O ANÔNIMATO NOS CRIMES CIBERNÉTICOS E A OCULTAÇÃO DELITIVA

Edenilson Machado Lima[1]

RESUMO

Por meio da presente pesquisa, buscou-se através de um levantamento teórico conceitual, tratar sobre a crimes cibernéticos no tocante a ocultação delitiva em face do anonimato, notadamente, uma das questões mais difíceis de serem solucionadas no meio jurídico social. Nesse sentido, objetivou descobrir, se levando em conta o crescente número de indivíduos que realizam condutas criminosas ocultas por meio de meios digitais, se é possível identificar quem são esses agentes criminosos e consequentemente aplicar-lhes a pena do crime tipificado no art. 154-A do Código Penal. A Metodologia empreendida na pesquisa foi o dedutivo, pois partiu-se de argumentos gerais para outros mais particulares, objetivando chegar a conclusões mais formais e lógicas, de acordo com as premissas estabelecidas. Infere-se, por fim, que por mais que a legislação penal o prevês como crime, invadir dispositivos móveis, e consequentemente lhe atribuir uma pena a este, verificou-se que o grande problema nos crimes virtuais é a identificação do sujeito ativo, que age sobre as ocultas da internet, o que torna impossível o seu rastreamento.

Palavras-chave: Crimes Cibernéticos; Meios Digitais; internet

1 INTRODUÇÃO

Através da presente pesquisa, buscar-se-á analisar se é possível identificar quem são os agentes criminosos por trás dos ataques cibernéticos. Notadamente, sabe-se que os meios digitais na Atualidade representam grandes avanços sociais, pois, apresenta meios acessíveis a sociedade.

Por outro lado, tornou-se crescente, o número de criminosos digitais que apoderam desse meio para práticas delitivas, cita-se, "ataques cibernéticos". É bem verdade que o Código Penal, por meio do art. 154-A que veio a ser, posteriormente, alterado pela Lei nº 14.155, de 2021, criminalizou a prática de invasão de dispositivos informático de uso alheiro, conectado ou não à rede de computadores com fins ilícitos e estranho, a vontade do usuário.

Destaca-se, que apesar de notória essa previsão, não se afastou efetivamente a prática criminosa, ora citada. Pelo contrário, aumentou-se consideravelmente. E certamente, os crimes

[1] Acadêmico do Curso de Direito do CEULP/ULBRA. E-mail:systemconectpalmas@rede.ulbra.br

virtuais pela extensão dos danos que os provocam, atormentam a sociedade: violando a privacidade, a intimidade, a honra, a dignidade, a operacionalidade, dentre outros. Colocando-os dessa forma, em dúvida, os direitos e garantias fundamentais dos usuários aos meios digitais.

Por oportuno, os crimes virtuais têm desafiado a efetividade das políticas públicas criminais no Brasil. Tendo em vista, a grande dificuldade em identificar quem são os agentes criminosos por trás dos ataques cibernéticos. Nesse sentido, o objetivo central da presente pesquisa é descobrir, se levando em conta o crescente número de indivíduos que realizam condutas criminosas sobre as ocultas dos meios digitais, é possível identificar quem são esses agentes criminosos, e posteriormente aplicar-lhes, a pena cominada do art. 154-A do Código Penal.

Adiante, os objetivos específicos do presente estudo tem por enfoque, a abordagem da evolução histórica dos crimes cibernéticos no Brasil, levando em conta o crescente número de crimes ocorridos; analisar a Lei nº 14.155/2021 e seus reflexos jurídicos nos crimes cibernéticos; e responder ao problema de pesquisa proposto, qual seja, levando em conta o crescente número de indivíduos que realizam condutas criminosas ocultas por meios digitais, se é possível identificar quem são esses agentes criminosos e consequentemente puni-los.

2 A EVOLUÇÃO HISTÓRICA DOS CRIMES CIBERNÉTICOS NO BRASIL

Com o propósito de consolidar a análise inerente aos crimes cibernéticos no Brasil, é preciso traçar um percurso histórico, a fim de se conhecer como se deu ainda a regulamentação desse crime no ordenamento jurídico pátrio, bem como verificar os fenômenos que desencadearam a necessidade de tipificação do aludido crime sob as ocultas do mundo virtual.

Inicialmente, é imperioso destacar o extraordinário alcance da informática nos dias hodiernos, como também a inexplicável e fugaz universalização da internet nessa pujante rede global, sedimentada pelos mais diversos e notáveis segmentos da tecnologia, que evidentemente, abre caminhos para a chamada Revolução 4.0, sob os arrimos da inteligência artificial.

Nesse diapasão, cabe destacar o surgimento da computação avançada, que remonta o ano de 1946 nos Estados Unidos, através do surgimento do primeiro computador totalmente eletrônico, uma enorme máquina de 30 toneladas e milhares de componentes. De um aparato tecnológico marcado por tamanha robustez, os computadores foram se tornando menores e mais eficientes, evoluindo mais ainda com o surgimento dos circuitos integrados em 1970, o que

marcou a entrada dos softwares, permitindo assim que pessoas desprovidas de conhecimentos especializados e populares em informática tivessem acesso a esse mundo novo (PIRES, 2009).

Tanto é verdade que, o surgimento da internet se deu principalmente:

> Durante a guerra fria, devido a uma disputa acirrada entre os Estados Unidos da América e a União Soviética, onde os respectivos países compreendiam a eficácia e a necessidade dos meios de comunicação para garantir vantagens e até mesmo a vitória. (NASCIMENTO, 2016, p.10).

É inconcebível a ideia que uma ferramenta mundialmente utilizada, que inclusive capitaneia o processo de globalização nos dias atuais, remontaria à um contexto eminentemente militar, a princípio com fins de estrita proteção e segurança de informações de interesses das respectivas nações.

Nesse contexto de confrontos ou iminência destes, havia um temor por parte dos Estados Unidos, de que a Rússia poderia desferir um ataque nuclear as suas bases militares, o que indubitavelmente, comprometeria todas as suas informações, e isso os tornaria mais vulneráveis aos seus inimigos. Em face desse receio, a nação norte-americana criou a rede ARPANET pela empresa ARPA, servindo única e exclusivamente como meio de proteção do Governo. (NASCIMENTO, 2016)

Em 1990, a rede ARPANET foi substituída pela rede NSF (Network File System), permitindo o acesso remoto transparente a arquivos no servidor. Entretanto, é em 1993 que a internet ganha uma expansão do seu acesso, através do sistema WWW – Word Wide Web, um sistema de documentos em hipermídia associados e executados na internet, criada pela empresa CERN, uma importante organização europeia para a investigação nuclear (NASCIMENTO, 2016).

Inobstante a todo esse processo evolutivo, é imperioso destacar a importância da internet no meio social, uma vez que esta dirige os vínculos institucionais e sociais, praticamente em todas as áreas, dada a operacionalização das demandas cotidianas – transações bancárias, comerciais, profissionais, entretenimento, interação, etc – que desencadeia um processo contínuo de modificação das relações humanas, de um modo geral.

Outrossim, em que pese os extraordinários benefícios propiciados pela internet, não se pode negar o avanço paralelo de condutas criminosas praticadas no mundo virtual, condutas estas que provocam danos às pessoas, violam direitos e garantias fundamentais, e, muitas vezes, são práticas oriundas da vulnerabilidade de parte da população com as ferramentas tecnológicas.

No Brasil, o surgimento da internet remonta o ano de 1988, através de um acesso realizado pelo Laboratório Nacional de Computação Científica (LNCC) à Bitnet, com uma conexão de 9600 bits por segundo estabelecida com a Universidade de Maryland. Após um processo de aprimoramento de acessos pelas universidades do país, é em 1994 que o governo brasileiro promove um meio de comercialização da internet, a cargo da Embratel e da RNP (MÜLLER, 2018).

