CURSO DE DIREITO

Júlia Charão

OS CRIMES CIBERNÉTICOS NA LEGISLAÇÃO BRASILEIRA E OS PROCEDIMENTOS DE INVESTIGAÇÃO

Santa Cruz do Sul
2017

Júlia Charão

OS CRIMES CIBERNÉTICOS NA LEGISLAÇÃO BRASILEIRA E OS PROCEDIMENTOS DE INVESTIGAÇÃO

Trabalho de Conclusão de Curso, modalidade monografia, apresentado ao Curso de Direito da Universidade de Santa Cruz do Sul, UNISC, como requisito parcial para a obtenção do título de Bacharel em Direito.

Prof. Ms. Cristiano Cuozzo Marconatto
Orientador

Santa Cruz do Sul
2017

TERMO DE ENCAMINHAMENTO DO TRABALHO DE CURSO PARA A BANCA

Com o objetivo de atender o disposto nos Artigos 20, 21, 22 e 23 e seus incisos, do Regulamento do Trabalho de Curso do Curso de Direito da Universidade de Santa Cruz do Sul – UNISC – considero o Trabalho de Curso, modalidade monografia, da acadêmica Júlia Charão adequado para ser inserido na pauta semestral de apresentações de TCs do Curso de Direito.

Santa Cruz do Sul, 22 de novembro de 2017.

Prof. Ms. Cristiano Cuozzo Marconatto
Orientador

De tanto ver triunfar as nulidades, de tanto ver prosperar a desonra, de tanto ver crescer a injustiça, de tanto ver agigantarem-se os poderes nas mãos dos maus, o homem chega a desanimar da virtude, a rir-se da honra, a ter vergonha de ser honesto.

(BARBOSA, R., 1914)

AGRADECIMENTOS

Incialmente, agradeço a Deus pela luz e força constantemente presentes na minha vida, me guiando e iluminando nos momentos de maior escuridão.

Agradeço, com especial carinho, aos meus pais, Marco Aurélio Charão e Solmi Elena Charão, por estarem sempre presentes me motivando a seguir em frente, por acreditarem na minha capacidade e, principalmente, por todo amor, carinho e paciência nos meus momentos de incerteza e nas inúmeras vezes em que estive ausente para poder concretizar esse sonho.

Aos meus amigos e familiares que nos momentos de dúvida me incentivaram e me fizeram ter a certeza que eu conseguiria atingir meus objetivos. Agradeço, ainda, aos professores e colegas do Curso de Direito por toda sabedoria compartilhada e pelo companheirismo.

Ao professor orientador, Cristiano Cuozzo Marconatto, por estar presente durante todo processo de realização desta monografia, transmitindo encorajamento, motivação e, acima de tudo, me auxiliando com todo seu conhecimento jurídico.

RESUMO

O presente trabalho monográfico trata do tema “crimes cibernéticos na legislação brasileira e os procedimentos de investigação”. Objetiva-se, com o auxílio da doutrina recente, analisar a legislação penal brasileira com relação aos crimes perpetrados no ambiente virtual, bem como tratar dos procedimentos de investigação utilizados para desvendar a autoria e garantir a repreensão dos crimes cibernéticos, analisando se tais procedimentos são efetivos no combate à criminalidade virtual. Considerando que os crimes cibernéticos estão crescendo com uma velocidade assustadora em nosso país, torna-se necessário promover uma discussão acerca desse tipo de delito, a fim de que seja possível promover o combate e, inclusive, a conscientização da população em relação ao uso das novas tecnologias. Assim, ocorrerá uma dissertação sobre a história da internet, o surgimento dos tipos penais cibernéticos e a relação da tecnologia informática com o Direito Penal. Após, será feita uma análise dos tipos penais presentes na legislação brasileira que podem ser praticados no meio virtual, assim como examinar-se-á quais os procedimentos de investigação utilizados. Dessa forma, o presente trabalho promove um estudo sobre os delitos executados no meio virtual e avalia se a legislação penal brasileira e instrumentos de investigação utilizados poderão promover um combate eficaz à esse tipo de crime. Para tanto, utiliza-se a metodologia de pesquisa bibliográfica, a qual consiste na leitura, fichamento e análise das doutrinas e artigos científicos sobre o tema.

Palavras-chave: crimes cibernéticos; legislação penal; procedimentos investigação.

ABSTRACT

The present study deals with the theme "cybercrimes in Brazilian legislation and investigation procedures". The purpose is to analyze, through recent doctrine, Brazilian criminal law in relation to crimes perpetrated on the internet and the investigation procedures used to discover the author of the crime and ensure the reprimand of cybercrime, analyzing if the criminal investigation is effective in preventing and fighting cybercrime. Considering that computer-related crimes are increasing at a fast pace in Brazil, it is necessary to promote a discussion about this type of crime, with the purpose to foment actions against cyber crimes and raise awareness for the responsible use of new technology. There will be a dissertation about the history of the Internet, the emergence of cybercrime laws and the relation between computer technology and criminal law. Afterwards, it will analyze the actions that are defined in law as a crime, as well as examine the investigative procedures. The presente work will promote a study about the computer crimes and assesses how well the Brazilian criminal laws and investigations can fight and prevent cybercrime. To do so, this research will use the methodology of bibliographic research, which consists in read and analyze doctrines and scientific articles related to the theme.

Keywords: cybercrimes; criminal law; investigation procedures.

SUMÁRIO

1 INTRODUÇÃO

É sabido que as transformações sociais e tecnológicas ocorridas nas últimas décadas revolucionaram a vida em sociedade, ampliando e modificando as formas de comunicação, acesso à informação e comércio. Dessa forma, as novas tecnologias e, principalmente, o advento da internet trouxeram inúmeros benefícios para a população mundial, tais como o rápido acesso à informação e a facilidade de comunicação entre os indivíduos, através de *sites*, aplicativos e redes sociais. Portanto, é inegável que o processo de globalização é constante e produz modificações profundas na sociedade contemporânea.

Nesse contexto, verifica-se que o acesso à internet está crescendo rapidamente, atingindo um número cada vez maior de pessoas que estão em frequente contato com o mundo virtual. Por outro lado, este quadro fático acaba facilitando, também, a perpetração de delitos com o auxílio da internet e das novas tecnologias.

