ISSN 2179-0167

REVISTA JurES - v.16, n.29, p. 29-61, jun. 2023

CRIMES VIRTUAIS: ANÁLISE DAS DIFICULDADES E LIMITAÇÕES AO COMBATE

VIRTUAL CRIMES: ANALYSIS OF DIFFICULTIES AND LIMITATIONS TO COMBAT

Fabiana Zacarias[1]
Centro Universitário de Ribeirão Preto, Brasil

Lucas Zacharias Freire[2]
Faculdade Reges de Dracena, REGES, Brasil

RESUMO
Esta pesquisa tem por fim realizar uma análise do surgimento do âmbito digital, da constante evolução tecnologica e seus notórios efeitos em nosso meio social, dando assim, ênfase aos crimes praticados no meio virtual. Tendo em vista as mudanças paradigmáticas promovidas pela globalização e dos avanços tecnológicos, a internet tornou-se um ambiente facilitador para a prática da violência. Assim, serão analisados como ocorrem os crimes cibernéticos, quais os perfis dos agentes e como estes se comportam. O presente trabalho também buscará entender quais são as limitações da justiça em termos de identificação de infratores, visando encontrar quais as previsões legais para sanções em âmbito nacional e internacional, verificando, ainda, a constante mutação no contexto digital e a comparação desta mutação tecnologica com o avanço legislativo, numa investigação vinculada à percepção do nível de eficiência da legislação, com a realidade fática. Dessa forma irá analisar a adequação da legislação penal brasileira em vigor e as medidas adotadas pelas autoridades competentes no combate a essa criminalidade, com um intuito final de julgar se há ou não um acompanhamento do fato social pelo direito, a fim de garantir uma maior estabilidade jurídica e, por consequência, social.

Palavras-chave: Direito Penal. Crimes Virtuais. Internet. Responsabilidade penal.

ABSTRACT
This research aims to carry out an analysis of the emergence of the digital environment, the constant technological evolution and its notorious effects on our social environment, thus emphasizing crimes committed in the virtual environment. In view of the paradigm shifts promoted by globalization and technological advances, the internet has become a facilitating environment for the practice of violence. Thus, it will be analyzed how virtual crimes occur, what the agents' profiles and how they behave. This work will also seek to understand the limitations of justice in terms of identifying offenders, aiming to find the legal provisions for sanctions at national and international levels, also verifying the constant change in the digital context and the comparison of this technological change with the legislative advance, in an investigation linked to the perception of the level of efficiency of the legislation, with the factual reality. In this way, it will analyze the adequacy of the Brazilian criminal legislation in force and the measures

[1] Mestre em Direitos Coletivos e Cidadania na "Universidade de Ribeirão Preto" – UNAERP, Ribeirão Preto/SP; Pós-graduada em Direito do Trabalho e Processo do Trabalho pela "Fundação Armando Álvares Penteado" FAAP, Ribeirão Preto/SP, Pós-graduada Direito Penal e Processual Penal pela "Fundação Eurípedes Soares da Rocha" – Marília/SP, graduada pela "Instituição Toledo de Ensino" - ITE de Presidente Prudente/SP. Advogada e professora universitária. E-mail: fazacarias@hotmail.com.
[2] Graduado pela Faculdade REGES de Dracena/SP. E-mail: lucaszfreire@hotmail.com.

adopted by the competent authorities to combat this crime, with the ultimate aim of judging whether or not there is a follow-up of the social fact by law, in order to ensure greater legal stability and, consequently, social.

Keywords: Criminal Law. Virtual Crimes. Internet. Criminal liability.

1 INTRODUÇÃO

O presente estudo foi realizado considerando a realidade da sociedade digital; sociedade em constante e múltiplas faces de evolução; em especial, o avanço da tecnologia representa um dos maiores impactos. Aos poucos, a *internet* deixou de ser apenas um meio de facilitação da vida comum, tornando-se, com o tempo, um meio de necessidade, uma ferrramenta indispensável para a realização de atos cotidianos. Vivemos, portanto, em uma modernidade que é caracterizada pelo volume diário de informações.

A sociedade da informação viabilizou diversas mudanças técnicas e sociais, possibilitando uma comunicação global e instantânea, facilitando a comunicação em diferentes setores. Todavia, toda mudança trás consigo aspectos positivos e negativos, ao passo que o avanço na tecnologia e a acelerada disseminação de informações dificultaram o controle da atividade de usuários no âmbito digital, de forma que o anonimato se tornou uma atrativa possibilidade dentro da internet.

Partindo da premissa de que o Direito acompanha o fato social e que o anonimato influencia no cometimento de atos ilícitos, exsurge a intervenção do Direito, visando, ao mínimo, reduzir a incidência destas práticas, pois, concomitantemente, ascende o problema relacionado à ausência de punição para quem cometeu a conduta considerada típica, ilícita e culpável, gerando por consequência uma instabilidade jurídica. Por isso, é necessário analise da dilação probatória, cuja identificação do agente ativo é complexa devido ao anonimato concedido pela rede.

Compreender como um problema funciona é sempre a primeira etapa para a elaboração de métodos de resolução e/ou aperfeiçõamento na identificação do agente. Desta forma, de maneira resumida, ficou claro que a sociedade está em constante mutação em vários aspectos, sendo um deles, a evolução digital, ao passo que esta,sob um prisma negativo, facilitou a execução de crimes virtuais devido ao

anonimato e a ausência de exposição física frente à conduta criminosa, dificultando assim a sanção institucionalizada para com os criminosos do âmbito cibernético.

Neste particular de colisão de direitos fundamentais foram analisadas questões legais que envolvem o tema, através de uma pesquisa doutrinária e jurisprudencial à luz da Lei n° 12.965/2014 – Lei do Marco Civil da *Internet*. Diante deste cenário é que entendemos a relevância que o estudo do tema possui,à medida que compreenderemos como o Estado busca lidar com esse tipo de delito. Ainda, entre os vários crimes possíveis no ambiente cibernético, pode-se destacar alguns, como por exemplo, os crimes contra a honra nas suas três espécies: calúnia, difamação e injúria, práticas de injúria racial, pornografia infantil, ameaça, estelionato, dentre outros.

Fez-se uma análise sobre a *internet* e o direito, para contextualização, apresentando seus principais aspectos, a análise terminológica e conceito crime virtual, bem como a classificação dos crimes virtuais e o sujeito ativo. Ademais, apresenta uma análise da evolução legislativa, em especial das Leis n.º 12.735 e 12.737 de 2012, conhecidas, respectivamente, como “Lei Azeredo” e “Lei Carolina Dieckmann” e as novas alterações legislativas da legislação penal. Por fim, analisa aspectos importantes sobre os crimes virtuais: a necessidade de prevenção e os desafios enfrentados no processo investigatório.

Diante da relevância social e complexidade do tema, não há possibilidade de esgotar a assunto, no entanto, o objetivo é incitar a discussão e analisar referências que constatem, ou não, melhorias e esclarecimentos sobre o assunto. Para tanto, quanto à metodologia, foi utilizado o método dedutivo como forma de abordagem da pesquisa e o procedimento empregado como técnica foi a revisão de literatura – doutrina, jurisprudência, artigos científicos e legislação – de modo a se ter uma percepção real e conclusão geral sobre o tema.

2 *INTERNET* E O DIREITO: CONTEXTUALIZAÇÃO E ASPECTOS IMPORTANTES

O acesso à *internet,* como Direito Fundamental, decorre dos valores da dignidade humana e da cidadania, assegurados constitucionalmente. “Na atualidade, o papel da *Internet* estende-se para além de um simples meio de comunicação,

porquanto passou a fazer parte da própria vida em sociedade como facilitador e mantenedor de relações humanas.” (PIMENTEL; CARDOSO, 2015, p. 48).

Assim, a ordem jurídica e a normativa constitucional garantem o direito fundamental à informação e liberdade de expressão, hiper dimensionados pelo uso da *internet,* novas tecnologias e desenvolvimento da informática

De acordo com Pinheiro (2010, p. 82) o acesso à informação constitui o maior valor de uma sociedade democrática, e a massificação da *internet* como serviço de informação e informatização, possibilita um aumento de competitividade global de comunidades antes marginalizadas.

No contexto da globalização, a *internet* tornou-se o principal meio de comunicação e informação. Está presente, de cordo com Sorg *et.tal* (2019, p. 9) em quase todas as atividades da vida privada. A quantidade e diversidade de informações que se pode acessar e compartilhar, a facilidade de comunicação, possibilita compartilhar mensagens e postar opiniões, produzindo uma nova forma de organizar a informação e e comunicação.

Nesta nova perspectiva, computadores, smartphones, tablets, GPS, câmeras digitais, e outros dispositivos eletrônicos são utilizados em crimes e ações ilegais. A disseminação das tecnologias e dos recursos eletrônicos “não estão sendo apenas empregados pelas empresas, mas também sendo mais utilizados na prática de diversos crimes, como estelionato, furto mediante fraude e pornografia infanto-juvenil, entre outros.” (CAIADO; CAIADO, 2018, p. 10). No mesmo sentido:

> Praticamente todas as pessoas físicas e jurídicas, de uma forma ou de outra, interagem no ciberespaço, pois a Internet se tornou indispensável em nossas vidas, possibilitando inúmeras facilidades que se estendem de simples contatos sociais até operações bancárias. Porém, justamente por se expandir por praticamente todas as residências, empresas e órgãos públicos, seu livre acesso redunda em problemas ligados à segurança desse sistema, sobretudo quando se trata de operações que envolvam informações que não sejam públicas, tais como dados sigilosos, informações pessoais e bancárias (GIMENES, 2013).