Salienta-se ainda que, a criação do Comitê Gestor Internet Brasil, permitiu um avanço maior dessa importante ferramenta, uma vez que objetivava traçar os rumos da implantação, administração e uso da internet no país, fomentando assim o desenvolvimento de serviços da internet no Brasil, recomendando padrões e procedimentos técnicos e operacionais, além de coletar, organizar e disseminar informações sobre esses serviços. (MULLER, 2018).

Segundo informações apontadas pelo Ministério da Ciência e Tecnologia, no ano de 2011, aproximadamente 80% da população brasileira teve acesso à internet, percentual este que corresponde a 60 milhões de computadores em uso, tornando assim o quarto país do mundo com maior número de usuários, ficando atrás apenas da China, Índia e Estados Unidos (BARBOSA, 2020).

Destarte, o surgimento da internet representou uma época de revolução no meio social, e, consequentemente promoveu importantes mudanças nos mais diversos segmentos, levando a humanidade à uma nova realidade, o que resultou na transformação de comportamentos, valores, costumes e hábitos.

Não obstante aos significativos avanços e melhorias propiciados por essa importante rede tecnológica, é notório que essa respectiva rede, tornou-se um campo de atuação criminosa nas mais diversas esferas, com impactos diretos na vida dos seus usuários, como também de forma indireta, quando uma ação criminosa causa danos à um sistema que atende toda uma coletividade.

É imperioso destacar que, os primeiros crimes virtuais ocorreram na década de 1960, com a manipulação de dados contidos em computadores, através de atos como sabotagem, espionagem e abuso ilegal de sistema computacional, todavia, a ausência de melhores condições técnicas obstaculizava a detecção de práticas dessa natureza. Outras ações como pirataria de programas, manipulação de valores nos caixas eletrônicos, abuso de telecomunicações, dentre outros, também ganharam novos contornos em 1980. (NASCIMENTO, 2018).

Cabe ressaltar que, os crimes virtuais surgem em um contexto de crescimento da internet, uma vez que a legislação era muito deficitária na tipificação e repressão de tais condutas, assim como, ineficiente em relação aos sistemas de defesas contra os invasores

cibernéticos. No entanto, foi com a criação da Convenção sobre Criminalidade do Conselho Europeu, que objetivava a sanção de métodos e leis capazes de deter os crimes virtuais, que buscou formular políticas públicas criminais eficazes.

Por sua vez, no Brasil, os crimes cibernéticos ganharam mais notoriedade no final da década de 90, ao ser descoberto uma invasão em vários sites ligados ao governo, e inclusive, ao site oficial do Supremo Tribunal Federal, o que de certa forma, despertou uma maior atenção, principalmente diante da imprevisibilidade de um crime virtual (MEDEIROS, 2015).

As instituições, empresas e a sociedade de um modo geral, vivenciam um pujante processo de modernização, a fim de conferirem maior eficiência e praticidade aos seus serviços, principalmente diante do anseio de uma sociedade cada vez mais imediatista, o que torna necessário a sistematização recorrente das suas demandas cotidianas.

Outro caso de notória repercussão foi o da atriz Carolina Dieckman, em que hackers invadiram suas redes, divulgando diversas imagens íntimas da atriz, motivando assim a criação de uma legislação voltada a proteção de dados, todavia, não é uma tarefa tão fácil assim, pois a identificação dos criminosos se torna cada vez mais difícil, posto que são criadas diversas barreiras virtuais tendentes a dificultar sua localização (FERREIRA; SANTOS, 2019).

Ressalta-se que a atenção legislativa aos crimes cibernéticos não se vincula estritamente ao da atriz, mas à uma conjuntura de acontecimentos que retratam o exponencial aumento dessas condutas, bem como a nocividade representada, diante da repercussão e danos que estes crimes provocam.

2.1 A EVOLUÇÃO LEGISLATIVA DOS CRIMES CIBERNÉTICOS NO BRASIL

O crescimento da internet e a modernização da sociedade, possibilitaram importantes mudanças no mundo globalizado. Todavia, juntamente com essa projeção, os crimes cibernéticos ganharam notoriedade no universo digital, impactando cada vez mais a sociedade, que se tornara tão dependente desse segmento da tecnologia. Para tanto, faz-se necessário uma análise acerca do processo de evolução na tipificação dos chamados crimes cibernéticos.

Os Estados Unidos foram pioneiros na regulamentação dessas condutas, editando em 1984, a legislação "Crime ControlAct", seguido pela Alemanha (1986), França (1988), Espanha (1995), até chegar a Convenção Europeia sobre Crimes Cibernéticos em 2001, que tinha como fito à uniformização da legislação europeia quanto a política criminal desses crimes (NASCIMENTO, 2018)

Por sua vez, no Brasil, a regulamentação se deu em passos mais lentos, a considerar que as primeiras legislações não se atrelavam efetivamente a coibir essas condutas delitivas de maneira mais abrangente. A Lei Pioneira (Lei nº 7.646/87), remete ao ano de 1987, quando se proibiu a propriedade intelectual sobre programas de computador e sua comercialização no país, seguido da Lei n.º 9.883/2000, em que passou a regulamentar a proteção de dados e os sistemas de informação, punindo principalmente os crimes de funcionários públicos que violem o sistema de informação da Administração Pública.

Essa evolução pode ser bem situada em dois momentos cruciais para a relação com este universo digital, quais sejam, a promulgação da Lei nº 12.737/2012 (Lei Carolina Dieckman) que dispõe sobre a tipificação criminal de delitos informáticos, alterando assim o Código Penal, como também a Lei nº 12.695/2014, o chamado Marco Civil da Internet, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. (SILVEIRA *et al*, 2017).

A Lei Carolina Dieckmann, dado a repercussão do caso à época, possibilitou uma revisão na penalização dos crimes virtuais no Brasil, no tocante a invasão e divulgação de conteúdos íntimos. Além disso, a lei também regulamentou os casos de pornografia não consentida, que se dá pela disseminação de fotos íntimas nas redes sociais, através da ação de hackers nos dispositivos móveis informativos. Por sua vez, o Marco Civil da Internet trouxe uma amplitude maior no que se refere a regulamentação da internet, além de fomentar os princípios, garantias, direitos e deveres para o uso da internet no Brasil, além de diretrizes para a atuação nos âmbitos dos Entes Políticos em relação à matéria.

Não menos importante, o objetivo central da lei em debate, é garantir isonomia dos dados apostos aos usuários, o que, evidentemente, há de possibilitar uma mesma velocidade do tráfego na rede, um acesso mais livre ao conteúdo depositados nos dispositivos, conservando uma intensidade equânime para as pessoas que acessem o conteúdo compartilhado na rede.

Todo esse percurso traçado na história digital, que sem dúvidas, é uma tecnologia recente, retrata um contexto tomado por deficiência na coibição das ações criminosas, de maneira que essas legislações socorreram a necessidade das pessoas de terem a sua liberdade de expressão, bem como o direito a privacidade e a proteção dos dados devidamente assegurados.

3 OS CRIMES CIBERNÉTICOS E A INEFICIÊNCIA DAS POLÍTICAS CRIMINAIS

A todo o instante, o ser humano tem algum contato com à rede mundial de computadores, através de variados aparelhos eletrônicos que se conectam à internet, tornando o século XXI marcado pela conectividade multifacetada, seja para acessos e sistemas de interação como Facebook e Instagram, aplicativos de comunicação como Whatsapp, videoconferências, consumo de bens e serviços, operações bancárias, fonte de consulta, enfim, muitos são os vantajosos recursos propiciados por essa ferramenta de trivial importância.

Todavia, em que pese as significativas vantagens que toda essa rede de conexão virtual promove, não se pode negar a nocividade de criminosos, com altíssima capacidade técnica, usando esse espaço para praticarem os mais diversos ilícitos, mesmo que feitos sob a ausência de elementos físicos que ensejem tais condutas, entretanto, com alto potencial danosos e prejudicial a sociedade de um modo geral.