Dessa forma, o cidadão se encontra cada vez mais exposto e vulnerável a ataques cibernéticos, o que evidencia a necessidade de uma legislação e persecução penal eficazes, promovendo, assim, a proteção do usuário da *web.*

A tendência é que os avanços tecnológicos e o amplo acesso à rede mundial de computadores assumam um papel cada vez mais relevante em nosso cotidiano, sendo que o Direito possui a árdua tarefa de se moldar a essa nova realidade e acompanhar a rápida evolução tecnológica.

Diante o exposto, o presente estudo tem como finalidade analisar a tipificação dos crimes cibernéticos na legislação penal do Brasil, promovendo comentários sobre os crimes que se encontram no Código Penal de 1940, que podem ser praticados em meio digital, assim como a legislação própria para tais delitos. Também tem por pretensão promover uma análise sobre quais os procedimentos de investigação utilizados para esclarecer a autoria dos crimes digitais, desvendando quais as formas mais utilizadas pelos criminosos virtuais para consumar o delito.

Para tanto, será utilizada a metodologia de pesquisa bibliográfica, a qual se baseia no estudo de obras jurídicas e artigos científicos acerca do tema, assim como na análise da legislação em vigor, utilizando o método dedutivo. Nesse passo, o presente trabalho será dividido em três capítulos.

Inicialmente, serão abordados os aspectos históricos do surgimento da

internet e dos primeiros delitos executados no meio virtual, assim como a evolução da legislação penal informática. Ainda, se promoverá uma discussão acerca da relação entre o Direito e as novas tecnologias.

Posteriormente, analisar-se-á o conceito de crime cibernético, bem como os delitos mais frequentemente cometidos através de dispositivos informáticos, promovendo um estudo sobre os crimes tipificados no Código Penal de 1940, no Estatuto da Criança e do Adolescente e os novos tipos penais trazidos pela Lei 12.737, de 30 de novembro de 2012.

Por fim, será feita uma análise sobre os métodos de investigação utilizados para comprovar a materialidade e a autoria dos crimes cibernéticos, com a finalidade de averiguar quais os procedimentos investigativos mais eficientes no combate aos crimes realizados no ambiente virtual.

2 ANTECEDENTES HISTÓRICOS DA INTERNET

A internet teve sua origem em pesquisas militares, na década de 1960, no auge do conflito entre os Estados Unidos e a União Soviética, período conhecido como “Guerra Fria”. A Agência de Investigação de Projetos Avançados (ARPA), um órgão militar e científico criado pelo governo dos Estados Unidos, criou a ARPANET, uma rede de armazenamento de dados desenvolvida com o intuito de evitar a perda irreparável de documentos do governo em caso de possíveis ataques soviéticos. A ARPANET, inicialmente, interligava a Universidade da California, a Universidade de Stanford e a Univerdade de Utah, utilizando da tecnologia do *packet switching* (troca de pacotes) e do armazenamento virtual (WENDT; JORGE, 2012).

Ao longo das décadas de 1970 e 1980, a ARPANET se expandiu realizando significativos avanços na comunicação remota entre computadores, porém, sua utilização ficou restrita ao ambiente acadêmico e científico. Em 1973, ocorreu a primeira conexão internacional interligando a Inglaterra e a Noruega, e, posteriormente, no final dos anos 70, a ARPANET passou a utilizar o TCP/IP, protocolo padrão usado até hoje. Durante a década de 1980 a ARPANET se expandiu pelos Estados Unidos promovendo a interligação entre as universidades, órgãos militares e o governo e passou a ser chamada de internet (WENDT; JORGE, 2012).

Entretanto, a verdadeira revolução do acesso à internet aconteceu com o desenvolvimento do famoso www. Antes, entre os anos de 1980 e 1990 “a capacidade de transmissão de gráficos era muito limitada e era dificílimo localizar a receber informações” (CASTELLS, 2005, p. 87). Então, no ano de 1990, o programador inglês Tim Bernes-Lee, em colaboração com Robert Cailliau, “construiu um programa navegador/editor, e chamou esse sistema de hipertexto de *World Wide Web*, a rede mundial” (CASTELLS, 2003, p. 18).

O surgimento do www deixou o acesso à internet significativamente mais aberto, compreensível e confortável, pois, conforme afirma Côrrea (2000, p. 10), “ofereceu aos usuários aquilo que mais apreciavam: a utilização da imagem, som e movimento, em vez da melancolia do texto puro”. O *world wide web* é um conjunto de padrões e técnicas que permitem o uso da internet por meio de navegadores, empregando o hipertexto e suas relações com a multimídia, como som e imagem. Assim, com a simplicidade do funcionamento do *world wide web* e o desenvolvimento das ferramentas do código HTML e do protocolo HTTPS, foi

possível a criação de sites dinâmicos e visualmente atrativos, o que impulsionou aumento do acesso à internet e consolidou o seu uso na vida em sociedade (CÔRREA, 2000).

A história da internet no Brasil começou no ano de 1988 quando a Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) se conectou ao Fermilab, um dos mais importantes centros de pesquisa científica dos Estados Unidos. A conexão entre a FAPESP e a instituição americana aconteceu através da utilização da *Bitnet*, uma rede que possibilitava a troca de correio eletrônico e arquivos. Pode-se observar que o desenvolvimento da internet em terras brasileiras aconteceu, primeiramente, no meio acadêmico e científico, realizando conexões entre os laboratórios e universidades brasileiras com universidades americanas (KNIGHT, 2014).

A internet deixou de ser de uso exclusivo da comunidade acadêmica e científica no Brasil quando foi regulamentado o seu uso comercial no ano de 1995. Ainda, em maio deste mesmo ano, foi criado o Comitê Gestor da Internet, com o objetivo efetivar a participação da sociedade nas decisões acerca da implantação e do uso da internet no Brasil e contou com a participação de membros do Ministério das Comunicações e do Ministério de Ciência e Tecnologia, representantes de provedores e prestadores de serviços ligados à Internet, representantes de usuários e da comunidade acadêmica (CÔRREA, 2000).

Conforme afirma Vieira (2003, p. 11), “o ano de 1995 pode ser considerado o marco-zero da internet comercial no Brasil e no mundo”.