Devido à insegurança jurídíca que é causada no âmbito digital e o receio social em todo o mundo, surgiu a necessidade da atuação legislação e métodos mais rigorosos de fiscalização, visando otimização dos meios de busca do agente. A

internet criou um novo paradigma, não apenas para a melhoria da qualidade de vida, mas atualmente representa um meio facilitador das práticas criminosas.

Caiado (2018, p.10) explica que, com esse novo paradigma, o desenvolvimento da tecnologia melhora o padrão de vida, contudo, ao mesmo tempo, aumenta exponencial e proporcionalmente, a consecução de diferentes práticas criminosas, “entre elas a criação de um dos crimes mais infames da sociedade moderna: a pornografia infanto-juvenil, e facilitando também o acesso a ele e a distribuição de material a este relacionado.” (CAIADO; CAIADO, 2018, p. 10).

Os crimes praticados nos meios digitais tomaram enormes proporções com o advento da sociedade digital e representam um enorme desafio a devida identificação e persecução pena. Assim sendo, é preciso destacar que:

> O acesso às novas tecnologias em um mundo cada vez mais conectado têm garantido diversos avanços nas relações sociais e econômicas. Entretanto, toda essa tecnologia também pode ser utilizada para a prática de crimes. Os crimes cibernéticos são uma realidade, várias espécies de crimes se originaram e outros já conhecidos ganharam uma nova roupagem diante do avanço tecnológico (ARAÚJO, 2018, p. 90).

Assim, surge com o estabelecimento da *internet* novas situações sociais, políticas, econômicas e, consequentemente, novas questões jurídicas. Nas palavras de Reale (2010, p. 2), o direito é “um fato ou fenômeno social; não existe senão na sociedade e não pode ser concebido fora dela. Uma das características da realidade jurídica é, como se vê, a sua socialidade, a sua qualidade de ser social.”

Por conseguinte, o Direito precisa ser adaptado às novas realidades. “Tem-se, então, no Direito Penal a *ultima ratio* para inibição ou punição da realização de um determinado fato ou ato humano não tolerado pela sociedade em certa época.” (SANTOS, 2018, p. 159). Desta feita, com os benefícios da *internet,* novos riscos surgiram. Com a inclusão digital:

> [...] disseminaram-se novas formas de assédio pessoal e abuso de crianças e adolescentes, e a privacidade dos indivíduos fica cada vez mais em xeque. A *Internet* tornou-se palco de cibercrimes, de práticas de censura de conteúdo em massa e de vigilância e espionagem ilegais realizadas por Estados nacionais. Suas ferramentas passaram a ser usadas por grupos que promovem violações de direitos humanos e exploram a fragilidade de serviços e infraestruturas públicos, inclusive ataques cibernéticos a sistemas militares (SORJ *et al;* 2018, p. 9).

No mesmo compasso da evolução tecnológica, abre-se espaço para os crimes virtuais, os quais vêm acarretando diversos prejuízos à sociedade. Como salienta Maues, Duarte e Cardoso (2018, p. 170), a imaterialidade da *internet* propícia a ausência de limites espaciais e temporais; seu amplo e genérico acesso "alavanca riscos oriundos da vulnerabilidade do meio digital, sendo assim, quanto maior a utilização da internet nas interações humanas, mais se potencializa a tendência de surgimento de problemas legais, inclusive, o nascimento de novos tipos de crimes."

Como explica Spinieli (2018, p. 206), foi a partir do grande levante de invasões aos computadores mundiais que trouxe para o Estado a responsabilidade única de vigiar e, ao mesmo tempo, garantir a proteção dos bens jurídicos relevantes para o meio social que se encontrava em risco, além de punir aquele que transgredisse tais valores.

A evolução levou-nos à era cive cibernética, com vantagens e desvantagens "que essa evolução tecnológica pode proporcionar. Tem havido, em todo o mundo, a criação de novos crimes cibernéticos, decorrentes da necessidade de ordenar, disciplinar e limitar o uso indevido da moderna e avançada tecnologia cibernética." (BITENCOURT, 2018, p. 554)

A *internet,* associada à disseminação das tecnologias da informação e comunicação, é um novo caminho para a prática de crimes já previstos na norma penal incriminadora, sendo necessário que a legislação seja adaptada aos crimes cometidos por meio virtual.

2.1 ANÁLISE TERMINOLÓGICA E CONCEITO DE CRIME VIRTUAL

É preciso destacar as diferentes teminologias adotadas doutrinariamente. "Os crimes realizados no meio virtual são denominados de crimes virtuais, digitais, informáticos, telemáticos, de alta tecnologia, crimes por computador, fraude informática, delitos cibernéticos, crimes transnacionais, dentre outras nomenclaturas." (MAUES; DUARTE; CARDOSO, 2018, p. 170).

Apesar de não existir e na doutrina e jurisprudência, uniformidade quanto à terminologia, Spiniel (2018, p. 201) explica que "o Brasil conta, nos dias de hoje, com

o Instituto Brasileiro de Direito Eletrônico (IBDE), cuja posição é no sentido de que a melhor nomenclatura seria “crime eletrônico”.” No mesmo sentido é o entendimento de Rossini (2002), segundo o qual a melhor denominação é aquela que leva o termo “informático” em sua composição. Gimenez (2013) destaca que a Organização para a Cooperação Econômica e Desenvolvimento da ONU utiliza o termo “crime de informática” para “qualquer conduta ilegal não ética, ou não autorizada, que envolva processamento de dados e/ou transmissão de dados”.

Tendo em vista os diferentes termos utilizados, este trabalho manteve a terminologia utilizada no projeto anteriormente apresentado, isto é, crimes virtuais, que são crimes que se caracterizam pela ausência física do agente ativo; por isso, ficaram usualmente definidos como sendo crimes virtuais. (TERCEIRO, 2002) Antes de conceituar o crime virtual, é importante algumas considerações a respeito do conceito de crime em si. O Código Penal não trouxe um conceito próprio de crime, apenas diferenciou crime de contravenção penal, não forneceu características ou detalhes que pudessem explicar e conceituar de fato. Diante disso, passou a ser papel da doutrina defini-lo (GRECO, 2015, p.193).

Assim, parte-se da premissa do crime sob os aspectos da materialidade, formalidade e pelo aspecto analítico. Nesse modo, o crime sob o prisma material:

> A concepção da sociedade sobre o que pode e deve ser proibido, mediante a aplicação de sanção penal. É, pois, a conduta que ofende um bem juridicamente tutelado, merecedora de pena. Esse conceito é aberto e informa o legislador sobre as condutas que merecem ser transformadas em tipos penais incriminadores (NUCCI, 2017, p.123).

Todavia, por esse aspecto, entende-se que crime é toda conduta humana que fere um bem jurídico fundamental. Por outro lado, pelo conceito formal de crime, Fernando Capez (2011, p.134) diz que: “o conceito de crime resulta da mera subsunção da conduta ao tipo legal e, portanto, considera-se infração penal tudo aquilo que o legislador descrever como tal, pouco importando seu conteúdo”.

Por fim, o prisma analítico, segundo Rogério Cunha (2015, p.148), “leva em consideração os elementos estruturais que compõe infração penal, prevalecendo fato típico, ilícito e culpável”. A partir do conceito analítico de crime, pode-se considerar que crimes virutuais são “delitos praticados contra ou por intermédio de

computadores", (WENDT; JORGE, 2012, p.18).

Rossini (2004, p.110) traz um conceito mais completo para crime virtual:

> [...] 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.

De um modo geral, pela doutrina majoritária, o crime virtual é, portanto, toda conduta típica, antijurídica e culpável realizada por meio de computadores, ou seja, toda atividade na qual um computador ou uma rede de computadores são utilizados como uma ferramenta para a prática delituosa.

2.1.1 Classificação dos crimes virtuais

Várias são as classificações doutrinárias sobre os crimes virtuais. Duas categorias são utilizadas: a dos crimes digitais próprios (ou puros) e a dos crimes digitais impróprios (ou mistos/impuros). Assim, é importante destacar a diferença entre crimes digitais próprios e impróprios:

> Crimes digitais próprios ou puros (condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os sistemas informáticos e os dados. São também chamados de delitos de risco informático. São exemplos de crimes digitais próprios o acesso não autorizado (*hacking*), a disseminação de vírus e o embaraçamento ao funcionamento de sistemas; e Crimes digitais impróprios ou mistos (condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os bens jurídicos que não sejam tecnológicos já tradicionais e protegidos pela legislação, como a vida, a liberdade, o patrimônio, etc). São exemplos de crimes digitais impróprios os contra a honra praticados na Internet, as condutas que envolvam trocas ou armazenamento de imagens com conteúdo de pornografia infantil, o estelionato e até mesmo o homicídio (CRESPO, 2015).

De acordo com Crespo (2015), pode-se afirmar que os crimes digitais são tanto os crimes tradicionais, já previstos em lei, praticados com auxílio da mais moderna tecnologia, bem como as condutas ilícitas passíveis de penas que se voltem contra os sistemas informatizados e os dados.

Os crimes virtuais próprios são aqueles em que a tecnologia propriamente dita (seja por intermédio de computadores, celulares ou afins) servirá com meio e fim para a prática delituosa desejada pelo criminoso e que irá danificar e/ou atingir *softwares* e *hardwares*.