Embora os mecanismos digitais de proteção e segurança de dados estão cada vez mais avançados e as técnicas de operacionalização dos dispositivos conectados à internet mais modernos, é nítido que a atividade dos agentes de crimes virtuais possui uma proporção cada vez maior, indicando assim que ainda há uma série de dificuldades na identificação e punição desses indivíduos.

Nesse sentido, as dificuldades encontradas pelo Ministério Público, Polícia e Judiciário brasileiro para efetivamente punirem os agentes que praticam o cyber crime, dificuldades estas que levam à uma sensação de impunidade, o que leva à uma percepção de que inexistem leis específicas suficientes para aplicar a devida punição. (CRUZ; RODRIGUES, 2018).

Dessa forma, o cerne dessa pesquisa consiste em uma análise concernente as dificuldades para se identificar os sujeitos ativos dos crimes cibernéticos, bem como os métodos utilizados para coibir tais práticas.

3.1 OS ESTUDOS PRELIMINARES SOBRE OS CRIMES CIBERNÉTICOS.

Inicialmente, há uma certa dificuldade de conceituar os crimes cibernéticos, em face da amplitude do meio virtual, de modo que é preciso ter parâmetros bem definidos para se formar um conceito do que seja eminentemente tais crimes.

Uma primeira conceituação dos crimes cibernéticos é um critério macro, pois tais crimes é um ato perigoso em si, pelo receio que qualquer definição de ampla extensão tende a incluir práticas que não podem ser tipificadas legalmente como crimes, por mais indevidas que sejam, bem como pelo receio de que a especificidade exagerada do conceito de crime cibernético possa

engessar ou tornar ineficiente qualquer medida, principalmente pelas constantes transformações tecnológicas (MONTEIRO, 2010).

Per si, os crimes cibernéticos caracterizam-se pela sua periculosidade em relação aos meios digitais, e que viola a privacidade de outrem, e, portanto, é uma atividade criminosa que tem como fim um dispositivo móvel, conectado em rede.

Por outro lado, "os crimes virtuais são fatos típicos e antijurídicos cometidos por meio da ou contra a tecnologia da informação, ou seja, um ato típico e antijurídico, cometido através da informática em geral, ou contra um sistema, dispositivo informático ou rede de computadores". (DAMÁSIO DE JESUS; MILAGRES, 2016, p.20).

Verberadas as ponderações conceituais dos crimes cibernéticos, mostra-se necessária uma análise dos elementos objetivos e subjetivos que adornam os respectivos crimes, levando em consideração que os crimes cibernéticos propriamente ditos, consistem na invasão de dispositivo telemático e ataque de denegação de serviço telemático ou de informação, ou seja, condutas voltadas para dispositivos ou sistemas de informação, e não os crimes comuns praticados pela via computacional.

Por sua vez,a legislação penal, sustenta que:

> A conduta vem representada pelo verbo invadir, que significa devassar, ingressar sem autorização. No crime em tela, o verbo invadir tem a conotação de acessar sem autorização, penetrar nos arquivos ou programas do dispositivo informático alheio. A invasão deve ser executada mediante violação indevida de mecanismo de segurança. Além disso, deve o agente ter a finalidade específica de obter, adulterar ou destruir dados ou informações, ou ainda instalar vulnerabilidades. Neste último caso, deve o agente visar à obtenção de vantagem ilícita. (ANDREUCCI, 2020, p.317)

Dessa forma, quando o computador, enquanto sistema tecnológico é usado como objeto e meio para execução do crime, invadindo dados armazenados na máquina, está diante do crime cibernético próprio, todavia, quando o computador é utilizado como instrumento de condutas ilícitas aptas a atingir um bem jurídico tutelado, como crime de pedofilia, ameaça, calúnia, dentre outros, está diante de um crime cibernético impróprio.

Nesse sentido, os crimes cibernéticos além de terem condutas que só podem ser praticadas estritamente no ambiente virtual, pode comportar delitos que, em tese, exigiriam uma realidade físico para se configurarem, como é o caso do estupro, injúria, calúnia, difamação, estelionato, etc,.

Por oportuno, o bem jurídico tutelado no presente crime é a própria liberdade individual e o direto à intimidade, bens intangíveis fundantes. O Agente Ativo, é qualquer pessoa que

comete a delinquência digital e a contraponto, o Agente Passivo é o proprietário do dispositivo informático invadido, tanto pode ser pessoa física como jurídica, ou outra pessoa estranha que tenha dados ou informações arquivadas no dispositivo.

Esmiuçando ainda, tem-se que o elemento objetivo do crime em comento é o dispositivo informático, que seria todo aparelho capaz de receber dados e ainda,de transmiti-los, precisando necessariamente ser alheio, e caso pertença ao utilizador, mesmo que os dados sejam inseridos por terceiro, o delito em questão não se configura, ressaltando ainda que é necessária a violação indevida de mecanismo de segurança, que seriam meios restritivos a acessos alheios.

E o elemento subjetivo consiste no dolo com o fim especial de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita (GUEIROS; JAPIASSÚ, 2018).

Por tratar-se de crime formal, os crimes cibernéticos independem de resultado naturalístico da conduta, ou seja, o crime se consuma ainda que a obtenção, adulteração ou a destruição dos dados ou informações não se efetive. A tentativa é perfeitamente possível, desde que iniciada a conduta, esta não se conclua por circunstâncias alheias a vontade do agente (CAPEZ, 2018).

A doutrina é acinte, conquanto a forma equiparada do crime cibernético, pois a priori esta consistiria em uma produção, oferecimento, distribuição, venda ou difusão de dispositivo ou programa de computador que atenda ao intuito de permitir a invasão de dispositivo informático alheio, ou seja, referem-se aos programas popularmente chamados de “cavalos de troia”, utilizados tanto para invadir o computador alheio, como também para servir de espião, coletando dados digitados no computador alheio, aptos a resultar na violação de informações sigilosas, como senhas de contas e cartões de crédito (CAPEZ, 2018).

A pena aplicada ao respectivo crime era de detenção, de três meses a um ano, aumentando-se a pena de um sexto a um terço se da invasão resultasse prejuízo econômico, e de um a dois terços caso haja divulgação, comercialização ou transmissão a terceiro a qualquer título, dos dados ou informações obtidos, e por fim, aumenta-se de um terço a metade, caso o crime seja praticado contra Presidente da República, Presidente do Supremo Tribunal Federal, Presidente da Câmara dos Deputados, do Senado Federal, da Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal, ou por fim, dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

No entanto, com a edição da lei 14.155, de 27 de maio de 2021, a pena do crime passou a ser de reclusão, de 1 (um) a 4 (quatro) anos, e multa. Porém, se da invasão ao dispositivo

móvel resultar prejuízo econômico a vítima, a pena é aumentada de 1/3 (um terço) a 2/3 (dois terços).

No que se refere a Ação Penal, consoante o artigo 154-B, esta será pública condicionada a representação, salvo se o crime for cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios, ou contra empresas concessionárias de serviços públicos.

3.2 OS PRINCIPAIS CRIMES CIBERNÉTICOS

Os crimes cibernéticos produzem efeitos que ultrapassam o campo digital, aflorando assim condutas que insurgem contra a honra e a moral das pessoas, suprimindo ainda uma capacidade de proporcionar algum tipo de defesa, dada a suscetibilidade de muitos usuários, que não exprimem aparatos técnicos no manejo da informática.

É preciso ressaltar que, mesmo diante desse contexto de vulnerabilidade, somado ainda a uma falta de conscientização com o uso do aparelho cibernético, os usuários encampam uma certa confiança e partilham informações sigilosas em sites, cujo se desconhece a credibilidade e origem, ingressam em conteúdo de entretenimento, sem qualquer prudência acerca do seu uso, de modo, que as pessoas se interligam plenamente com os meios eletrônicos.