> Assim, em meados da década 1990, a Internet estava privatizada e dotada de uma arquitetura técnica aberta, que permitia a interconexão de todas as redes de computadores em qualquer lugar do mundo; a www podia então funcionar com *software* adequado, e vários navegadores de uso fácil estavam à disposição do público (CASTELLS, 2003, p. 19)

Entretanto, foi apenas no final de década de 90 que a internet começou a virar febre mundial, crescendo em proporções extraordinárias, tanto em número de usuários quanto de provedores. A exploração econômica da internet e a constante evolução da navegação na *web*, tornando-a mais agradável e acessível, acabou contribuindo significativamente com o processo de globalização. O constante crescimento do acesso à rede auxiliou, inclusive, na consolidação da sociedade da informação, pois a internet se estabeleceu como importante meio de comunicação e divulgação de informações (CASTELLS, 2005).

O rápido desenvolvimento tecnológico e as facilidades advindas das tecnologias da informação e comunicação fizeram com que o ambiente virtual se tornasse parte da rotina das pessoas. Assim, na visão de Castells (2005, p. 40) “as redes interativas de computadores estão crescendo exponencialmente, criando novas formas e canais de comunicação, moldando a vida e, ao mesmo tempo, sendo moldadas por ela”.

O aumento da utilização da internet aconteceu, também, em razão do barateamento dos computadores e da criação dos dispositivos móveis com acesso à rede, tais como os *notebooks*, *smartphones* e *tablets*. Dessa forma, podemos utilizar a internet em praticamente qualquer lugar no nosso dia-a-dia (WENDT; JORGE, 2012).

Sobre as implicações criadas pelo advento da era digital, Corrêa (2000, p. 2) afirma que

> [...] a rapidez desse salto qualitativo e quantitativo de tecnologia, porém, é incompatível com os conceitos e padrões contemporâneos, contribuindo, assim, para o aparecimento de conflitos entre as novas tecnologias e a sociedade. A presença cada vez mais forte dos computadores em nossas vidas, a capacidade de coletar e analisar dados pelas empresas e pelo Estado, e de disseminá-los através de rápidas vias de telecomunicações, nos têm proporcionado benefícios, mas, na mesma proporção, também malefícios.

Hoje, as pessoas estão dependentes da internet, utilizando-a para comunicação, trabalho, compras e lazer, e assim, consequentemente, passamos inúmeras horas do dia conectados à rede. Assim sendo, inevitavelmente, o ambiente virtual começou a ser usado para práticas delituosas, pois “a internet é um paraíso de informações, e, pelo fato de estas serem riquezas, inevitavelmente atraem o crime. Onde há riqueza há crime” (CÔRREA, 2000, p. 43).

2.1 Evolução dos crimes cibernéticos e da legislação penal informática

Os delitos praticados contra ou por meio de dispositivos informáticos foram denominados de crimes cibernéticos. Os termos *“*cibercrime*”*, “crimes digitais”, “crimes informáticos”, dentre outras nomenclaturas, também são usados para definir as condutas realizadas através da internet que acabam causando transtornos ou prejuízos à vítima. Cabe ressaltar que os crimes cibernéticos não são apenas aqueles que se concretizam através da internet, mas também aqueles que praticados no sistema cibernético como um todo (WENDT; JORGE, 2012).

Os crimes cibernéticos tiveram início na década de 1960 com delitos de alteração, cópia e sabotagem de sistemas computacionais. Existem divergências acerca da definição do primeiro delito cometido. Entretanto, alguns doutrinadores apontam que o primeiro crime cibernético teria ocorrido no ano de 1978, na Universidade de Oxford, quando um aluno copiou uma prova de uma rede de computadores, ou seja, o delito teria se caracterizado por uma invasão seguida de uma cópia. Todavia, neste caso, a conduta do estudante não pode ser considerada muito lesiva, tendo em vista que os arquivos do computador não foram removidos ou danificados, o aluno apenas copiou o arquivo que desejava, sem a intenção de publica-lo (JESUS; MILAGRE, 2016).

Porém, foi apenas mais tarde, nas décadas de 1980 e 1990, quando o acesso à internet se expandiu, que os crimes cibernéticos se tornaram mais comuns. Dentre as práticas delituosas mais utilizadas na época se encontram a disseminação de vírus, pornografia infantil, invasão de sistemas e a pirataria (JESUS; MILAGRE, 2016).

No ano de 1982, Richard Skrenta, na época com apenas quinze anos de idade, desenvolveu um vírus chamado *Elk Cloner,* que tinha por objetivo infectar computadores e se difundia através de cópias de disquetes contaminados. Nota-se que o termo “vírus de computador” ainda não existia à época. Em 1984 foi criado um vírus de computador chamado *Brain,* que atingia o setor de inicialização do computador e causava lentidão nas operações do sistema. O *Brain* foi criado com a finalidade de detectar o uso não autorizado de um software médico desenvolvido para monitoramento cardíaco. Todavia, o código sofreu alterações maliciosas que o transformaram em um vírus que se disseminava através de disquetes infectados. Em relação ao assunto, existem divergências sobre o surgimento do primeiro vírus de computador, para alguns o primeiro foi o vírus *Elk Clone,* porém, outros entendem que o pioneiro foi o vírus *Brain* (WENDT; JORGE, 2012).

Já no ano de 1986, surgiram os primeiros Cavalos de Troia, dentre os quais pode-se exemplificar o caso do *PC White*, que se apresentava como um processador de textos, porém, quando executado, apagava e corrompia os arquivos do disco rígido do computador. Mais tarde, no ano de 2004, com a popularização de dispositivos utilizados para o acesso à internet, surgiu o primeiro vírus de celular, denominado *Cabir*, que se disseminava por *Bluetooth* com o propósito de descarregar completamente a bateria dos celulares infectados (WENDT; JORGE, 2012).

Portanto, pode-se observar que as práticas delituosas, como, por exemplo, a invasão de computadores e a disseminação de vírus, surgiram e evoluíram simultaneamente com o progresso da tecnologia. Sendo assim, os crimes cibernéticos se tornaram um problema de abrangência mundial, pois o ambiente virtual fornece uma sensação de liberdade e impunidade aos criminosos.

A Suécia foi o primeiro país a criar normas em relação à violação de bens informáticos. Porém, foram os Estados Unidos da América os precursores do verdadeiro combate aos crimes cibernéticos, promovendo debates sobre os delitos cometidos via internet desde 1970 e promulgando, em 1986, a *Computer Fraud and Abuse Act.* Inclusive, no ano de 1988, Robert Morris foi o primeiro *hacker* a ser condenado pela lei *Computer Fraud and Abuse Act* norte-americana, já que foi o responsável pela criação de um dos primeiros vírus do mundo que prejudicou mais de 6 mil computadores *(*JESUS; MILAGRE, 2016).

