas Gerais, 2001. Disponível em: <https://repositorio.ufmg.br/bitstream/1843/BUOS-

96MPWG/1/disserta__o_t_lio_lima_vianna.pdf>. Acesso em: 10 jul. 2021.

WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Crimes cibernéticos: Ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport, 2012.

WENDT, Emerson. **Inteligência Cibernética: a (in)segurança virtual no Brasil**. São Paulo: Editora Delfos, 2011.