Dada a evolução fugaz das tecnologias, capitaneada por essa nova revolução, a chamada "Revolução 4.0", com a descoberta de mais aparelhos, aplicativos, conteúdos, dentre outros meios de acesso, é difícil se catalogar taxativamente um rol de condutas no campo virtual que ensejem necessariamente em um crime cibernético, com base no conceito já exposto, e ainda na relação desses crimes com o cotidiano real. Portanto, essa pesquisa destaca, sob um aspecto de popularidade, os principais crimes dessa seara virtual.

Considerando que a internet é um espaço que comporta um relacionamento interpessoal e entretenimento, por meio das redes sociais, os crimes contra a honra possuem muita relevância, pois muitas pessoas apropriam dos meios virtuais para difamarem, caluniarem e injuriarem, através de postagens, compartilhamentos de fakenews, vídeos distorcidos, enfim, a internet se tornou um campo de guerra, cujos usuários militam agressivamente por um determinado conjunto de ideias, valores e conceitos pessoais.

Nessa seara, se classifica também os crimes relacionados a pornografia e pedofilia infantil, que nos termos do Estatuto da Criança e do Adolescente, é defeso vender, expor a venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica

envolvendo criança ou adolescente, caso o agente infrator a contrarie, o ECA prevê como pena de reclusão, de 4 (quatro) a 8 (oito) anos de prisão.

Por oportuno, é importante traçar uma distinção entre pedofilia e pornografia infantil, tendo em vista que a pedofilia se trata de uma perversão, cujo adulto força as crianças à uma determinada situação, enquanto na pornografia infantil, não há esse contato entre o agente e a vítima, pois a mera comercialização de materiais fotográficos e visuais de cunho erótico, e que tenha criança e adolescentes, já configura o ilícito. (VENTURA, 2017)

A pedofilia não depende necessariamente de um contato físico entre o agente e o infante ou adolescente, com certas práticas sexuais, pois até mesmo no meio virtual, através de um vídeo chamado ou mesmo uma sala de bate papo, o criminoso seduz as vítimas e as leva a cometer algum ato. Outrossim, o cyberespaço é um campo fértil para a propagação da pornografia infantil, de modo que o consumidor desse tipo de conteúdo, já demonstra uma certa predisposição a pedofilia, dada a sua atração por esse tipo de conteúdo.

Os crimes contra o patrimônio também são praticados no meio virtual, como o estelionato e as fraudes, devido a expansão do comércio virtual, que oferece as mais variadas opções de mercado, facilitando assim o acesso ao consumidor. Todavia, tal benesse oferece um potencial risco de estelionato e fraude, posto que é um meio de atuação dos criminosos, em face da vulnerabilidade do consumidor, o que lhe confere, inclusive, o direito de arrependimento, nos termos da legislação consumerista, e também a escassez de ferramentas que identifiquem tais práticas no momento da transação online.

O estelionato ocorre quando o criminoso invade ou mantém a vítima em erro, com fins à uma vantagem ilícita, através do envio de um link, seja pelo e-mail ou qualquer outro espaço de comunicação, que redirecione a vítima a uma página de compra, inclusive, apta a captar dados bancários, e ainda com ofertas ludibriantes. A fraude por sua vez, se dá pela invasão, modificação ou qualquer outra forma de adulteração em sistema de dados (MEDEIROS; UGALDE, 2020).

A internet como fonte de navegação, acesso à informação e meio de entretenimento, também abriga um submundo, que promove um mercado oculto e ilegal, operado à parte do controle dos gigantes da tecnologia e das autoridades, revelando cristalinamente as facetas criminosas que se concentram nessa rede, denominada de DeepWeb. (PRUDENTE, 2020).

Outrossim, a Deep Web é comumente comparada com um iceberg, cuja superfície representa o conteúdo constante em páginas de fácil detecção pelos mecanismos de rastreamento, ou seja, site de acesso amplo, enquanto a parte submersa que representa efetivamente esse submundo é composto por páginas dinâmicas, não indexadas e com

acessibilidade restrita, com uma dimensão muito maior do que a superfície. (PRUDENTE, 2020)

Se as investigações pelos meios convencionais da internet já encontram diversos obstáculos, quanto mais esse submundo, que tem mecanismos muito mais avançados, em termos de criptografia, mascarando os meios de acesso do usuário, garantindo ampla confidencialidade das informações e sigilo de identidade, o que evidentemente ofusca mais ainda o alcance das investigações, e facilita a expansão do mercado negro.

Ações deflagradas pela Polícia Federal como a Operação Singular, identificou integrantes de uma organização criminosa especializada em crimes bancários, com ampla atuação na Deep Web, incluindo assim estelionatos, furtos, fraudes em concursos públicos, fraudes bancárias, vendas de cartões de crédito clonados e ainda a alteração da nota de candidatos no exame nacional da Ordem dos Advogados do Brasil (OAB), tudo pago através de criptomoedas, certamente com a intenção de ofuscar qualquer possibilidade de rastreamento (PRUDENTE; 2020).

Saliente-se que, nesse submundo cibernético, há uma camada como a Hidden Wiki e o Tor Links, que referem a sites de pesquisas que funcionam como indicação de hiperlinks classificados por assunto, enquanto a outra camada, é composta por conteúdos fechados e grupos específicos, que exigem senhas ou códigos de acesso, permanecendo ocultos por outras camadas. (FRANCO, 2013)

É imperioso destacar que a Deep Web é, indubitavelmente, um espaço muito organizado, com meios de proteção escalonados pelos mais diversos sistemas ocultos, evidenciando uma projeção crescente da criminalidade virtual, abrigando as práticas mais repugnantes, servindo ainda de afluência das organizações criminosas.

Nesse diapasão, os assuntos encontrados na Deep Web classificam-se como sendo:

> Crimes bancários, que abarcam além da lavagem de dinheiro, venda de contas bancárias e de cartões de crédito; crimes de tráfico, como de drogas, de armas e munições; mercado de contrabando, com a venda de eletrônicos de última geração, comércio de remédios e de animais; crimes de falsificação, como de passaporte e outros documentos, de cidadania, de dinheiro de diversas nacionalidades; crimes ligados ao sexo e pornografia, que englobam a zoofilia, parafilia, necrofilia, pedofilia, sadomasoquismo, snuffs de sexo, prostituição, vídeo de estupradores e sexo forçado, mutilação de órgãos genitais e turismo sexual; terrorismo, com snuffs de ataques terroristas e de homem-bomba; tutoriais para a construção de bombas; grupos de extremistas, bioterrorismo e armas nucleares e outros crimes diversos, como teste de vírus potentes; experiências médicas; conspirações diversas que geram violência; lavagem de dinheiro; canibalismo. (FRANCO, 2013, p. 40).

Portanto, nesse submundo virtual, com ampla influência da evolução tecnológica, houve um dimensionamento dos crimes já conhecidos, e ainda abriram espaço para que estes se tornassem mais complexos ainda, sendo um terreno fértil para as organizações criminosas ampliarem suas ofertas nesse mercado oculto, garantido ainda a impunidade desses agentes que se camuflam no anonimato.

Desse modo, não se pode negar a importância da internet nos dias hodiernos, capitaneando esse processo de globalização e revolucionando a vida de pessoas, nas mais diversas áreas. Todavia, é clarividente os riscos que essa importante ferramenta tende a provocar, em face da atuação cada vez mais nefasta de criminosos que se apropriam desse meio para incorrerem nas condutas ilícitas, dada a vulnerabilidade de muitas pessoas, ou mesmo, os obstáculos que dificultam a investigação policial.

3.3 AS DIFICULDADES NA IDENTIFICAÇÃO DA AUTORIA DOS CRIMES CIBERNÉTICOS

Diante do número cada vez mais crescente dos crimes cibernéticos, um dos grandes desafios para os órgãos de repressão consistem na dificuldade de identificação e punição dos autores destes respectivos crimes, considerando que estes não somente agem às ocultas do mundo digital, como também desenvolvem os mais variados e avançados bloqueios que certamente atrasam essa identificação.