Já em relação ao surgimento dos delitos digitais no Brasil,

> [...] temos notícias dos primeiros crimes de *phising scam* bancário (pescaria de senhas) em 1999. Igualmente, outro caso célebre foi o de um empresário e ex-controlador de uma rede de varejo, acusado à época de ter enviado, de Londres, *e-mails* para o mercado financeiro com informações falsas alardeando o risco de quebra de um banco. Muito se debateu, a partir de então, sobre os problemas envolvendo a investigação de crimes informáticos, que poderiam ser praticados em qualquer localidade do mundo. Mais que isso, começou-se a refletir sobre a necessidade de leis que tratassem de crimes informáticos (JESUS e MILAGRE, 2016, p. 24).

Apesar do Código Penal de 1940 já prever a punição em relação à determinados crimes comuns que podem ser cometidos por meio da internet, começou a se questionar a necessidade de leis específicas para tratar dos crimes cibernéticos. A legislação penal informática no Brasil teve como um dos seus marcos a Lei nº 9.609 de 19 de fevereiro de 1998, já que foi a primeira lei a descrever infrações no âmbito da informática, conforme podemos exemplificar através do art. 12 da referida lei:

> Art. 12. Violar direitos de autor de programa de computador:
> Pena - Detenção de seis meses a dois anos ou multa.
> § 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente:
> Pena - Reclusão de um a quatro anos e multa.
> § 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.
> § 3º Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo:

> I - quando praticados em prejuízo de entidade de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo poder público;
> II - quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo.

Ainda no ano de 1998, o Supremo Tribunal Federal julgava um caso de pornografia infantil nas antigas BBS (*Bulleting Board System/Internet*). O julgado se tornou histórico e foi relatado pelo Ministro Sepúlveda Pertence, que afirmou que nem todos os delitos cometidos por meio da internet necessitavam de nova tipificação, pois a tecnologia poderia ser utilizada apenas como um novo meio para a concretização de crimes conhecidos (JESUS; MILAGRE, 2016).

Mais tarde, a Lei nº 9.983 de 2000 trouxe algumas alterações ao Código Penal, dentre elas se encontra a tipificação de crimes cibernéticos, tais como os crimes de "Inserção de dados falsos em sistema de informações" e "Modificação ou alteração não autorizada de sistema de informações" (BRASIL, 2000).

A primeira condenação por pirataria virtual em terras brasileiras aconteceu somente em janeiro de 2004, quando um jovem de 19 anos foi condenado a seis anos e quatro meses de prisão por aplicar golpes através da internet no Brasil e nos Estados Unidos (2006, <http://www1.folha.uol.com.br>).

Outro caso de destaque foi a Operação Pégasus da Polícia Federal, a qual viabilizou a prisão de 114 piratas virtuais em sete estados brasileiros. A quadrilha se especializou na invasão de contas bancárias por meio da internet, desviando aproximadamente R$ 80 milhões no ano de 2005 (2006, <http://www1.folha.uol.com.br>).

Sobre a evolução da legislação brasileira em relação aos crimes cibernéticos, Jesus e Milagre (2016, p. 70) afirmam:

> Dentre vários projetos de lei sobre o tema que tramitam ou tramitaram no Congresso Nacional, destacamos o Projeto de Lei nº 84/99, de autoria do então deputado Deputado Luiz Piauhylino, apresentado em 24 de fevereiro de 1999. Esse projeto tramitou por 13 anos, recebeu substitutivos, posteriormente reuniu outros projetos que tratavam de temas semelhantes. Foi também apelidado de “AI-5 digital” e de “Lei Azeredo”, eis que o político brasileiro Eduardo Azeredo foi o relator do projeto em diversas fases e também um dos defensores da sua aprovação. O Projeto, que em sua redação original, em 1999, continha dezoito artigos, converteu-se na Lei nº 12.735/2012, com apenas quatro artigos. De fato, sofreu forte rejeição da sociedade, ativistas e pessoas que protestavam contra o possível vigilantismo e riscos de uma lei que poderia punir, segundo o ativismo, o “fato de ser internauta”. Não foi possível aprovar o Projeto de Lei nº 84/99 como desejado, tanto que desmanchou, desfigurou-se absolutamente, eis que, ao ler a Lei nº 12.735/2012, não se imagina que tenha se originado do

precitado projeto de lei. (Grifo original).

Ainda no ano de 2012, foi promulgada a Lei nº 12.737 que apresentou a tipificação de delitos cibernéticos, acrescentando os artigos 154-A e 154-B ao Código Penal de 1940, dentro dos crimes contra a liberdade individual. A referida lei ficou conhecida como “Lei Carolina Dieckmann”, em virtude de fato envolvendo a invasão do computador e o vazamento de fotos íntimas da atriz na internet. O caso teve grande repercussão na mídia à época, pois as fotos vazadas foram compartilhadas através das redes sociais e se espalharam rapidamente, o que acabou causando grande constrangimento à atriz e fermentou a discussão sobre o direito à intimidade dos usuários da internet (OLIVEIRA JUNIOR, 2013).

Outro momento importante para a legislação brasileira foi a promulgação da Lei nº 12.965, no dia 23 de abril de 2014, conhecida como o Marco Civil da Internet, que tem como objetivo estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil (CARVALHO, 2014).

Apesar das críticas, o Marco Civil da Internet se mostra uma norma importante dentro do Direito Brasileiro, pois disciplina os direitos e deveres dos usuários, estabelecendo uma ligação entre o direito e a tecnologia.

Assim, pode-se observar que o Brasil passou por grandes discussões acerca da necessidade de leis que regulassem o uso da internet no país e tipificassem os delitos cibernéticos. Hoje, verifica-se que a legislação brasileira já possui normas específicas tipificando os crimes informáticos, o que demonstra uma evolução em relação ao combate dos delitos cometidos dentro do ambiente virtual.

Segundo dados fornecidos pelo jornal Estadão, 42,2 milhões de brasileiros foram vítimas de crimes virtuais no ano de 2016, verificando-se um aumento de 10% no número de delitos cibernéticos em comparação com o ano de 2015 (2017, <http://economia.estadao.com.br>).

O Brasil ocupa, ainda, o 5º lugar no ranking de detecções de *malwares* bancários no planeta. O *malware* é um software malicioso que pode infectar computadores, *tablets* ou *smartphones*, corrompendo sistemas, roubando informações bancárias e, inclusive, tentando impedir que os usuários acessem seus próprios computadores. Ou seja, é uma grande ameaça cibernética que pode trazer inúmeros prejuízos para a vítima (2016, <http://www20.opovo.com.br>).