Têm-se como exemplos de crimes virtuais próprios, as condutas de invadir *e-mails,* redes sociais, *sites,* instalar arquivos ardilosos (como “Cavalo de Tróia”) entre outros. Barreto e Brasil (2016, p.17) conceituam crime virtual próprio como aqueles em que o dispositivo informatizado e/ou seu conteúdo é o alvo dos criminosos - os sistemas informatizados, bancos de dados, arquivos ou terminais (computadores, *smartphones, tablets*) são atacados por criminosos, normalmente após a identificação de vulnerabilidades, seja por meio de programas maliciosos ou por engenharia social (golpista engana a vítima, fazendo com que forneça informações pessoais e/ou estratégicas).

Por outro lado, os crimes virtuais impróprios (impuros) são aqueles praticados através do uso do computador, sendo este, o instrumento para a prática delituosa violandobens jurídicos já tutelados.

Conforme exemplifica Caiado e Caiado (2018, p. 17):

> estelionato e furto eletrônicos (fraudes bancárias), invasão de dispositivo informático e furto de dados, falsificação e supressão de dados, armazenamento; produção; troca; publicação de vídeos e imagens contendo pornografia infanto juvenil (arts. 241 e 241-A, do ECA - Lei nº 8.069/1990), assédio e aliciamento de crianças (art. 241-D, do ECA - Lei nº 8.069/1990, ameaça, *cyberbullying* (veiculação de ofensas em blogs e comunidades virtuais), incitação e apologia de crime, prática ou incitação de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional, venda ilegal de medicamentos.

Para Albuquerque (2006, p.168), os crimes virtuais impuros “diriam respeito aos crimes em que os recursos informáticos constituem o meio de execução, tendo como objeto bens jurídicos que já são protegidos por tipos penais existentes”. Na sociedade da informação, a incidência de ilícitos penais “têm por objeto material ou meio de execução o objeto tecnológico informático: *hardware*, *software*, redes, etc.

Outra classificação agrupa os crimes em três grupos: o crime virtual puro, o crime virtual misto e o crime virtual comum. Segundo Fiorillo (2013, p. 140-145):

> a. O crime virtual puro corresponderia à conduta ilícita voltada para o sistema do computador, para a violação do equipamento e de seus componentes, inclusive dados e sistemas (software, hardware e meios de armazenamentos);
> b. Os crimes virtuais mistos aqueles em que o uso de meios computacionais é condição necessária para a efetivação da conduta, embora o bem jurídico visado seja diverso do informático (transferência ilícita de valores ou “salemislacing” – retiradas diárias de pequenas quantias de milhares de contas bancárias);

> c. Os crimes virtuais comuns corresponderiam àqueles em que a internet é utilizada como instrumento de realização do delito que já tipificado na lei penal (como os crimes contra a honra e a veiculação de pornografia infantil)

De acordo com esta classificação, conforme exemplifica Santos (2018, p. 168), a primeira abrange as formas tradicionais da criminalidade, tais como a fraude ou a falsificação, a segunda se refere à publicação de conteúdos ilícitos em meios de comunicação eletrônicos (pornografia infantil ou incitamento ao racismo) e a terceira, os crimes perpetrados exclusivamente nas redes eletrônicas (ataques contra sistemas de informação, bloqueio de serviços e pirataria).]

Independente da classificação doutrinária, quando o computador é utilizado como um meio para a prática do crime, esse será caracterizado independentemente de existir uma lei que pune especificamente aquela conduta cometida em meio virtual, seja com a finalidade de consumar atos que atinjam bens jurídicos ligados à informática propriamente dita ou a outras categorias protegidas pelo Direito.

2.1.2 Sujeitos dos crimes virtuais

Como em quaisquer outros tipos de crimes, entende-se como sujeito ativo aquele que pratica a conduta criminosa, enquanto o sujeito passivo é aquele que sofreu com a violação do bem jurídico.

Nucci (2017, p. 131) explica que o sujeito ativo (autor ou agente) é “a pessoa que pratica a conduta descrita pelo tipo penal”. Ou seja, é quem realiza a ação ou omissão típica, nos delitos dolosos ou culposos. Apenas pode ser sujeito ativo a pessoa humana, e não animais ou coisas. O sujeito passivo do delito, conforme Nucci (2017, p. 134), é o titular do bem jurídico protegido pelo tipo penal incriminador, lesado ou ameaçado de lesão. Podem figurar como sujeitos passivos – vítimas, ofendidos -, a pessoa física ou o indivíduo, mesmo incapaz, o conjunto de indivíduos, a pessoa jurídica, a coletividade, o Estado ou a comunidade internacional, de acordo com a natureza do delito.

Nos crimes virtuais, no polo ativo, portanto, é muito comum associarem os *hackers* à figura dos criminosos da *internet,* porém, *hacker* é apenas uma expressão dada, dentre muitas outras, para caracterizar uma pessoa que possui muito conhecimento no meio informático e que invade sistemas, só que não

necessariamente visa o ilícito.

De acordo com Assunção (2017, p. 33), o termo *hacker*, desde as décadas de 1970 e 1980, serve para designar “fuçadores”. Com o passar do tempo, foi utilizado pela mídia para nomear invasores de sistemas, até hoje esse termo é utilizado de forma peculiar: designa um garoto de doze anos que aciona o computador da escola para mudar sua nota ou um fraudador que engana pessoas, enviando-lhes *e-mail* para para capturar senhas de acesso.

Por isso, há várias outras designações para diferenciar os autores dos crimes praticados, como por exemplo, a figura dos *crackers*, que são aqueles que necessariamente utilizam do seu conhecimento para o mal, obtendo vantagens ilícitas, através de danificação de sistemas, furto de senhas, dados, documentos, entre outros. De forma genérica, é a “denominação para alguém que possui uma grande habilidade em computação. *Cracker*, *black-hat* ou *script kiddie*, neste ambiente, denomina aqueles *hackers* que têm como *hobby* atacar computadores. Portanto, a palavra *hacker* é gênero, e *cracker*, espécie.” (GIMENES, 2013)

Moisés Cassanti (2014, p. 2) traz uma distinção entre os conceitos de *hacker* e *cracker.* Embora ambos seja termos que se referem a experts em computadores, a principal diferença está na forma como cada um utiliza esse conhecimento:

> Apesar do termo *hacker* sempre aparecer associado a roubo de dados e invasão de sistemas, no entendimento de especialistas em computação, os verdadeiros criminosos são designados como *crackers.* A palavra deriva do verbo em inglês “to crack”, que significa quebrar. Entre as ações, estão a prática de quebra de sistemas de segurança, códigos de criptografia e senhas de acesso a redes, de forma ilegal e com a intenção de invadir e sabotar para fins criminosos. O termo *hacker,* por sua vez, serve para designar um programador com amplo conhecimento sobre sistemas, mas sem a intenção de causar danos. Inclusive, a habilidade para lidar com sistemas e programações, muitas vezes, é utilizada pela própria polícia em investigações ou até mesmo no desenvolvimento de *softwares* com o intuito de limar brechas de segurança, criar novas funcionalidades ou adaptar as antigas.

Desta forma, a “questão da segurança no ciberespaço não é de interesse apenas das pessoas físicas ou das empresas, sendo altamente relevante para órgãos públicos, para agentes políticos e para o próprio Estado.” (GIMENES, 2013). Qualquer pessoa pode ser sujeito passivo, até mesmo empresas e instituições, e, devido às técnicas dos cibercriminosos acabam tendo suas informações e bens

violados.

3 EVOLUÇÃO LEGISLATIVA: LEIS N.º 12.735 E 12.737 DE 2012, CONHECIDAS, RESPECTIVAMENTE, COMO “LEI AZEREDO” E “LEI CAROLINA DIECKMANN”

No Brasil, o cenário em relação aos crimes digitais próprios foi modificado em 2012 com a edição das leis nº 12.735 e 12.737, conhecidas, respectivamente, como “Lei Azeredo” e “Lei Carolina Dieckmann”, em referência ao relator do projeto de lei, o deputado federal Eduardo Azeredo e à atriz, no caso paradigmático em que teve fotos com conteúdo de nudez divulgadas pela *internet.*

Desde então, “os crimes digitais, cada vez mais comuns no nosso cotidiano, passaram a contar com mais algumas normas que tipificam condutas antes irrelevantes para o Direito Penal.” (CRESPO, 2015)

Conforme ensina Maues, Duarte e Cardoso (2018, p. 172-173) a lei 12.735/2012 estabelece a obrigatoriedade de interrupção imediata de mensagens com conteúdo racista, além de retirá-las de qualquer meio de comunicação e a criação das delegacias virtuais. O intuito da lei foi alterar o Código Penal, o Código Penal Militar e a lei contra o racismo (Lei n.º 7.716/89) visando à tipificação de “condutas realizadas mediante o uso de sistema eletrônico digital ou similares, que sejam praticadas contra sistemas informatizados e similares”.

O artigo 4.º da lei estipula “Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado”, ou seja, a criação de setores de combate ao crime virtual nas delegacias comuns e delegacias especializadas em crimes eletrônicos. O artigo 5.º da referida lei acrescentou no artigo 20 da lei 7.716/89 (Lei de Combate ao Racismo) o inciso II do § 3.º estipulando que: “a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio” de mensagens racistas.