Sabe-se que a instauração do inquérito policial depende de indícios suficientes de autoria e materialidade, e, portanto, as investigações que comportem crimes cibernéticos precisam alcançar meios que culminem na identificação do autor do respectivo crime, e é evidente, que isso depende de uma estrutura tecnológica que dê suporte para isso. Portanto:

> O Estado não pode estigmatizar o indivíduo e tampouco alcançar pessoas abstratas com meras inferências. A perfeita identificação do autor e a correta delimitação da infração cometida são essenciais para se punir o criminoso virtual principalmente, quando se considera o ambiente virtual em que o crime foi praticado, caracterizado pela ausência da presença física do infrator. (MALAQUIAS, 2015, p. 119).

Os criminosos se utilizam do anonimato para a prática desses crimes, uma vez que o ambiente virtual possibilita que o agente crie ou mesmo transforme a sua identidade da forma que lhe convém, o que tende naturalmente a desvirtuar o alcance de muitas investigações. Não se pode olvidar que há formas de se encontrar o autor do delito, como por exemplo, através do

número do IP (Internet Protocol), que serve como uma espécie de endereço no mundo cibernético, assemelhando ao Registro Geral de cada cidadão, o que em certa medida possibilita o rastreio do local onde a rede é acessada (SCHIAVON, 2009).

Existem meios de o Estado firmar cooperações com empresas especializadas no ramo cibernético, que certamente tem no seu bojo de mercado, provedores e mecanismos com alto potencial de fazer a identificação desses criminosos, todavia, é necessário não só um altíssimo investimento na aquisição desses mecanismos, como também a exigência de uma melhor capacitação e qualificação do quadro técnico de profissionais.

Diante disso, há uma série de denominações para identificar os autores de condutas ilícitas cibernéticas, quais sejam os hackers e crackers, sendo estes os invasores de computadores e sistemas para a consecução dos fins ilícitos, enquanto aqueles se referem aos que modificam softwares, desenvolvendo novas funcionalidades, encontrando falhas em sistemas para empresas, ajudando a corrigi-las, de modo que usam este conhecimento para a melhoria da segurança. (BORTOT, 2018).

Diante disso, há uma concepção errônea acerca da identificação desses agentes que trafegam pelo espaço virtual. Pois, no senso comum, os hackers seriam agentes que atuam de forma criminosa para a obtenção de fins ilícitos, como por exemplo, a invasão de sistemas, fraudes, vendas de dados bancários, etc, entretanto, essas atividades são típicas dos crackers.

O hackeamento não abriga necessariamente a ilegitimidade ou mesmo terrorismo cibernético, até mesmo porque a própria distinção entre hackers e crackers, encontram guarida nas regras éticas entabuladas pelas comunidades de programadores de software, que consideram hackers como agentes, cujas ações são seladas pelos valores positivos intrínsecos da maestria tecnológica, liberdade, jogo e partilha no mundo digital, enquanto os crackers, se apropriam de truques mal-intencionados dedicados ao vandalismo e roubo tecnológico, usando de toda expertise para tal (RAYMOND, 2003).

Vale destacar que nas distinções supramencionadas, a ênfase recai sobre os crimes cibernéticos inerentes à violação de dados e informações em si, configuradas pela invasão de dispositivos eletrônicos. No entanto, é evidente que há condutas que não se enquadra nesse aspecto técnico, como por exemplo a pornografia infantil, grupos de whatsapp voltados para alguma intenção criminosa, e assim por diante.

Portanto, os crimes cibernéticos possuem uma amplitude muito maior do que se possa imaginar, e não consistem somente na invasão de dispositivos eletrônicos, mas, na utilização dos dispositivos próprios para fins criminosos.

O Brasil é um país ainda muito deficitário no que diz respeito a segurança cibernética, ocupando o 33º lugar em uma lista que contém 219 países, sem contar a quantidade crescente de denúncias, frente à uma completa falta de infraestrutura no âmbito das Polícias Federal e Civil, bem como a carência de profissionais especializados em crimes dessa natureza (LESSA; VIEIRA, 2017).

Esse quadro deficitário revela a necessidade de políticas públicas destinadas aos órgãos de segurança, com capacitação dos profissionais, e um alinhamento dos entes federativos visando o fomento de mecanismos voltados a identificação desses agentes, principalmente a se considerar a existência de quadrilhas especializadas nesses crimes, com uma estrutura bem organizada.

Destarte, há uma interação entre criminosos de estados ou até mesmo países diferentes, que se utilizam de recursos tecnológicos avançados com o uso de criptografia, mecanismos estes que impossibilitam os investigadores determinarem o conteúdo das conversas entre os criminosos. (WENDT; JORGE, 2013).

Por outro lado, a grande dificuldade em relação a esses crimes, não se restringem necessariamente na falta de norma que os classifica, mas sim na falta de tecnologia e mão de obra, somada à recusa de empresas de informação prestarem um auxílio a polícia e ao judiciário, que muitas vezes não prestam as informações devidas, mesmo diante de uma decisão judicial. (CRUZ; RODRIGUES, 2018).

Mesmo que cometidos em um meio cibernético, o procedimento de investigação desses crimes não pode ser alheio aos parâmetros legais, e, portanto, a necessidade de comprovar a materialidade e autoria já se torna um entrave nessa identificação, isso porque a aplicação da sanção penal prescinde da certeza da prática do crime, e contanto, nos termos da legislação processual penal, a inexatidão quanto a prática efetiva do crime, e do seu autor, acarretam a absolvição do réu.

No ato da investigação, primeiramente a polícia precisa identificar o momento em que o crime foi praticado, logo após, a forma e o local do ilícito, seguido pela localização do endereço IP, que após identificado, é preciso um contato com a empresa que disponibiliza o número da rede e assim que se identifica o criminoso. Todavia, o próprio preceito constitucional que tutela a proteção a privacidade e os dados, tornam a obtenção de provas morosa, tendo em vista que é necessário a autorização judicial para a realização dessas investigações (CRUZ; RODRIGUES, 2018).

O próprio sistema de justiça padece de infraestrutura tecnológica que garanta efetividade na marcha do processo, de maneira que essa morosidade frente às práticas de crimes que

ocorrem com total fugacidade, e ainda com a criação de entraves para sua identificação, colocam o sistema investigativo em desvantagem, pois os criminosos continuam operando suas máquinas e se insurgindo nos seus ilícitos.

4 ANÁLISE DA LEI Nº 14.155/2021 E SEUS OS REFLEXOS JURÍDICOS NOS CRIMES VIRTUAIS

A crescente impunidade dos agentes delituosos que atuam as ocultas da internet tem ocasionado uma série de debates no meio social, especialmente no Brasil. Tanto é verdade, que em 27 de maio de 2021, foi sancionada a Lei n.º 14.155, de 27 de maio de 2021 que alterou o Código Penal, para tornar mais graves os crimes de violação de dispositivos informático, furto e estelionato cometidos de forma eletrônica ou pela internet, além de alterar o Código de Processo Penal, definindo a competência em modalidades de estelionato em crimes virtuais.

O Código Penal antes da Lei n.º 14.155/2021, por meio do art.154-A, previa que o agente delituoso que invadisse dispositivo alheio, conectado ou não, de forma estranha a vontade consentida, com fins egoísticos, era penalizada com detenção de 3 (três) meses a 1 (um) ano e multa, porém, a nova lei aumentou a pena de reclusão, para 1 (um) a 4 (quatro) anos, e multa.