2.2 A relação entre o direito e as novas tecnologias

A internet está a cada dia mais se tornando uma ferramenta de uso indispensável no cotidiano das pessoas. Com o advento das novas tecnologias e a ampliação do uso da internet, principalmente através dos *smartphones*, está-se em constante contato com o mundo virtual. A tecnologia mudou as nossas formas de comunicação, negócios, consumo e afetou, inclusive, os nossos relacionamentos pessoais.

Os aspectos positivos dos avanços tecnológicos são abundantes e inquestionáveis, entretanto, também pode-se identificar inúmeros problemas e aspectos negativos provenientes destes avanços, como, por exemplo, o surgimento dos crimes cibernéticos. Deste modo, imprescindível que se proceda à uma análise da relação entre o Direito e as novas tecnologias, especialmente a internet.

Do ponto de vista da relação do Direito com a revolução tecnológica,

> [...] o grande desafio para o direito é a compreensão e o acompanhamento dessas inovações, garantindo assim a pacificação social, o desenvolvimento sustentável dessas novas relações e, acima de tudo, a manutenção do próprio Estado Democrático de Direito. Aos operadores do direito cabe a difícil tarefa de estudar e encontrar respostas, sensatas e inteligentes, para os novos desafios advindos desse novo paradigma, fazendo com que a pessoa humana e as novas tecnologias possam coexistir dentro de uma nova concepção de mundo (CORRÊA, 2000, p. 4).

No âmbito do Direito Penal esse desafio é ainda maior, uma vez que a tipificação dos procedimentos realizados no meio virtual não pode ser generalizada e necessita ser amplamente discutida, pois, uma das grandes qualidades da internet são a liberdade e o rápido acesso à informação. Portanto, o Direito Penal deve regulamentar o ambiente virtual e fornecer segurança aos seus usuários, mas, ao mesmo tempo, não deve restringir as suas liberdades individuais e o livre acesso à informação.

Nesse sentido, a existência da tecnologia de informática em rede de computadores no campo do Direito

> [...] propõe vários desafios, entre os quais o mais evidente é a necessidade de se construírem mecanismos reguladores para o controle das atividades desenvolvidas nesse meio, que impõe, pelas suas características, mudança de um paradigma repressivo para um paradigma preventivo em nossa legislação. Em outras palavras, a rede não pode ser controlada pela tentativa de proibição de acesso à informação, mas apenas pela maior socialização dos usuários nas formas adequadas e seguras de sua utilização (CÔRREA, 2000, p. 8).

As condutas transgressoras e lesivas que surgiram da evolução da tecnologia não podem ser ignoradas pelo ordenamento jurídico, pois, quando não existem limites, se torna extremamente difícil assegurar que as pessoas não invadam a esfera pessoal de outrem, causando danos. Logo, “a lei é, e sempre será, essencial para a prevenção e punição dos crimes, sejam estes dentro do mundo material ou digital” (CÔRREA, 2000, p. 58).

A falta de tipificação dos crimes informáticos pode gerar uma sensação de impunidade no meio virtual, e assim, consequentemente, ampliar a prática de condutas ilícitas na internet, pois os criminosos cibernéticos se sentem livres para delinquir e prejudicar terceiros. Outro fator que incentiva a prática de delitos é o anonimato, pois este funciona como um facilitador para a consumação dos delitos no meio virtual, possibilitando que o transgressor se esconda atrás do anonimato.

Nas palavras de Jesus e Milagre (2016, p. 20):

> Não podemos aceitar que na sociedade da informação vigore a lei de tabelião, autotutela ou a lei do mais forte, mas é sabido que o Direito deve prevalecer, fazendo valer a justiça nos conflitos entre cidadãos desta sociedade digital. Faz-se preciso o mínimo controle para fazer frente àquele que realiza uma conduta antissocial cibernética. Ser internauta não é delito, assim como ser cidadão não é infração criminal, mas ambos, internauta ou cidadão, podem praticar, sim, infrações. É cediço que, pelo princípio da legalidade, não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal. Ninguém pode ser responsabilizado por fato que a lei desconsidera como de relevância pena. O Direito, como ciência humana, não pode ficar para trás. Leis que estabeleçam os direitos dos usuários da Internet e deveres dos prestadores são fundamentais para que o Judiciário possa fazer frente a violações e riscos inerentes a sociedade da informação, e, sobretudo, de modo a evitar decisões contraditórias e injustiças diante de casos concretos.

Necessário que se destaque que o Direito está sempre atrás do fato social, ou seja, só é possível a regulamentação em lei após a concretização do fato social no âmbito coletivo. A tecnologia se desenvolve em uma velocidade espantosa, da qual o Direito não consegue acompanhar, trazendo inovações e, consequentemente, problemas, os quais devem ser amparados pela lei, como uma forma de tentativa de solução. Sendo assim, necessitamos de “normas que protejam o cidadão em face da automação e dos riscos do uso indevido das novas tecnologias” (JESUS; MILAGRE, 2016, p. 18).

O sistema jurídico brasileiro têm a lei como fonte principal e, em decorrência disso, o processo legislativo é bem mais lento do que os avanços tecnológicos e as

consequências advindas destes. Entretanto, se é possível o encaixe da conduta antissocial perpetrada no meio virtual a um crime já tipificado em lei vigente, o aplicador do Direito não pode optar pela omissão (JESUS; MILAGRE, 2016).

A verdade é que existem inúmeros problemas envolvendo a legislação e a rapidez da evolução tecnológica. Por exemplo, com o surgimento de crimes informáticos complexos e inéditos, que exigem uma resposta do meio jurídico, a "busca incessante pela normatização do novo pode resultar na promulgação de leis vagas e esparsas" (CÔRREA, 2000).

Os legisladores brasileiros têm o desafio de criar leis que não se tornem obsoletas com o constante desenvolvimento tecnológico e que sejam abrangentes, no sentido de não mencionar técnicas ou dispositivos informáticos específicos que possam se tornar ultrapassados e, assim, tornar a lei inutilizável em um curto espaço de tempo.