A Lei 12.737/2012, conhecida como “Lei Carolina Dieckmann” em alusão à atriz, dispõe sobre a tipificação criminal de delitos informáticos. Incluiu, pois, o novo tipo penal “invasão de dispositivo informático” (art. 154-A e 154-B do CPB), e alterou os arts. 266 e 298 do CPB, tipificando penalmente a conduta de quem “interrompe

serviço telemático ou de informação de utilidade pública, ou impede ou dificulta- -lhe o restabelecimento" e equiparando a documento particular o cartão de crédito ou débito, tipificando penalmente o crime de falsificação de cartão, respectivamente. (SANTOS, 2018, p. 172)

O art. 154-A do Código Penal descreve nos seus parágrafos algumas hipóteses qualificadoras e causas de aumento de pena. Acrescente-se que uma das alterações promovidas pela Lei 14.155 de 2021 ocorreu no crime de invasão de dispositivo informático, previsto no art. 154-A do Código Penal, criado originariamente pela Lei Carolina Dieckmann. "Desta feita, o legislador modificou o tipo incriminador e, também, previu maior sancionamento para o comportamento." (FIGUEIREDO, 2021) Quanto às questões processuais, é importante consignar que:

> [...] o artigo 154-B do Código Penal trouxe a definição da ação penal cabível, pois a ação penal é pública condicionada à representação. Trata-se de direito disponível, dependendo de provocação do ofendido. Em razão da disponibilidade do bem jurídico tutelado, o consentimento do ofendido exclui o direito de punir do Estado. No entanto, a ação penal será pública incondicionada se o crime for cometido contra dispositivos da administração pública (MAUES; DUARTE; CARDOSO, 2018, p. 1750).

De acordo com Spinielli (2018, 207), o objeto jurídico penalmente tutelado no art. 154-A é a liberdade individual no que é pertinente com a inviolabilidade dos sigilos. A conduta invasora recai sobre o dispositivo informático alheio, que figura como objeto material, esteja conectado ou não à *internet*.

O núcleo típico é o verbo "invadir", que significa, em apertada conceituação, ocupar determinado lugar à força. Qualquer pessoa pode titularizar o polo ativo do crime, bem como pode ser qualquer um a vítima, desde que tenha um dispositivo informático, que pode ser celulares, câmeras, CDs, DVDs e computadores. Entre as hipóteses de aumento de pena, o Brasil contemplou o seu primeiro tipo penal específico contra as problemáticas criminais do ambiente virtual.

3.1 A IMPORTÂNCIA DO MARCO CIVIL DA *INTERNET*

Nos últimos anos, o ordenamento jurídico brasileiro passou por algumas mudanças em função da jurisprudência relacionada ao julgamento de crimes

cibernéticos, especialmente com a aprovação do Marco Civil da *Internet* (MCI), sancionado em 23 de abril de 2014, pela Lei nº 12.965/2014. Esta lei trouxe diversos dispositivos que influenciam a investigação dos crimes virtuais.

O Marco Civil da Internet (MCI) (Lei nº 12.965/2014) estabeleceu princípios, garantias, direitos e deveres para o uso da internet no Brasil. (SANTOS, 2018, p. 172). Com o advento do Marco Civil da *Internet* a responsabilidade quanto à retirada de conteúdo encontrado através de sites de provedores de busca somente configura-se quando não tomadas as providências para a retirada do conteúdo ante ordem judicial e a não identificação do autor da postagem.

Além disso, a Lei 12.965/2014 elencou garantias, princípios, direitos e deveres para a utilização da *internet*, envolvendo provedores de conexão, de aplicação e usuários e regulou o uso da rede em território nacional. Aborda assuntos como direitos e garantias dos usuários, neutralidade de rede, proteção aos registros, atuação do Poder Público na melhoria do uso da *internet* e a responsabilidade dos provedores.

Nesta perspectiva, o decreto nº 8.772/2016 regulamentou o marco civil da *internet* tratando, entre outras coisas, “da guarda e proteção de dados por provedores de conexão e de aplicação, além de apontar medidas de transparência na requisição de dados cadastrais pela administração pública e parâmetros para a apuração e fiscalização de infrações.” (MAUES; DUARTE; CARDOSO, 2018, p. 175-176).

O Marco Civil da *Internet* teve como objetivo estabelecer princípios, garantias, direitos e deveres para o uso da *Internet,* cujo acesso é considerado um direito do cidadão:

> [...] teve por objetivo estabelecer princípios, garantias, direitos e deveres para o uso da Internet, cujo acesso é considerado um direito do cidadão. Sua criação teve importância ímpar na regulação das relações digitais, especialmente no que tange a: inclusão digital (art. 27); exigência de neutralidade da rede (art. 9º), evitando, assim, a discriminação da informação; proteção à intimidade e ao sigilo dos dados (art. 7º, I, II, III), inclusive com a exigência de consentimento expresso do usuário para a coleta, o uso, o armazenamento e o tratamento de dados pessoais (art. 7º, IX); e garantia da liberdade de expressão, como fundamento do uso da Internet no Brasil (art. 2º). O detalhamento de garantias consumeristas aplicáveis às relações no ambiente digital também é um ponto positivo da norma (vide art. 7º, IV a VIII e XI a XIII). (COSTA, 2016)

Segundo Costa (2016), uma das críticas mais severas ao Marco Civil da *Internet*, refere-se à necessidade de notificação judicial específica para responsabilização dos provedores por danos decorrentes de conteúdo gerado por terceiros (art. 19), o que estimularia a judicialização, na contramão da tendência conciliatória. Além disso, a necessidade de autorização judicial para a retirada dos conteúdos danosos foi criticada em virtude da velocidade de "disseminação" dos conteúdos postados na rede, pois aguardar uma ordem judicial pode maximizar o dano, ou torná-lo irreparável.

Para a apuração criminal o Marco Civil da *Internet* traz efeitos para a investigação criminal. O art. 13 estabelece que o provedor de conexão (o responsável pelo serviço de acesso do usuário à *internet*) deverá manter a guarda dos registros de conexão (dados como o IP, com data, horário e fuso horário da conexão de acesso), sob sigilo, em ambiente controlado e de segurança, pelo prazo de um ano.

De acordo com Machado (2014), em uma eventual investigação criminal, cruzando-se os registros de acesso a aplicações de internet, armazenados pelo provedor de aplicativos de *internet*, com os registros de conexão, guardados pelo provedor de acesso, é possível a localização geográfica do ponto de acesso à rede mundial de computadores, a partir do qual se acessou o aplicativo de *internet* para o cometimento de crimes.

3.2 NOVAS ALTERAÇÕES LEGISLATIVAS: LEI n.º 14.155/21 INCREMENTA PUNIÇÃO DE CRIMES ELETRÔNICOS E INFORMÁTICOS

O cenário de pandemia causada pela Covid-19, a prática dos crimes digitais vêm crescendo de forma assustadora. Em razão do distanciamento e isolamento social grande parte dos serviços passaram a ser à distância, através do *home office*, como uma forma de não contaminação do novo vírus.

Neste contexto, aumentou o uso da *internet* e, como consequência, o número de golpes virtuais. De acordo com Cadoso (2020), a criminalidade cibernética existe há tempos, no entanto, o avanço e a facilidade da utilização da *internet* e dos recursos tecnológicos compõe um ambiente atrativo para exploração de crimes. O cenário de isolamento social decorrente da crise pandêmica do Covid-19

transformou, inevitavelmente,

> a rotina de milhões de pessoas, que estas passaram a ter que se adaptar às pressas com a nova realidade e realizar suas tarefas de suas casas por meio do ambiente virtual que passou então a ser questão de sobrevivência, entretanto local este cheio de armadilhas principalmente para os menos inexperientes." (CARDOSO, 2020).

Segundo dados da Febraban (Federação Brasileira de Bancos), no período de isolamento social, bancos registraram aumento de 80% nas tentativas de ataques de *phishing*, alta de 70% na fraude do falso funcionário e crescimento de 65% no golpe do *motoboy.* De acordo com a Federação, durante a quarentena:

> [...] houve alta de 60% em tentativas de golpes financeiros contra idosos, o que resultou em uma campanha de alerta com o apoio da Secretaria Nacional de Promoção e Defesa dos Direitos da Pessoa Idosa, vinculada ao Ministério da Mulher, da Família e dos Direitos Humanos, e do Banco Central. A FEBRABAN e seus bancos investem constantemente em campanhas e ações de conscientização em seus canais de comunicação com os clientes para orientar a população a se prevenir de fraudes. [...] Atualmente, 70% das fraudes estão vinculadas à engenharia social, que consiste na manipulação psicológica do usuário para que ele lhe forneça informações confidenciais, como senhas e números de cartões para os criminosos (FEBRABAN, 2021).

Ainda, um relatório recente elaborado pela Unit 42 (2020), foram detectados, milhares (de fato mais de 100.000) domínios registrados contendo termos como "covid", "vírus" e "corona". Foram identificados 116.357 domínios recém-registrados com nomes relacionados à corona vírus entre 1º de janeiro e 31 de março. Desses, 2.022 são classificados como "maliciosos" e mais de 40.000 são considerados de "alto risco". Além disso, de 1º de fevereiro a 31 de março, testemunhamos um crescimento de 569% nos registros de domínios maliciosos.