Isso porque, a pena tem entre os principais aspectos, a prevenção e com isso, repelir condutas adversas e que não são compatíveis com padrões aceitos por seus pares. Assim sendo:

> Busca-se sustentar que o merecimento de pena criminal, além de seus aspectos preventivos, contém também um juízo de desvalor ético-social, sendo merecedor de pena somente aquela conduta que merece a desaprovação ético-social por sua capacidade para pôr em perigo ou danificar gravemente as relações dentro da comunidade jurídica. (BITTAR, 2015, p. 104)

Entrementes, a pena do Código Penal aplicada aos Crimes Virtuais, mostrava-se inócuo diante a perspectividade do crime. Destaca-se que o Poder Público detém o *jus puniendi* e como tal deve-se formular políticas públicas criminais que de fato, reprima condutas infracionais. E assim, a pena elementar do art. 154-A do CP, mostrava-se enfraquecida, e uma das consequências principais era justamente, a brandeza da pena ao crime em análise. Destaca-se ainda que:

> A nova lei introduziu sensíveis modificações no artigo 155 do Código Penal, para inserir uma nova qualificadora no § 4º-B, determinando que 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. (PEREIRA, 2021, p. 20).

Nesse ínterim e por isso, a nova lei propiciará uma grande inovação na legislação penal pátria, posto que o aumento das penas representa um instrumento de coercibilidade face aos criminosos cibernéticos. E assim, propiciar maior segurança aos meios digitais particulares e público.

Afinal de contas, a internet, "é um novo caminho para a realização de delitos já praticados no mundo real, sendo necessário que as leis sejam adaptadas para os crimes eletrônicos. Essa é a nova missão da Justiça: adaptar os vários dispositivos do Código Penal no combate ao crime digital" (KOURY MAUES *et al*, 2018, p. 177).

Por outro lado, o contexto contemporâneo e a crise pandêmica que assola o mundo, inclusive o Brasil, propiciou um grande aumento do número de usuários conectados as plataformas digitais, seja para as práticas de lazer, ou até mesmo, a alta aderência ao trabalho home office. Tornando-os, vulneráveis aos crimes virtuais.

E ainda, recentemente, o Superior Tribunal de Justiça sofreu um ataque de "cibercrimonoso", com graves consequências para o Tribunal. Esses mesmos criminosos seguiram suas tentativas de ataques a outros órgãos da Administração Pública. No Brasil empresas privadas também são alvos de mega ataques de "hackers" no seu dia a dia, provocando grandes prejuízos materiais e financeiros. (ALVES, 2020).

Outrossim, por mais que hajam leis que abafam parte dessas condutas delituosas, e tenham penas ríspidas capazes de inibir algumas práticas delituosas, é impossível, em grande parte identificar um harcher, pois atuam as sombras da internet, maliciando os principais meios de comunicação social, especialmente e-mail, whatssap, facebooks, e ainda, clonando senhas bancárias por meio de apps que, ora são instalados na loja eletrônica de aplicativos.

Adentrando na ineficácia da lei Carolina Dieckeman:

> Não há hoje nenhuma lei capaz de combater um hacker que usa a Deep Web para invadir computadores no mundo inteiro, não existe uma base legal em que as autoridades competentes possam se apoiar para fazer uma investigação com uma punição, e tentar impedir essa ação de hackers tornando a web ainda mais vulnerável como descreve Cordeiro, 2015: "infelizmente não há regramento jurídico existente para tal ferramenta, concluindo-se que o direito é especifico não alcança este mundo virtual, ao menos agora, quem sabe em futuro mais próximo" (BEZERRA; SILVA, 2020, p. 17).

Não obstante, por mais que seja penoso a identificação dos sujeitos ocultos na web sites, e que invadem os meios digitais, o poder público não se eximirá de politizar e tutelar a honra humana, "valor humano que também veio a ser protegido pela Constituição, por estar muito próxima da dignidade, do respeito e da boa reputação" (BAHIA, 2020, p. 196).

Tanto é, que a privacidade e a intimidade vêm expressamente prevista no texto constitucional, e que são consideradas invioláveis. Em verdade, representam o próprio direito de personalidade, e como tal, qualquer pessoa que tenha esta cláusula de inviolabilidade quebrada, tem o pleno direito de buscar o Poder Judiciário para fazer cessar este gravame.

Desta forma, a Lei n.º 14.155/2021 visa também, tutelar o direito de personalidade que é a própria fundamentação da dignidade da pessoa humana. Isso porque, o Código Penal já no art. 21, infere que, a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a norma em debate.

Portanto, a vida privada enquanto fundamentação dos direitos da personalidade:

> Cuida da vida privada da pessoa, espécie de intimidade que se mostra exteriormente, como, por exemplo, no âmbito do local onde a pessoa atua e no de seu relacionamento familiar ou profissional; também no tocante à sua imagem; resguardando-se o sossego no lar. Por outro lado, a intimidade mostra-se no interior da pessoa, estando afeta aos direitos da personalidade, como a honra, os segredos etc. Ao Poder Judiciário, a pedido do interessado, cabe adotar as medidas necessárias para impedir a violação ou fazer cessá-la. Assim, por medida cautelar ou antecipação de tutela, poderá o interessado realizar esse intento, como, por exemplo, inibir ou reprimir a discriminação sexual. (AZEVEDO, 2019, p. 75)

Consequentemente, o dano causado a intimidade e privacidade da pessoa, se sobrepõe qualquer política criminalizatória; no entanto, silenciar diante das mazelas da criminalidade digital, é omitir um problema de relevante valor social que, é a dignidade da pessoa humana. A contraponto, dos valores sociais intangíveis já colacionados. Por isso, a que homenagear as mudanças introduzidas pela Lei em comento que ocasionará significativas mudanças em relação as políticas criminais no Brasil em relação aos crimes virtuais.

Adiante, a Lei n.º 14.155/2011, inovou o art. 171 do Código Penal, ao penalizar a conduta delituosa utilizada por meio de fraude eletrônica, isso porque é crescente o número de vítimas desta prática. Segundo o §2º-A do aludido dispositivo, 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.

Essa prática é costumeira, no mercado digital de consumo, em que o criminoso se utilizando de meios artificiosos, induz a vítima ao engano por meio de uma promessa falsa, aliás:

> Como uma das consequências dos avanços tecnológicos, sobretudo nos últimos 30 anos, estabeleceu-se um novo parâmetro para a facilidade e velocidade do tráfego de informações. Trata-se de atividade constante e praticamente instantânea, e independe de distância ou de diversidade quanto às realidades onde se encontram inseridas os sujeitos. Porém, proporcional à fluidez, tem-se a dificuldade de controle. (TEIXEIRA; CHAVES, 2019)

Desta forma, os Cibercriminosos muitas das vezes são ardilosos na culminância das infringências penais, não necessitam utilizar de violência ou grave ameaça para os seus feitos ardis. Utilizam da própria fraqueza digital e necessidade humana, afim de obterem os resultados esperados.

Por fim, a lei em estudo, vem para aprimorar a legislação penal consoante aos crimes cibernéticos, prevendo penas mais severas e rígidas, e assim, tentar inibir tais práticas criminosas. Além de garantir um mínimo de segurança possível, visto que um dos maiores problemas de segurança pública, é conter o avanço propagador dos crimes cibernéticos.

CONCLUSÃO

Em virtude dos fatos mencionados, percebe-se que o surgimento da internet e sua evolução ao longo dos anos, representaram um grande avanço social, por outro lado, abriu portas para a criminalidade digital, diante das fragilidades dos sistemas e a exposição do cidadão aos meios digitais.

A contento, os agentes infratores atuam de forma ardilosa e sutil, as ocultas da internet. E infelizmente, apesar de ter no ordenamento jurídico pátrio, dispositivos de lei que dispõe que, tais condutas são consideradas crimes, e, portanto, passíveis de pena preventiva e repressiva. Percebe-se que o grande desafio não reside nos instrumentos normativos, mas sim, nas políticas públicas criminais de inteligência capazes de identificar quem são esses agentes anônimos.

Por outro lado, os crimes virtuais extrapolam, a privacidade e intimidade humana, através da veiculação indevida da imagem da pessoa por meio da pornografia infantil, práticas de racismos e fraudes em contratos eletrônicos, além dos crimes contra a honra, entre outros.