Jesus e Milagre (2016, p. 30) observam que para que se possa legislar sobre condutas informáticas

> [...] identifica-se, primeiramente um comportamento que possa ser concretizado por uma ou mais técnicas informáticas, que existam ou que venham a ser criadas. Comportamento este que mereça a tutela penal e, nesse sentido, se eleva tal comportamento ao *status* de crime, se realmente corresponder a uma atividade reprovável. Ao se legislar sobre crimes informáticos, não se começa pela análise de uma técnica, tampouco definindo tipos penais, mas analisando condutas incriminávéis que podem ser realizadas por diversas formas (técnicas) e que mereçam a consideração do Direito Penal. Do mesmo modo, uma técnica pode ser integrante de uma ou mais condutas penalmente relevantes. Um "cavalo de troia", por exemplo, pode servir a uma invasão, mas também para permitir o dano ou mesmo o comportamento inesperado de um sistema informático. Por outro lado, nem toda a técnica se enquadra em um comportamento incriminável. Este pode ser, *data vênia,* um dos principais erros de grande parte dos doutrinadores e legisladores sobre o tema: confundirem técnica com conduta. (Grifo original)

É importante, conforme explicado acima, que não se confunda técnica com conduta, pois, por muitas vezes, determinadas técnicas poderão ser utilizadas tanto para a concretização de condutas ilícitas como para procedimentos que não trazem malefício algum. Usaremos como exemplo a invasão de dispositivo informático.

Um criminoso cibernético pode usar técnicas específicas para invadir o computador de uma determinada pessoa, sem autorização, obter fotos íntimas e usa-las contra o usuário para chantagem ou divulgação nas redes sociais. Por outro lado, um técnico de informática necessita usar das mesmas técnicas para invadir um computador, com autorização, a fim de impedir a iminente perda de arquivos

importantes para o usuário. Em ambos os casos o agente estaria usando de uma determinada técnica para invadir um computador, no primeiro exemplo, podemos constatar a ilicitude do ato, pois é visivelmente danosa à vítima. No segundo exemplo, assim como no primeiro, o agente usa da referida técnica para invadir um computador, no entanto, possui autorização e está tentando impedir que o dono do computador sofra danos irreparáveis com o extravio de arquivos, não se caracterizando uma conduta lesiva.

No próximo capítulo, haverá uma análise mais profunda da legislação penal brasileira sobre os crimes cibernéticos, apontando os acertos e os equívocos do legislador na tipificação dos delitos informáticos, considerando os desafios supracitados na relação entre o Direito e as novas tecnologias.

Recentemente, no mês de maio de 2017, o mundo assistiu alarmado o ataque cibernético de escala global sem precedentes que afetou ao menos 150 países e atingiu mais de 300 mil computadores. O ataque foi idealizado por um grupo de *crackers* que exploraram de uma falha de segurança do Windows para infectar milhares de computadores, bloqueando o acesso dos usuários aos seus arquivos e solicitando o resgate em dinheiro, através das *bitcoins*, para recupera-los. Os criminosos virtuais exigiam o pagamento da quantia de, no mínimo, US$ 300,00, que deveria ser efetuado em *bitcoins*, uma moeda virtual criptografada difícil de rastrear e que não necessita da intermediação de bancos ou autoridades financeiras (2017, <http://brasil.elpais.com>).

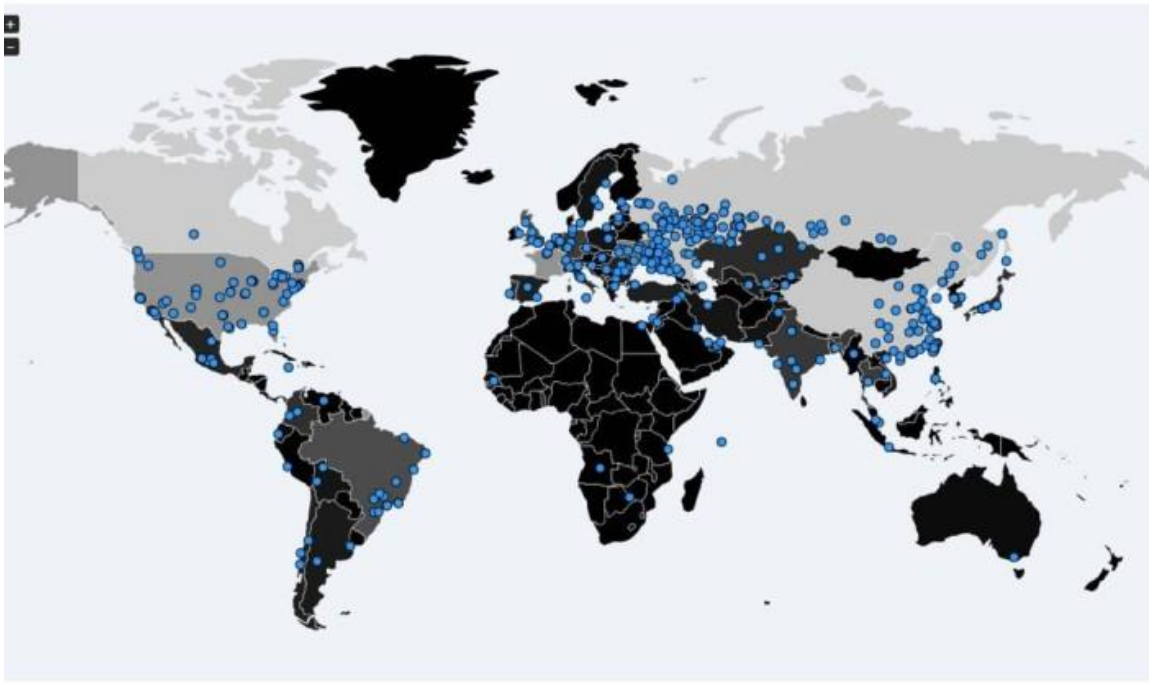
O ciberataque se disseminou, na maior parte dos casos, através de *e-mails* infectados pelo vírus *ransomware,* apelidado de *WannaCry*, um tipo de *malware* que sequestra os dados do disco rígido do computador através da criptografia. Ao clicar no link malicioso enviado por *e-mail*, aparentemente confiável, o computador da vítima é imediatamente infectado, assim como todos os que estão conectados em rede com ele, propagando o vírus rapidamente (D'URSO; D'URSO, 2017).