Os criminosos estão provendo ataques com as seguintes táticas:

> *Webshops* falsos: sites fraudulentos que ofereciam itens de alta demanda, como máscaras faciais ou desinfetantes para as mãos, por um preço com desconto.
> Armadilha de cartão de crédito: scripts em outras lojas maliciosas que vendem produtos relevantes para pandemia para roubar informações de cartão de crédito.
> *E-books* falsos: domínios criados para explorar o medo do consumidor e forçá-los a comprar ebooks sobre COVID-19 reproduzindo um vídeo sobre as situações e eventos mais assustadores relacionados à pandemia.
> Farmácias ilícitas: sites não licenciados e que utilizam sites comprometidos que usam nomes de domínio, sugerindo a venda de remédios para o COVID-19, quando na verdade anunciam Viagra e outros medicamentos não relacionados ao vírus. (UNIT 42, 2020)

Destaca-se aqui, no que tange ao combate à criminalidade dos crimes virtuais, a publicação da Lei n.º 14.155, de 27 de maio de 2021, que 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.* Na justificação ao Projeto de Lei (BRASIL, 2021), consta que os criminosos, em função da branda legislação brasileira, estão escolhendo o Brasil como terreno fértil para seguirem impunes pela prática de fraudes e crimes praticados de forma eletrônica:

> Esse tipo de crime tem atingido, 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 Coronavírus 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 (BRASIL, 2021).

De forma resumida e conclusiva, Figueiredo (2021) elenca as principais alterações legislativas introduzidas pela Lei n.º 14.155/2021. Para o autor, a lei promoveu importantes alterações no tratamento de crimes cometidos no contexto da *internet,* ao modificar o art. 154-A do Código Penal, retirando do tipo penal a exigência de prática do crime mediante violação indevida de mecanismo de segurança, o que configura mudança prejudicial ao réu e, por isso, não pode retroagir; como a pena do crime previsto no art. 154-A passou a ser pena incrementada, passando a ser crime de médio potencial ofensivo, não retroage por ser prejudicial ao réu.

Da mesma forma, a lei estabelece um aumento de pena concernente à existência de prejuízo econômico e cria uma modalidade qualificada de furto, o furto qualificado pelo emprego de fraude eletrônica (art. 155, § 4º-B). Foram criadas majorantes específicas para o furto qualificado pelo emprego de fraude eletrônica, as quais exigem, para incidência, a avaliação da gravidade do resultado (art. 155, § 4º-C, incisos I e II).

Figueiredo destaca que foi criada uma modalidade qualificada de estelionato, o estelionato mediante fraude eletrônica (art. 171, § 2.º-A); I), bem como foram criadas majorantes específicas para o estelionato eletrônico, as quais exigem para incidência, análise da gravidade do resultado (art. 171, §§ 2º-B e 4º).

Neste ponto, é preciso transcrever o que ensina Costa, Fontes e Hoffmann (2021) sobre a diferença entre o furto mediante fraude e o estelionato. No furto, a fraude é utilizada para burlar a vigilância da vítima, possibilitando ao agente a subtração, enquanto, no estelionato, a fraude é usada como meio de obter o consentimento da vítima, que entrega voluntariamente o que o agente deseja. Quanto ao direito intertemporal da lei penal no tempo, aos autores destacam que:

> A Lei 14.155/21, na parte penal em que estabelece novas qualificadoras e majorantes, inclusive aumentando penas, consiste em *novatio legis in pejus*, e por isso não retroage a fatos anteriores (art. 5º, XL da CF e art. 2º do CP). À exceção da majorante do estelionato contra vítima idosa (art. 171, §4º do CP), em que o patamar de aumento deixou de ser unicamente o dobro, passando a ser entre 1/3 e o dobro, podendo assim retroagir para beneficiar. Ademais, aplica-se a súmula 711 do STF se o delito de invasão de dispositivo informático for praticado como crime permanente (ex: invasão de *notebook* que se prolonga ininterruptamente no tempo por vários dias, para que o *hacker* continue obtendo dados e prejudicando a vítima) ou como crime continuado (COSTA; FONTES; HOFFMANN, 2021).

A nova lei criou, ainda, uma nova regra de competência (art. 70, § 4º do Código de Processo Penal) segundo a qual a competência territorial, no peculato eletrônico, é definida pelo domicílio da vítima. Quanto à fixação da competência, o Figueiredo (2021) propõe que a mesma regra seja adotada no caso de furto eletrônico, por analogia, mas que isso não se estenda a outros crimes cometidos pela *internet*, em nome do princípio da segurança jurídica, para que os processos não sejam obliterados em intermináveis discussões acerca da competência (fincando-se a necessidade de o legislador regulamentar a matéria).

Com relação à aplicação da lei processual penal no tempo, o referido autor entende necessária a aplicação do art. 2.º do Código de Processo Penal, em conjunto com art. 43 do Código de Processo Civil, a fim de que a modificação da competência territorial não afete casos nos quais já apresentada a inicial acusatória. Por outro lado, investigações em curso devem ser encaminhadas para o Juízo do domicílio da vítima, devendo ser eventual ação penal intentada obedecer à nova regra.

Outra alteração legislativa importante foi a edição da Lei 14.132/21 que insere no Código Penal o art. 147-A para tipificar o crime de perseguição. A finalidade é a tutela da liberdade individual, abalada por condutas que constrangem alguém a ponto de invadir severamente sua privacidade e de impedir sua livre determinação e o exercício de liberdades básicas.

De acordo com Cunha (2021), a perseguição de que trata o tipo penal nos remete ao denominado *stalking*, termo que, em inglês, é utilizado para designar a perseguição contumaz e obsessiva. O crime é de ação livre em todas as suas formas, mas o agente pode se valer de mensagens por meios variados (SMS, *WhatsApp*, *Telegram,* Skype etc.), de *e-mails*.

Nestas hipóteses, fala-se em *cyberstalking*, considerado um problema crescente diante da quantidade de pessoas que mantêm perfis em diferentes redes sociais, nas quais publicam, sem a devida cautela, imagens e informações de sua vida pessoal. De acordo com Cunha (2021), os instrumentos tecnológicos favorecem a perseguição da vítima, propiciando “a atuação do *stalker* aleatório, que, por acaso, se interessa obsessivamente por alguém com perfil exposto em rede social e passa a se valer desse meio para perseguir e atemorizar.”

Por vezes, as informações obtidas em ambientes virtuais permitem ao perseguidor a atuação tão eficaz quanto a presencial; ao mesmo tempo, o fácil acesso e o anonimato do *stalker* apresentam-se como fator de manutenção da prática delituosa. No contexto, urge a intervenção do direito como forma de controle social legítimo e eficaz de regulação da sociedade da informática.

3.2.1 Índice de Segurança da Unisys no Brasil

Unisys Security Index (2020) é o mais antigo monitoramento global de segurança digital – representa um índice que mede a segurança digital tanto em nível mundial quanto em nacional. “Globalmente, as preocupações gerais com a segurança do consumidor permanecem em alta, mas as prioridades mudaram devido ao impacto do COVID-19.” (UNISYS, 2020)

O Unisys Security Index de 2020 foi baseado em pesquisas nacionais de amostras representativas de um total de 15.699 residentes adultos de 18 a 64 anos de idade em 15 países. Foram aplicadas entrevistas online junto a grupos

epresentativos com o mínimo de 1.000 indivíduos de várias países, inclusive o Brasil.

Durante a pesquisa, realizada entre 16 de março e 5 de abril de 2020, a pandemia de COVID-19 era predominante em todos os países analisados. Em nível mundial, foi constado que: 58% as preocupações com a segurança pessoal tiveram o maior aumento; 41% seriamente preocupado com uma violação de dados enquanto trabalhava remotamente; 62% estão preocupados com desastres naturais, como pandemias. (UNISYS, 2020)

No Brasil, os principais resultados foram que 71% não acreditam que organizações estão protegendo bem dados de clientes na nuvem; 80% estão preocupados com fraudes bancárias; 85% deixariam de fazer negócios com instituições financeiras que não cuidassem bem de seus dados; 72% estão preocupados com sua saúde física durante a crise de saúde mundial (UNISYS, 2020).

De acordo com a pesquisa de 2020, o Brasil é o país com o maior crescimento em preocupações relacionadas a assuntos de segurança no mundo. Estes dados justificam a relevância social presente pesquisa e a necessidade de aperfeiçoamento da legislação:

> [...] a fraude bancária e o roubo de identidade, assuntos extremamente ou muito preocupantes para 80% e 78% dos brasileiros, respectivamente. Invasões cibernéticas ou vírus compõem a terceira maior preocupação no Brasil, com 73%, seguido de desastres naturais, com 72%. Essa última área, que consiste na ocorrência de inundação, furacão, incêndio florestal ou epidemia, registrou um crescimento de 10% na preocupação em relação ao ano passado. Ao passo que a atenção com segurança nacional, que se refere à proteção à guerras e ao terrorismo, diminuiu 4% em relação à 2019, sendo muito importante para metade dos brasileiros (51%). Especificamente no âmbito da Covid-19, a infraestrutura de saúde do Brasil e a estabilidade econômica são as principais preocupações durante uma crise de saúde global, respectivamente para 85% e 84% dos entrevistados. Em terceiro, ficou a saúde física da família, considerada extremamente ou muito preocupante para 83% dos brasileiros durante a pandemia. (UNISY, 2021)

Estes índices são exemplos importantes e refletem a importância no combate à criminalidade cibernética na sociedade contemporânea.

4 A PREVENÇÃO COMO FATOR DE PROTEÇÃO

Um dos principais fatores de sucesso dos ataques cibernéticos é a exploração das vulnerabilidades do usuário final. Muitos usuários ainda não se deram conta das ameaças de uma simples visita à *internet.*

Por isso, é muito importante investimento na prevenção. Empresas e governos devem investir em campanhas educativas de navegação segura e conscientização sobre o bom uso das ferramentas e tecnologias. Tais campanhas, de acordo com Araújo (2018, p. 11), visam à prevenção e minimização dos danos. Outras medidas simples, indicadas pelo autor, são a ativação da extensão dos arquivos, monitoramento dos anexos dos *e-mails,* manutenção de programas atualizados, controle de permissões de instalação e execução, utilização de aplicativos de fontes confiáveis

Ademais, de acordo com Pinheiro (2011), é possível melhorar o nível de proteção dos entes públicos, das empresas e dos dados dos cidadãos brasileiros. Para tanto, propõe a educação digital como meio de inclusão digital e prevenção, por meio da implementação de campanha de conscientização de segurança da informação pública, voltada ao cidadão e aos servidores públicos, orientando sobre proteção de senha, bloqueio de estação de trabalho, necessidade de desligar o equipamento quando não estiver sendo usado e de manter atualizados os *softwares* de antivírus.