Não obstante, a falta de rigor da pena do tipo penal do art. 154-A do Código Penal Brasileiro antes da Lei 14.155/2021, era considerado um grande atraso em relação a normativa penal voltadas para os crimes virtuais. Isso porque, os crimes cibernéticos têm sido cada vez mais constantes no cenário social atual.

Como exemplo, pode citar o lamentável episódio de ataques cibernéticos no site do Superior Tribunal de Justiça, no dia 03 de novembro de 2020, tornando o sistema indisponível e sem funcionalidade, prejudicando os trabalhos e consultas públicas no portal.

Diante da crescente disparidade dos crimes virtuais, o legislador constituinte, editou no dia 2 de maio de 2021, a Lei n.º 14.155/2021 que alterou o Código Penal, no que tange ao endurecimento das penas aos crimes virtuais, e com isso, possibilitou um grande avanço na legislação penal.

Ademais, é preciso ressaltar que o Sistema Penal, ainda é muito ineficiente em relação a criminalização dos crimes virtuais, pois, a identificação dos agentes anônimos ainda é uma realidade, que o Estado vivencia. Outrossim, é notável a tentativa do Gestor Público e das autoridades em fortificar as normas penais em relação a quem, invade computadores, sistemas de internet alheio, mas é preciso considerar que não é o suficiente para apreendê-los.

Por fim, a formulação de políticas públicas criminais, tem dois obstáculos latente, o primeiro é de como identificar quem são os agentes criminosos que atua por trás de um computador, e devassa sistemas alheios e essenciais. E o outro, de como capturar o desconhecido, já que as autoridades de segurança pública se querem são capazes de identificar os vândalos por trás destes ataques.

REFERÊNCIAS BIBLIOGRÁFICAS

ALVES, Maria Hiomara dos Santos. **A evolução dos crimes cibernéticos e o acompanhamento das leis específicas no brasil**. Disponível em:<https://jus.com.br/artigos/64854/a-evolucao-dos-crimes-ciberneticos-e-o-acompanhamento-das-leis-especificas-no-brasil> Acesso em: 15 de maio de 2021

ALVES, Paulo. **Ataque hacker ao STJ: seis coisas que você precisa saber sobre o caso**. Disponível em:<https://www.techtudo.com.br/listas/2020/11/ataque-hacker-ao-stj-seis-coisas-que-voce-precisa-saber-sobre-o-caso.ghtml> Acesso em: 01 de julho de 2021.

ANDREUCCI, Ricardo Antônio. **Manual de direto penal.** 14ª Ed. São Paulo: Saraiva, 2020.

AZEVEDO, Álvaro Villaça**. Curso de direito civil: teoria geral do direito civil: parte geral.** 2ª Ed. São Paulo: Saraiva, 2019.

BAHIA, Flávia. **Direito constitucional.** 4ª Ed. Salvador: Juspodvim, 2020.

BAUMAN, Zygmunt. **Modernidade líquida.** São Paulo: Zahar, 2001

BEZERRA, Clara Augusta Silva*etal*.**A ineficácia da prestação jurisdicional no combate aos crimes virtuais: a persecução penal.** Disponível em:<https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/1258/1/___TCC%20CLARA%20AUGUSTA%20%281%29.pdf> Acesso em: 12 de maio de 2021

BITENCOURT, Cezar Roberto. **Código penal comentado**. 10ª ed. São Paulo: Saraiva, 2019.

BITTAR, Walter Barbosa. **A punibilidade do direito penal**. ___. Ed. São Paulo: Almedina, 2015.

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

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. **Código Penal**. Diário Oficial da União, Rio de Janeiro, 31 dez. 1940.

BRASIL. **Lei 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em:<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 28 de junho de 2021

BRASIL. **Lei 14.155, de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Disponível em:< http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm> acesso em: 01 de julho de 2021

BRASIL**. Lei 9.610, de 19 de fevereiro de 1998.** Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Diário Oficial da União, Brasília, 20 fev. 1998.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil.** Diário Oficial da União: seção 1, Brasília, DF, ano 139, n. 8, p. 1-74, 11 jan. 2002. PL 634/1975.

BRASIL. **Projeto de Lei n° 4.287, de 2019**. Código Penal disponível em: < https://www25.senado.leg.br/web/atividade/materias/-/materia/137947> Acesso em 16 de maio 2021

BRITTO, Carlos Ayres. **O Humanismo como categoria constitucional**. 2ª Ed. Belo Horizonte: Fórum, 2012.

CAMILLO, Carlos**. Manual de teoria geral do direito. __**São Paulo: Almedina, 2019

CANOTILHO, J.J.G. **Direito constitucional e teoria da constituição**. 7ª Ed. _____: Almeida, 1941.

CARVALHO, GABRIEL CHIOVETTO. **Crimes cibernéticos**. Disponível em:<https://conteudojuridico.com.br/consulta/Artigos/51878/crimes-ciberneticos> Acesso em: 28 de junho de 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.**Disponível em:<https://www.researchgate.net/profile/Marcelo-Carvalho-13/publication/268809917_a_trajetoria_da_internet_no_brasil_do_surgimento_das_redes_de_computadores_a_instituicao_dos_mecanismos_de_governanca/links/54774a430cf2a961e4825bd4/a-trajetoria-da-internet-no-brasil-do-surgimento-das-redes-de-computadores-a-instituicao-dos-mecanismos-de-governanca.pdf>Acesso em 10 de maio de 2021

CORRÊA, Fabiano Simões. **Um estudo qualitativo sobre as representações utilizadas por professores e alunos para significar o uso da internet**. Disponível em:<https://teses.usp.br/teses/disponiveis/59/59137/tde-08102013-162610/publico/Fabiano_Correa_Mestrado.pdf> Acesso em 10 de maio de 2021

CRUZ, Diego; RODRIGUES, Juliana. **Crimes cibernéticos e a falsa sensação de impunidade.**Disponível em:<http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf> Acesso em 22 de abril de 2021

DORIGON, Alessandro. SOARES, Renan Vinicius de Oliveira. **Crimes Cibernéticos: dificuldades investigativas na obtenção de indícios da autora e prova da materialidade.** Disponível em <https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade/3> Acesso em 18 de abril de 2021

FERREIRA, Cláudia Regina Fachin*et al.* **Evolução Dos Crimes Cibernéticos e a Violência Contra Mulher.** Disponível em:<https://ambitojuridico.com.br/cadernos/internet-e-informatica/evolucao-dos-crimes-ciberneticos-e-a-violencia-contra-mulher/>Acesso em: 15 de maio de 2021.

FROTA, Jéssica Olivia Dias. PAIVA, Maria de Fátima Sampaio. **Crimes virtuais e as dificuldades para combate-los.** Disponível em <https://flucianofeijao.com.br/novo/wp-content/uploads/2018/11/ARTIGO_CRIMES_VIRTUAIS_E_AS_DIFICULDADES_PARA_COMBATE_LOS.pdf> Acesso em 05 de maio de 2021

HENRIQUES, A.; MEDEIROS, J. B**. Metodologia Científica na pesquisa jurídica.** 9ªed. São Paulo: Atlas, 2017.

JESUS, Damásio de. **Direito penal 2 – Parte Especial**. 36ª ed. São Paulo: Saraiva,2020.

JHOHNSON, Allain G. **Dicionário de Sociologia: Guia prático da linguagem sociológica**. Rio de Janeiro: Jorge Zahar Ed., 1997.

KOURY MAUES, Gustavo Brandão *et al***. Crimes virtuais: uma análise sobre a adequação da legislação penal brasileira.** disponível em:<https://www.unirios.edu.br/revistarios/media/revistas/2018/18/crimes_virtuais.pdf>Acesso em 11 de maio de 2021.