O ataque afetou o funcionamento de inúmeras empresas, organizações e instituições públicas pelo mundo, tais como hospitais britânicos, a empresa espanhola de telecomunicações Telefónica, a fabricante de automóveis Renault, a empresa de correios americana FedEx, entidades financeiras russas, entre outras. Para exemplificar a gravidade do crime, podemos observar que, somente no Reino Unido, cerca de 16 hospitais públicos foram alvos do ciberataque e enfrentaram dificuldades para acessar os prontuários dos pacientes, atrapalhando os serviços das ambulâncias e outros serviços de assistência médica e, por conseguinte,

colocando em risco inúmeras vidas (D'URSO; D'URSO, 2017).

Os efeitos do ataque cibernético em massa também atingiram o Brasil, provocando a interrupção no funcionamento do sistema de diversas empresas e órgãos públicos, inclusive, os obrigando a tirar sites do ar e desligar os seus computadores. O Instituto Nacional do Seguro Social teve os seus computadores afetados e foram obrigados a suspender os atendimentos em todas agências do país. Além do INSS, a Petrobras, os Tribunais de Justiça de determinados Estados e o Ministério Público de São Paulo são alguns exemplos de órgãos que tiveram que lidar com os transtornos advindos da propagação do vírus *ransomware* (2017, <http://g1.globo.com>).

Figura 1 – Mapa-Mundi, no qual os pontos azuis identificam quais os locais atingidos pelo ciberataque global.



Fonte: El País/Malware Tech (2017, <http://brasil.elpais.com>)

O ataque cibernético de escala global e suas consequências serviram de alerta para a sociedade sobre as vulnerabilidades a que a população está exposta na internet, reforçando a ideia de é necessário tomar medidas urgentes para fornecer uma maior segurança os seus usuários. Além disso, o combate aos crimes informáticos deve ser melhor debatido, tanto no âmbito da tipificação destes crimes quanto no desenvolvimento de métodos investigativos que permitam desvendar a identidade dos criminosos. Não se pode permitir que estes delinquentes tenham a liberdade para cometer crimes de grandes proporções, com danos irreparáveis, sem

que haja punição.

Outro aspecto preponderante é o fato de que a internet é um território sem fronteiras, o que possibilita que o infrator se encontre hospedado em um determinado país e, mesmo assim, esteja cometendo crimes simultaneamente em diversos outros países. Tais circunstâncias de territorialidade acabam dificultando a punição dos criminosos cibernéticos, visto que existem numerosos conflitos entre países tanto no âmbito político quanto no jurisdicional.

Os efeitos do ataque cibernético em massa reafirmam a necessidade de uma discussão aprofundada em relação aos crimes cibernéticos no Brasil, com o propósito de aperfeiçoar a legislação penal informática e os procedimentos de investigação, e, assim, diminuir a impunidade dos crimes cometidos no ambiente virtual.

3 CRIMES CIBERNÉTICOS

O crime cibernético é conceituado como

> [...] fato típico e antijurídico, cometido através da informática em geral, ou contra um sistema, dispositivo informático ou rede de computadores. Em verdade, pode-se afirmar que, no crime informático, a informática ou é o bem ofendido ou o meio para a ofensa a bens já protegidos pelo Direito Penal (JESUS; MILAGRE, 2016, p. 49).

Em outras palavras, pode-se afirmar que crimes cibernéticos são os ilícitos consumados por intermédio da internet, com o auxílio desta, ou até mesmo contra a tecnologia da informação em si, os quais trazem algum tipo de dano à vítima, seja uma vítima determinada ou mesmo à coletividade (FIORILLO; CONTE, 2016).

Ainda, é necessário destacar que existem inúmeras denominações acerca dos crimes relacionados às novas tecnologias: crimes de computador, *cybercrimes*, delitos informáticos, crimes virtuais, crimes eletrônicos, crimes informáticos, crimes cibernéticos, crimes digitais. Verifica-se que, apesar de serem nomeações distintas, no fundo acabam por significar a mesma coisa (JESUS; MILAGRE, 2016).

O ambiente cibernético é novo e se encontra em constante evolução, modificando-se rapidamente, por muitas vezes, da noite para o dia. Nesse contexto, observa-se que o espaço geográfico, bem como a presença física, não são mais essenciais para a prática dos delitos (MALAQUIAS, 2015).

Portanto, os crimes digitais são um fenômeno recente, inerente ao surgimento da sociedade da informação e às transformações tecnológicas. Com a rápida evolução tecnológica, tratar dos delitos perpetrados no meio virtual se tornou um desafio, tendo em vista que o Código Penal Brasileiro é da época do rádio e visivelmente omisso na tipificação dos crimes cibernéticos, situações nas quais a informática deveria ser protegida pelo Direito Penal (JESUS; MILAGRE, 2016).

Dentro desse contexto, essencial trazer à reflexão o Princípio da Legalidade no âmbito do Direito Penal, amparado constitucionalmente pelo artigo art. 5º, XXXIX da Constituição Federal, o qual preconiza que “não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal”.

Destarte, a reserva legal se caracteriza como uma limitação ao poder punitivo estatal e uma garantia constitucional fundamental do homem, assegurando que os indivíduos só poderão ser punidos se e quando praticarem condutas previamente definidas em lei como crimes. Conclui-se, portanto, que só haverá

crime nas hipóteses taxativamente previstas na legislação penal (CAPEZ, 2013).

Conforme afirma Malaquias (2015. p. 74), “diversas condutas dos criminosos cibernéticos ainda se constituem como atípicas, impedindo também a utilização da analogia em prejuízo do acusado (*in malam parte*), o que é inadmissível no Direito Penal”.

Posto isto, destaca-se que no Brasil

> [...] algumas condutas encontram respaldo na legislação vigente, notadamente, aquelas nas quais a internet tornou-se mais um modo executória do delito. Por outro lado, os meios tecnológicos também propiciaram o advento de novas práticas delitivas que necessitam de previsão legal para que adquiram tipicidade, sobretudo, quando estamos diante dos crimes informáticos ditos puros (FIORILLO; CONTE, 2016, p. 217).

Não obstante, verifica-se que o Código Penal de 1940 é eficiente em relação aos crimes comuns cometidos por meio da internet, pois tipifica inúmeros delitos já conhecidos pela sociedade que começaram a ser praticados com frequência no ambiente virtual, como exemplo os crimes de estelionato e pornografia infantil. Assim, nessa modalidade, tem-se os mesmos crimes já tipificados na legislação penal, porém, utilizando-se o meio virtual como meio para a perpetração.