Araújo (2018, p. 100) explica que algumas empresas de cibersegurança também desenvolvem ferramentas gratuitas para descriptografar dados infectados. Diante de ataques, a equipe de segurança da informação poderá estudá-lo, podendo desenvolver novos mecanismos de defesa para novos vírus - os procedimentos de prevenção não se esgotam e outros procedimentos técnicos são utilizados.

Além disso, Pinheiro (2011) destaca que o Poder Público brasileiro precisa levar a sério as questões de segurança da informação nacional. Tem crescido os ataques a *sites* de governo, porque os mesmos são extremamente vulneráveis. Para tanto, elenca como necessário revisar nível de segurança da informação dos sites de governo, melhorando programação dos códigos fontes, criptografando bases de dados; implementar plano de contingência e continuidade e demais medidas para

evitar interrupção; realizar monitoramento permanente do ambiente, para pegar um ataque logo no início e identificar seu autor; criar policiamento online (não apenas a delegacia de crimes eletrônicos), bem como aprovar leis que melhorem tipificação dos crimes eletrônicos.

Assim, conforme ensina Woloszyn (2018, p. 154), é preciso a adoção de políticas públicas de pesquisa e desenvolvimento de uma tecnologia cibernética nacional, além da formação de quadros especializados que deem suporte técnico à legislação de combate a crimes cibernéticos, permitindo, assim, a responsabilização penal.

4.2 ANÁLISE DO PROCESSO INVESTIGATÓRIO: DESAFIOS ENFRENTADOS

A tarefa de identificar os sujeitos ativos dos crimes virtuais não é nada fácil, e isso se deve ao fato de que, na maioria das vezes, os criminosos utilizam da rede pública de *internet* (em espaços públicos como *shopping,* praças, *lan houses* entre outros), a qual a transferência de dados não fica protegida, o que facilita na interceptação para a prática delituosa e na não identificação desses sujeitos:

> Uma das questões mais complexas que envolvem os crimes virtuais e digitais é a identificação do usuário, devido aos hackers nem sempre é fácil rastrear o IP *(Internet Protocol* ou em português Protocolo de internet), o qual identifica o usuário, o qual atualmente só é fornecido mediante solicitação judicial, a proposta é de que as forças policiais e o MP, possuam acesso de forma livre sem a necessidade de requisitar, até mesmo como forma de agilizar essa identificação e cessar o crime, pois esse dado deve oferece, nome, filiação e o endereço domiciliar do indivíduo, cabe aqui ressaltar que muitos criminosos aproveita-se de *lan house* para o cometimento do crime, o que dificulta e muito a identificação, sem contar ainda que softwares atuais conseguem mascarar o IP, ou os provedores se mostram carentes de dados essenciais do usuário. (SOUZA, 2018)

Por isso, há alguns métodos que são realizados pelas equipes investigadoras capazes de auxiliar na identificação, e é de suma importância também que a autoridade policial esteja sempre se atualizando, fazendo da tecnologia sua aliada para a busca de provas para um eventual processo penal.

Desse modo, um dos recursos utilizados na investigação é o Protocolo de Internet(IP), o qual é muito importante para ajudar na identificação dos criminosos, já que é através do número do IP que será possível descobrir o local em que o

sujeito acessou arede, e assim, na localização dele. Assunção (2014, p.49) esclarece que o IP é um conjunto de números que identificam seu computador em uma rede, como se fosse um número de telefone: cada computador ou equipamento ligado à *internet* possui um endereço de IP.

Assim, o endereço de IP é um dos métodos de investigação para que o sujeito do crime seja identificado. No entanto, não é a única forma utilizada pelos investigadores, tendo em vista que existem vários instrumentos que possibilitam esconder o número do IP, tornando o trabalho deles mais delicado.

Dessa forma, uma outra técnica de investigação dos crimes virtuais é o da engenharia social. Assunção (2014, p. 64) explica que por meiso de técnicas é possível fazer com que alguém execute algum *software* malicioso (*malware*), como *keyloggers* ou *trojans,* que forneça informações, ou mesmo através de um *fake mail*, uma forma como podemos conseguir dados importantes. Por outro lado:

> Esta prática visa a enganação ou exploração da confiança dos usuários levando-os a efetuar uma determinada ação para obter informações importantes ou sigilosas sobre eles. Geralmente o golpista se faz passar por outra pessoa ou instituição, ou finge ser um profissional em determinada área. A diferença entre ataques de engenharia social e, por exemplo, a tentativa de um atacante conseguir acesso a um determinado site é a escolha das ferramentas utilizadas. Um atacante irá procurar por vulnerabilidades no servidor da vítima enquanto um engenheiro social utilizará algumas técnicas de persuasão estimulando o medo, a curiosidade, a ganância ou a simpatia da vítima para obter a informação ou acesso desejado (CASSANTI, 2014, p.15-16).

A engenharia social, portanto, é meio utilizado para influenciar alguém na rede (por exemplo, uso de símbolos de órgãos públicos, de empresas e instituições) e que tem como objetivo coletar dados e informações sigilosas. Apesar desta técnica ser utilizada frequentemente utilizada por criminosos, como uma forma de coletar dados, também é instrumento hábil utilizado por investigadores.

Como bem destaca Wendt e Jorge (2012, p.22) a engenharia social pode também ser utilizada no âmbito de investigação criminal contra o crime. Exemplo comum é o caso de policial infiltrado em uma organização criminosa para coletar indícios sobre a prática de crimes. Nesses casos são utilizadas técnicas de engenharia social para que seja coletado o maior número de informações.

Ainda, existem também as chamadas fontes abertas, as quais são aplicadas

de forma que disponibilizará ao investigador, buscar livremente em qualquer lugar (meio) e sem restrições, os dados que necessita para dar continuidade a sua investigação. Nesse sentido, Barreto e Wendt (2020, p.15), nos elucida muitas informações estão disponíveis ao público e não exigem nenhuma restrição ao acesso – são conhecidas também como Inteligência de Fontes Abertas, ou seja, “uma forma de coletar selecionar e adquirir informações que possam ser úteis à produção do conhecimento. Podem ser obtidas através da leitura de jornais, periódicos, pesquisas de cunho acadêmico, livros, revistas, e principalmente através da *Internet.”*

As fontes abertas, juntamente dos outros métodos de investigações vêm auxiliando e desempenhando um papel fundamental na investigação policial, têm por objetivo a produção de provas e a identificação dos criminosos, e, assim, ajuda na construção do inquérito ou até mesmo pode evitar a consumação das práticas criminosas virtuais.

Ao mesmo tempo que a internet é de grande importância para a sociedade, trouxe como ponto negativo as práticas criminosas. De acordo com Lessa e Vieira (2017, p. 19), cumpre às autoridades policiais investigar essas práticas, em um primeiro momento, para apurar a materialidade e autoria do crime, pois surgem muitos desafios quanto ao procedimento investigatório que devem ser superados para alcançar a celeridade e eficácia na identificação do responsável.

Neste ponto, a Lei Geral de Proteção de Dados (Lei n.º 13.709/2018) traz reflexos importantes em sede das investigações criminais. Ao analisar a Lei 12.965/2014 - Marco Civil da Internet, é possível apontar o entrave nas investigações devido à necessidade de obter ordem judicial para buscar as informações necessárias, visando à correta identificação do usuário responsável pelo crime.

Konno Júnior (2021) explica que durante a investigação criminal, os investigadores se deparam com situações em que é necessária a obtenção de dados que possam individualizar determinada pessoa. São necessárias às diligências policiais informações quanto ao cadastro de linhas telefônicas, assinatura de internet fixa, contas bancárias e diversas outras situações, tanto para a identificação de investigados, quanto para outras vítimas.

Por isso, para o autor, o Marco Civil da *Internet* não é aplicável a uma conduta criminosa e, por isso, é possível a requisição dos dados cadastrais pela Autoridade Policial durante a investigação de qualquer crime:

> Pacífico também na doutrina e na jurisprudência a dispensa à reserva de jurisdição, prescindindo de autorização judicial para tanto. Também, pacífico é o entendimento de que não há violação da intimidade do investigado, visto que tais dados não revelam detalhes pessoais, mas tão somente colaboram na sua individualização e localização. Porém, com a entrada em vigor da Lei Geral de Proteção de Dados, surge a disposição de armazenamento e tratamento de dados pessoais, abrangendo mais informações do que os dados cadastrais. A questão é, seria possível, em determinados casos específicos, o acesso a esses dados pessoais pela Autoridade Policial, dispensando-se a autorização judicial? (KONNO JUNIOR, 2020).

Para Konno (2020), assim como para Pinheiro (2020) o fornecimento de tais informações à Autoridade Policial dispensa autorização judicial. No mesmo sentido é a opinião de Leitão Júnior (2020) que entende que Lei Geral de Proteção de Dados trouxe reflexos positivos nas investigações criminais – com este novo marco legal, espera que cesse os arbítrios na negativa de dados pessoais requisitados em sede de investigações – a nova lei não pode ser pretexto para impedir ou dificultar o fornecimento ou acesso ágil e oportuno de dados fundamentais nas investigações.