LESSA, Isabella Maria Beldissera. VIEIRA, Tiago Vidal. **Crimes virtuais: análise do processo investigatório e desafios enfrentados.** Disponível em <https://www.fag.edu.br/upload/contemporaneidade/anais/594c13e45d209.pdf> Acesso em 26 de junho de 2021

LIMA, Maria Vitória Ribas de Oliveira. SILVA, Jefferson David dos Anjos. **Os principais cibercrimes praticados no Brasil.** Disponível em <https://editorarealize.com.br/editora/anais/conedu/2018/TRABALHO_EV117_MD1_SA19_ID7393_13082018131829.pdf> Acesso em 12 de maio de 2021

MADEU, Diógenes *et al*. **Coleção direito vivo: introdução ao estudo e à teoria geral do direito**.__São Paulo: Saraiva, 2015

MARCONI, Maria de Andrade e LAKATOS, E. Maria. **Metodologia Científica**. 7ª ed. São Paulo: Atlas, 2017.

MAZZONI, Cesar Augustus *et al*. **Crimes virtuais: evolução no combate**. Disponível em:<https://jus.com.br/artigos/59468/crimes-virtuais-evolucao-no-combate> Acesso em: 20 de abril de 2021

MEDEIROS, Diego. **Crimes virtuais**. Disponível em:<https://jus.com.br/artigos/42734/crimes-virtuais> Acesso em 14 de maio de 2021

MEDEIROS, Gutembergue Silva; UGALDE, Júlio César Rodrigues. **Crimes cibernéticos: considerações sobre a criminalidade na internet.** Disponível em <https://ambitojuridico.com.br/cadernos/direito-penal/crimes-ciberneticos-consideracoes-sobre-a-criminalidade-na-internet/#_ftn21> Acesso em 29 de abril de 2021

MELLO, Celso Antônio Bandeira de. **O Contéudo Jurídico do Princípio da Igualdade**. 4ª Ed. Salvador: Juspodivm, 2020.

MINISTÉRIO PÚBLICO FEDERAL**. Crimes Cibernéticos – Manual Prático de Investigação**. Disponível em: <https://www.cnmp.mp.br/portal/images/Palestras/Atua%C3%A7%C3%A3o_do_MP_no_combate_aos_crimes_cibern%C3%A9ticosINFANCIA_E_JUVENTUDE.pdf> Acesso em 27 de junho de 2021

MONTEIRO, Renato Leite. **Crimes Eletrônicos: uma análise econômica e constitucional.** Disponível em;<http://www.dominiopublico.gov.br/download/teste/arqs/cp142465.pdf> Acesso em 27 de junho de 2021

MULLER, Nicolas. **O começo da internet no Brasil.** Disponível em:<https://www.oficinadanet.com.br/artigo/904/o_comeco_da_internet_no_brasil> Acesso em: 14 de maio de 2021

NASCIMENTO, Natália Lucas do. **Crimes cibernéticos.** Disponível em:<https://cepein.femanet.com.br/BDigital/arqTccs/1311401614.pdf> Acesso em14 de maio de 2021

NUCCI, Guilherme de Souza. **Manual de direito penal**. 16ª ed. São Paulo: Editora Forense, 2020.

OTOBONI, Gustavo Henrique dos Santos *et al*.**Crimes Cibernéticos: Phishing**. Disponível em: <https://ambitojuridico.com.br/edicoes/revista-191/crimes-ciberneticos-phishing/> Acesso em 28 de junho de 2021.

PEREIRA, Jeferson Botelho. **Aspectos jurídicos da novíssima Lei n 14. 155, de 21 de maio de 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 01 de julho de 2021

PINHEIRO, Patrícia Peck. **Ataques e crimes cibernéticos: conheça os principais tipos**. Disponível em <http://genjuridico.com.br/2020/12/07/ataques-e-crimes-ciberneticos/> Acesso em 10 de maio de 2021

PINHEIRO, Patrícia Peck. **Direito digital.** 6ª Ed. São Paulo: Saraiva, 2016.

PRADO, Luiz Regis. **Curso de Direito Penal Brasileiro.** 19ª ed. São Paulo: Editora Forense, 2019.

PRUDENTE, Amanda Juncal. **O impacto da deep web no tráfico humano: análise a partir da responsabilidade do Estado.** Disponível em <https://uenp.edu.br/pos-direito-teses-dissertacoes-defendidas/direito-dissertacoes/16224-amanda-juncal-prudente/file> Acesso em 15 de maio de 2021

ROCHA, Carolina Borges. **A evolução criminológica do Direito Penal: Aspectos gerais sobre os crimes cibernéticos e a Lei 12. 737/2012.** Disponível em:<https://jus.com.br/artigos/25120/a-evolucao-criminologica-do-direito-penal-aspectos-gerais-sobre-os-crimes-ciberneticos-e-a-lei-12-737-2012> Acesso em: 26 de junho de 2021

RODRIGUES, Claudia de Paula Alves. SANTOS, Luana Miranda. SILVA, Kamila Gomes da. **Crimes Cibernéticos.** Disponível em http://anais.unievangelica.edu.br/index.php/cifaeg/article/view/6174, Acesso em 25 de junho de 2021

SANTOS, Coriolano Aurélio Almeida Camargo. **Atual cenário dos crimes cibernéticos no Brasil.** Disponível em http://pweb01.mp.rj.gov.br/Informativos/2_cao/2010/marco_abril/ATUAL_CENARIO.pdf > Acesso em 27 de junho de 2021.

SCHIAVON, Fabiana. **Crimes eletrônicos deixam rastros que ajudam punição.** Disponível em <https://www.conjur.com.br/2009-jul-25/identificar-autores-crimes-eletronicos-cada-vez-possivel> Acesso em 07 de maio de 2021

SCHMIDT, Guilherme. **Crimes Cibernéticos**. Disponível em:<https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos> Acesso em: 28 de junho de 2021

SILVA, Hugo Hayran Bezerra. C**rimes Cibernéticos: uma análise sobre a eficácia da lei brasileira em face das políticas de segurança pública e política criminal** disponível em:

< http://www.conteudojuridico.com.br/consulta/artigo/55020/crimes-cibernticos-uma-anlise-sobre-a-eficcia-da-lei-brasileira-em-face-das-polticas-de-segurana-pblica-e- poltica-criminal> Acesso em 10 de maio 2021

SILVA, Jesica Luana Pereira da. **Crimes Cibernéticos E Sua Evolução Jurídica – A Internet Não É Terra De Ninguém ?**Disponível em:<https://www.laad.com.br/2020/06/23/crimes-ciberneticos-a-internet-nao-e-terra-de-ninguem/> Acesso em 26 de junho de 2021

SILVEIRA *et al.* **Crimes cibernéticos e invasão de privacidade à luz da lei Carolina Dieckmann.** Disponível em:<https://jus.com.br/artigos/61325/crimes-ciberneticos-e-invasao-de-privacidade-a-luz-da-lei-carolina-dieckmann> Acesso em 10 de maio de 2021

SOUZA, Eric Henrique. **Crimes digitais e evolução da legislação**. Disponível em:<https://ericmsouza.jusbrasil.com.br/artigos/420184154/crimes-digitais-e-evolucao-da-legislacao>Acesso em 26 de junho de 2021

STRECK, Lenio Luiz. **Jurisdição Constitucional**. 6ª Ed. Rio de Janeiro: Forense, 2019.

TAVARES, André Ramos. **Curso de Direito Constitucional**. 18ª Ed. São Paulo: Saraiva Educação, 2020.

TEIXEIRA, Filipe Silva; CHAVES, Fábio Barbosa. **Os crimes de fraude e estelionato cibernéticos e a proteção ao consumidor no e-commerce. Disponível em:<**https://jus.com.br/artigos/73480/os-crimes-de-fraude-e-estelionato-ciberneticos-e-a-protecao-ao-consumidor-no-e-commerce>Acesso em: 01 de julho de 2021

TEIXEIRA, Tarciso. **Direito Digital e Processo Eletrônico**. 5ª Ed. São Paulo: Saraiva Educação, 2020.