5 CONSIDERAÇÕES FINAIS

A expansão da *internet* no decorrer dos anos trouxe inúmeros benefícios à sociedade, no entanto, em sentido paralelo, proporcionou abertura à prática de crimes virtuais. Trata-se a *internet,* portanto, de universo que tem sido associado à disseminação de práticas criminosas, inclusive já previstas por normas penais, demonstrando-se imperiosa a adaptação da legislação criminal voltada à adaptabilidade à nova criminalidade no ambiente virtual.

Nesse mesmo sentido, a doutrina majoritária entende como crime virtual toda conduta típica, antijurídica e culpável que se realiza por intermédio de computadores ou de redes computacionais como ferramenta para a prática delitiva. Além disso, faz-se possível classifica-los em *próprios* e *impróprios*. Ocorre que, independentemente da classificação doutrinária, se o computador for como meio para a prática do crime, este restará caracterizado, mesmo que exista tipo penal que puna, deforma

específica, a conduta cometida no meio virtual, independentemente de sua finalidade, se relaciona a bens jurídicos concernentes à informática ou a outros.

Já naquilo que se relaciona à sujeição ativa, os crimes virtuais, de regra, são comuns, ou seja, podem ser praticados por quem quer que seja, independentemente de caracteres pessoais ou funcionais. No que concerne ao polo ativo, entretanto, é comum o entendimento de que somente os *hackers* praticam crimes na *internet.* Ocorre que o termo (*hacker*) é somente uma expressão utilizada, dentre várias outras, no sentido da caracterização da pessoa que dispõe de conhecimentos informáticos bastantes para invadir sistemas. Ocorre que nem sempre sua atuação será ilícita.

Além disso, há várias designações possíveis para os referidos agentes, notadamente para aqueles que, efetivamente, praticam crimes virtuais, como os *crackers*, que utilizam seu conhecimento informático para praticar condutas danosas ou obtendo vantagens ilícitas, por intermédio de condutas como a danificação de sistemas e furto de senhas, dados e documentos. O objeto material dos delitos é o dispositivo informático alheio conectado ou não à *internet.* Já o núcleo do tipo se configura com a prática do verbo *invadir*, equivalente a ocupar determinado lugar à força. Trata-se do primeiro tipo penal consagrado pelo Poder Legislativo brasileiro relacionado ao ambiente virtual.

A superveniência do denominado Marco Civil da *Internet* permitiu a atuação no sentido da localização geográfica do ponto de acesso à rede mundial de computadores, a partir do qual foi acessado o aplicativo por intermédio do qual foi cometido crime. Notadamente no âmbito da pandemia da Covid-19, a prática dos crimes digitais cresceu de maneira assustadora, em decorrência do isolamento social imposto pelo Poder Público e, notadamente, da transferência de vários serviços para o *home office*.

Nesse sentido, para combater a criminalidade nesse contexto é que foi a publicação da Lei n.º 14.155, de 27 de maio de 2021, que altera o Código Penal para agravar os crimes de violação de dispositivo informático, furto e estelionato cometidos eletronicamente ou por meio da pela *internet*, tratando, contudo, de crime de ação livre em todas as suas formas, de maneira que o agente pode se valer de programas e aplicativos variados, notadamente de sistemas mensageiros como

WhatsApp, *Telegram*, *Skype* e *e-mails*.

A necessidade do referido diploma é corroborada por relatório da *Unisys Security Index*, que é o mais antigo índice de monitoramento global acerca da segurança digital, representando um índice que afere a segurança digital em níveis mundial e nacional. Conforme pesquisa publicada no ano de 2020, o Brasil é o país no qual mais aumentam preocupações concernentes à segurança no mundo, situação que reflete a importância quanto ao combate à criminalidade cibernética no mundo contemporâneo.

Finalmente, um dos principais fatores para o sucesso dos ataques cibernéticos é, justamente, a exploração das vulnerabilidades dos usuários que, por sua vez, ainda não perceberam a significância das ameaças concernentes à simples visita à *internet.* Demonstra-se imperiosa, nesse contexto, a educação digital dirigida à inclusão digital e à prevenção por intermédio da implementação de campanhas de conscientização relacionada à segurança da informação pública.

Há, portanto, necessidade de se voltar ao cidadão e servidores públicos, orientando acerca da proteção de senha, do bloqueio da estação de trabalho, da necessidade de desligar o equipamento quando não estiver em uso, bem como de manter atualizados os *softwares* de antivírus.

Ocorre que a identificação dos sujeitos ativos dos crimes virtuais é difícil, situação que se deve ao ao fato de que, em regra, os criminosos utilizam da rede de *internet* disponibilizada em espaços públicos, a exemplo de *shopping,* praças e *lan houses* entre outros. Nessas hipóteses, a transferência de dados não restaria protegida, situação que facilita a interceptação da prática delitiva, porém, dificulta a identificação dos agentes.

Há, ainda, métodos utilizáveis pelas equipes investigadoras que podem auxiliar nessa identificação, de maneira que devem se atualizar forma constante e ininterrupta no que concerne aos avanços tecnológicos. Uma dessas técnicas, entretanto, é a denominada *engenharia social*, contexto no qual se força ou se induz em erro o agente no sentido de executar *software* malicioso (*malware*), que forneçam informações sensíveis, ou um *fake mail*, para conseguir dados importantes.

Além disso, identifica-se a possibilidade de utilização de *fontes abertas,* que

podem disponibilizar ao investigador a busca livre em qualquer lugar e sem restrições dos dados necessários para dar continuidade no que concerne à sua investigação. Estas, em paralelo a outros métodos investigativos, auxiliam no desempenho do fundamental papel na investigação policial, notadamente no que se relaciona à produção de provas e a identificação dos criminosos.

Tais estratégias podem auxiliar na construção do inquérito e, excepcionalmente, evitar a consumação de práticas criminosas virtuais. Nesse âmbito é que a Lei Lei Geral de Proteção de Dados (LGPD), em que pese sua relevância quanto às investigações criminais, não pode impedir ou dificultar o fornecimento ou o rápido e oportuno acesso a dados necessários às investigações.

Conclui-se que o combate à criminalidade digital no Brasil perpassa não apenas a necessidade de tipificação das condutas danosas praticadas no ambiente virtual, como, também, necessita de uma política pública dirigida à educação dos usuários das redes. Além disso, é imperiosa a constante evolução das técnicas investigativas concernentes a essas práticas, assim como a remoção de barreiras legislativas concernentes à obtenção de dados dos agentes.

REFERÊNCIAS

ALBUQUERQUE, Roberto Chacon de. Os objetos intangíveis na era da criminalidade informática. **Espaço Jurídico,** Jornal of Law, v.7, n.2, p.165-178, 2006. Disponível em: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/8794>. Acesso em: 02 mar. 2021.

ARAÚJO, Fábio Lucena de. ASPECTOS JURÍDICOS NO COMBATE E PREVENÇÃO AO RANSOMWARE. *In:* DOMINGOS, Fernanda Teixeira Souza et al. C**rimes cibernéticos:** coletânea de artigos. Brasília: MPF (Ministério Público Federal), 2018. Cap. 5. p. 90-115. Disponível em: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos. Acesso em: 22 jul. 2021.

ASSUNÇÃO, Marcos Flávio Araújo. **Segredos do *Hacker* Ético.** 5. Ed. Florianópolis: Visual Books, 2014.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil,** de 05 de outubro de 1988. Preâmbulo. Disponível em:

<http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 30 jun. 2021.

_____. **Lei nº 14.155, de 2021**. Brasília, DF, 27 maio 2021. Justificação. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=8889742&ts=1600958354757&disposition=inline. Acesso em: 03 ago. 2021.

_____. **Decreto-Lei nº 2.848 de 7 de dezembro de 1940**. Código Penal. Diário Oficial da República Federativa do Brasil, Brasília, DF, 31 dez. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 11 jun. 2020.

_____. **Lei nº 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da República Federativa do Brasil, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 11 jun. 2020.

_____. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 11 jun. 2020.

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

_____; WENDT, Emerson. **Inteligência e investigação criminal em fontes abertas**. Rio de Janeiro: Brasport, 2020.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal:** Parte Especial, v.3, 14 ed., São Paulo: Saraiva Jur, 2018.

CAIADO, Felipe B.; CAIADO, Marcelo. Combate à pornografia infantojuvenil com aperfeiçoamentos na identificação de suspeitos e na detecção de arquivos de interesse. *In:* DOMINGOS, Fernanda Teixeira Souza *et al*. C**rimes cibernéticos**: coletânea de artigos. Brasília: MPF (Ministério Público Federal), 2018. Cap. 1. p. 8-25. Disponível em: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos. Acesso em: 22 jul. 2021.

CAPEZ, Fernando. **Curso de Direito Penal.** Parte Geral, v.1, 15 ed. São Paulo: Saraiva, 2011.

CARDOSO, Nágila Magalhães. A pandemia do cibercrime. **Revista Eletrônica Direito & Ti**, [*s. l*], v. 1, n. 12, 2020. Disponível em: https://direitoeti.emnuvens.com.br/direitoeti/article/view/88. Acesso em: 23 jul. 2021.

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais**. Rio de Janeiro:

Brasport, 2014.

COSTA, Adriano Sousa; FONTES, Eduardo; HOFFMANN, Henrique. Lei 14.155/21 incrementa punição de crimes eletrônicos e informáticos. **CONJUR**, [*s. l*], 28 maio 2021. Disponível em: https://www.conjur.com.br/2021-mai-28/opiniao-lei-1415521-incrementa-punicao-crimes-eletronicos-informaticos#author. Acesso em: 26 set. 2021.

COSTA, Thabata Filizola. **A importância do Marco Civil da *Internet*:** lei nº 12.965/14. Lei nº 12.965/14. 2016. Disponível em: https://thabatafc.jusbrasil.com.br/artigos/313088224/a-importancia-do-marco-civil-da-internet. Acesso em: 14 mar. 2021.

CRESPO, Marcelo. **Crimes digitais**: do que estamos falando? 2015. Disponível em: https://canalcienciascriminais.jusbrasil.com.br/noticias/199340959/crimes-digitais-do-que-estamos-falando. Acesso em: 02 ago. 2021.

CUNHA, Rogério Sanches. **Manual de Direito Penal**. Parte geral. 3 ed. Rio de Janeiro: Jus Podivm, 2015.

CUNHA, Rogério Sanches. **Lei 14.132/21:** insere no código penal o art. 147-a para tipificar o crime de perseguição. Insere no Código Penal o art. 147-A para tipificar o crime de perseguição. 2021. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2021/04/01/lei-14-13221-insere-no-codigo-penal-o-art-147-para-tipificar-o-crime-de-perseguicao/. Acesso em: 03 ago. 2021.

FEBRABAN - Federação Brasileira de Bancos. **Conheça as tentativas de golpes financeiros mais comuns na pandemia e saiba como evitá-los**. 2021. Disponível em: https://portal.febraban.org.br/noticia/3522/pt-br/. Acesso em: 21 jul. 2021.

FIGUEIREDO, Rudá. **Crimes eletrônicos e Lei 14.155/2021**. 2021. Ministério Público da Bahia. Disponível em: https://webcache.googleusercontent.com/search?q=cache:HVygkI8lRrQJ:https://www.mpba.mp.br/sites/default/files/biblioteca/criminal/artigos/codigo_penal_-_parte_especial/crimes_eletronicos_e_lei_14.155-2021.pdf+&cd=1&hl=pt-PT&ct=clnk&gl=br. Acesso em: 20 set. 2021.

FIORILLO, Celso Antônio Pacheco. **Crimes no meio ambiente digital.** São Paulo: Saraiva, 2013.

GIMENES, Emanuel Alberto Sperandio Garcia. Crimes virtuais. **Revista de Doutrina**: TRF4, [*s. l*], *on line*, 2013. Disponível em: https://revistadoutrina.trf4.jus.br/index.htm?https://revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html. Acesso em: 20 jul. 2021.

GRECO, Rogério. **Curso de Direito Penal.** Parte Geral, v.1, 17 ed. Rio de Janeiro: Impetrus, 2015.

KONNO JÚNIOR, Jânio. Dados cadastrais e dados pessoais na investigação criminal. **Revista Eletrônica Direito & Ti**, [*s. l*], v. 1, n. 12, 2020. Disponível em: https://direitoeti.emnuvens.com.br/direitoeti/article/view/89. Acesso em: 23 jul. 2021.

LESSA, Isabella Maria Baldissera; VIEIRA, Tiago Vidal. CRIMES VIRTUAIS: análise do processo investigatório e desafios enfrentados. In: SIMPÓSIO DE SUSTENTABILIDADE E CONTEMPORANEIDADE DAS CIÊNCIAS SOCIAIS, 5., **Anais [...],** 2017. p. 1-25. Disponível em: https://www.fag.edu.br/upload/contemporaneidade/anais/594c13e45d209.pdf. Acesso em: 05 ago. 2021.

LEITÃO JÚNIOR, Joaquim. REFLEXOS DA LEI GERAL DE PROTEÇÃO DE DADOS EM SEDE DAS INVESTIGAÇÕES CRIMINAIS. **Revista Eletrônica Direito & Ti**, [*s. l*], 2020. Disponível em: http://direitoeti.com.br/artigos/reflexos-da-lei-geral-de-protecao-de-dados-em-sede-das-investigacoes-criminais/. Acesso em: 23 jul. 2021.

PIMENTEL, Alexandre Pinto; CARDOSO, Mateus Queiroz. A regulamentação do direito ao esquecimento na lei do marco civil da *internet* e a problemática da responsabilidade civil dos provedores. **Revista da AJURIS**, v. 42, n. 137, Mar., 2015.

PINHEIRO, Patricia Peck. **Direito digital.** 4. ed. São Paulo: Saraiva, 2010.

_____. **Proteção de Dados Pessoais:** comentários à Lei n. 13.709/2018 (LGPD). 2.ed. Saraiva Educação. São Paulo, 2020.

_____. Como proteger sites de governo de atentados de cyberterrorismo, crimes eletrônicos e guerra cibernética. 2011. **Migalhas de peso.** Disponível em: https://www.migalhas.com.br/depeso/137303/como-proteger-sites-de-governo-de-atentados-de-cyberterrorismo--crimes-eletronicos-e-guerra-cibernetica. Acesso em: 04 ago. 2021.

MAUES, Gustavo Brandão Koury; DUARTE, Kaique Campos; CARDOSO, Wladirson Ronny da Silva. CRIMES VIRTUAIS: uma análise sobre a adequação da legislação penal brasileira. **Revista Científica da Fasete**, Paulo Afonso, p. 166-180, 2018. 2018-1. Disponível em: https://www.unirios.edu.br/revistarios/media/revistas/2018/18/crimes_virtuais.pdf. Acesso em: 23 jul. 2021.

NUCCI, Guilherme de Souza. **Manual de Direito Penal**. 13 ed. Rio de Janeiro: Forense, 2017.

MACHADO, Felipe. **Marco Civil traz efeitos na apuração criminal, mas pode invadir privacidade**. 2014. Disponível em: https://www.conjur.com.br/2014-jul-14/felipe-machado-marco-civil-traz-efeitos-apuracao-criminal. Acesso em: 03 ago. 2021.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. O problema na tipificação penal dos crimes virtuais. **Jus Navigandi**, Teresina, a. 6, n. 58, ago. 2002. Disponível em: < https://jus.com.br/artigos/3186/o-problema-na-tipificacao-penal-dos-crimes-virtuais>. Acesso em: 20 jul. 2021.

ROSSINI, Augusto Eduardo de Souza. Brevíssimas considerações sobre delitos informáticos. **Caderno Jurídico**, Ano 2, n. 4, jul. 2002.

SANTOS, Paulo Ernani Bergamo dos. Direito internacional e o combate à cibercriminalidade contra crianças. *In:* DOMINGOS, Fernanda Teixeira Souza *et al*. **Crimes cibernéticos**: coletânea de artigos. Brasília: MPF (Ministério Público Federal), 2018. Cap. 8. p. 156-183. Disponível em: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos. Acesso em: 22 jul. 2021.

SPINIELI, andré luiz pereira. Crimes informáticos: comentários ao projeto de lei nº 5.555/2013. *In:* DOMINGOS, Fernanda Teixeira Souza *et al*. **Crimes cibernéticos**: coletânea de artigos. Brasília: MPF (Ministério Público Federal), 2018. Cap. 10 p. 198-217. Disponível em: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos. Acesso em: 22 jul. 2021.

SORJ, Bernardo *et al* (org.). **Sobrevivendo nas redes:** guia do cidadão. São Paulo: Moderna, 2018. 82 p. Disponível em: https://crianca.mppr.mp.br/arquivos/File/publi/santillana/sobrevivendo_nas_redes_guia_2018.pdf. Acesso em: 05 jul. 2021.

SOUZA, Ludimila de Freitas. Marco civil da *internet* e os crimes virtuais. **Conteúdo Jurídico**, Brasília-DF: 05 ago. 2021. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/51965/marco-civil-da-internet-e-os-crimes-virtuais. Acesso em: 05 ago. 2021.

TEIXEIRA, Fernanda *et al* (org.). **Crimes cibernéticos:** coletânea de artigos. Brasília: MPF (Ministério Público Federal), 2018. 275 p. 2ª Câmara de Coordenação e Revisão, Criminal. Disponível em: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos. Acesso em: 22 jul. 2021.

UNIT 42. **Não entre em pânico**: ameaças cibernéticas covid-19. ameaças cibernéticas COVID-19. 2020. Disponível em: https://unit42.paloaltonetworks.com/covid19-cyber-threats/. Acesso em: 20 mar. 2021.

UNISYS. **2020 Índice de Segurança da Unisys no Brasil**. 2020. Principais descobertas no Brasil. Disponível em: https://www.unisys.com/unisys-security-index/brazil. Acesso em: 05 jul. 2021

_____. **Unisys Security Index**. 2020. Principais descobertas em todo o mundo. Disponível em: https://www.unisys.com/unisys-security-index/brazil. Acesso em: 05 jul. 2021.

_____. **Brasil é o país com maior crescimento em preocupações com segurança no mundo, mostra estudo da Unisy**. Disponível em: https://www.unisys.com/pt/news-release/br-brasil-e-o-pais-com-maior-crescimento-em-preocupacoes-com-seguran%C3%A7a/. Acesso em: 05 jul. 2021.

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

WOLOSZYN, André Luís. Ciberespionagem: entraves na apuração de provas e responsabilização penal. *In:* DOMINGOS, Fernanda Teixeira Souza *et al*. **Crimes cibernéticos**: coletânea de artigos. Brasília: MPF (Ministério Público Federal), 2018. Cap. 7. p. 134-155. Disponível em: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos. Acesso em: 22 jul. 2021.