Como salientam Jesus e Milagre (2016, p. 49), “o crime virtual pode ser um crime-meio, mas vem se desenvolvendo como crime-fim, o que demandou, aliás, a tipificação de alguns crimes informáticos próprios, com a edição das Leis n. 12.735/2012 e n. 12.737/2012”.

Posto isto, os crimes de estelionato e pornografia infantil, citados anteriormente, são considerados como um crime-meio, visto que podem ser cometidos tanto no ambiente virtual quanto fora dele, sendo este usado apenas como instrumento para a consumação do delito. Por outro lado, o crime de invasão de dispositivo informático, introduzido na norma penal brasileira pela Lei nº 12.1737/2012, é considerado crime-fim, uma vez que o bem jurídico protegido é a segurança dos dispositivos e dados informáticos (JESUS; MILAGRE, 2016).

Nas palavras de Malaquias (2015, p. 73)

> [...] a conduta no crime cibernético na maioria dos tipos penais emergentes é pluriofensiva, tendo em vista que, via de regra, ofende diversos bens jurídicos tutelados, como por exemplo, a “invasão de dispositivo informático” alheio com a finalidade de obter, destruir, adulterar bancos de dados ou informações e em consequência desse ato ilícito, posteriormente divulgar, vender, distribuir o produto obtido com a invasão (fotografias, vídeos, banco de dados etc.), causando prejuízos financeiros ou expondo a vida íntima e

> privada da vítima. Esse é o típico exemplo de crime formal que se exaure com a primeira conduta, independentemente das consequências e dos resultados posteriores que, via de regra, ferem diversos bens jurídicos tutelados pela lei penal. (Grifo original)

Dentre as inúmeras classificações doutrinárias utilizadas para caracterizar os delitos perpetrados no ambiente virtual, entende-se que a mais adequada seria aquela que apresenta uma distinção entre crimes cibernéticos em que as novas tecnologias são usadas como instrumento para a prática de velhos crimes, já há muito tempo tipificados pelo Direito Penal, e crimes cibernéticos em que a própria informática é o bem jurídico protegido (JESUS; MILAGRE, 2016).

Posto isto, ressalta-se que esta pesquisa utilizará a corrente doutrinária que estrutura a classificação dos delitos informáticos em crimes cibernéticos próprios/puros e crimes cibernéticos impróprios/impuros.

3.1 Crimes cibernéticos próprios

Os crimes cibernéticos próprios são aqueles em que “o bem jurídico ofendido é a tecnologia da informação em si” (JESUS; MIALGRE, 2016, p. 52). Ou seja, são os delitos que estão vinculados com a utilização das tecnologias de informação e comunicação para a consumação do delito, como, por exemplo, a conduta ilícita que tem por objetivo principal o sistema de computador, danificando o equipamento informático e seus componentes, inclusive dados e sistemas (FIORILLO; CONTE, 2016).

Existe um grande desafio em relação aos crimes informáticos próprios, haja vista que não possuem grande amparo na legislação brasileira, que se demostra lacunosa, não enquadrando criminalmente muitas práticas lesivas às vítimas, em razão do princípio da legalidade (FIORILLO; CONTE, 2016).

Assim sendo, torna-se impraticável punir uma conduta que, embora constitua essencialmente um ilícito, pois causa danos à vítima, não possui correspondência típica na legislação penal. Um exemplo desta dificuldade de enquadramento típico da conduta lesiva aos dados informáticos seria a disseminação de vírus através de programa de computador malicioso.

Desta maneira, com o advento das novas tecnologias e, consequentemente, o surgimento de novas práticas delitivas, verifica-se necessária a previsão legal de tais condutas, para que adquiram tipicidade, especialmente nos casos dos crimes

cibernéticos próprios (FIORILLO; CONTE, 2016).

Nesse contexto, no ano de 2012, foi promulgada a Lei nº 12.737, apelidada de “Lei Carolina Dieckmann”, a qual trouxe a tipificação de delitos informáticos ao Código Penal Brasileiro, auxiliando a diminuir a omissão da legislação penal brasileira em relação aos crimes cibernéticos (MALAQUIAS, 2015). No entanto, tal legislação ainda é considerada tímida diante da gama de condutas que diariamente são perpetradas por meio informático e escapam à tipificação penal.

Cabe assinalar, ainda, que os novos tipos penais apresentados pela Lei nº 12.737/2012 “são crimes afetos, via de regra, à categoria de crimes informáticos próprios, onde o bem jurídico protegido é a segurança dos dispositivos e dados informáticos” (JESUS; MILAGRE, 2016, p. 53).

Na sociedade contemporânea, está cada vez mais raro encontrar pessoas que não interajam com pelo menos um dispositivo informático. Estima-se que, até o fim do ano de 2017, o Brasil terá um smartphone por habitante, dados que ilustram o crescente contato da sociedade brasileira com as novas tecnologias de comunicação e a necessidade de tipificação dos delitos cometidos no meio informático (2017, <http://link.estadao.com.br>).

Portanto, para melhor elucidar o tema, passa-se à análise mais aprofundada dos principais tipos penais introduzidos pela Lei Carolina Dieckmann no ordenamento jurídico brasileiro.

3.1.1 Invasão de dispositivo informático

A Lei nº 12.737/2012 introduziu no Código Penal de 1940 o artigo 154-A, que tipifica o crime de invasão de dispositivo informático, trazendo punição para aqueles que invadirem dispositivo informático através de violação de mecanismos de segurança, com o intuito de destruir, alterar, adulterar e obter dados e informações sem a prévia autorização, expressa ou tácita, do titular do equipamento ou instalar vulnerabilidades para obter vantagem ilícita (MALAQUIAS, 2015).

Ante a ausência de definições específicas sobre os termos trazidos pela referida lei, cabe trazer à baila as palavras de Jesus e Milagre (2016, p. 86):

> Não temos um glossário na Lei n. 12.737/2012, o que pode gerar interpretações distintas para o termo “dispositivo informatizado”. Invadir é devassar, ato ou ação de acessar indevidamente, mas à força, irrupção. Entrar em certo lugar e ocupa-lo pela força ou tomar, conquistar, na linguagem técnica, *ownar* (tomar a propriedade) ou realizar um *takeover*. Na

> sociedade da informação, dispositivo informático é todo o dispositivo capaz de tratar informação, diga-se, armazenar ou processar dados (cálculo, alteração, inclusão ou exclusão). (Grifo original)

Isto posto, percebe-se que o ato de invasão deve ser doloso, uma vez que necessita da vontade do agente em obter, adulterar ou destruir dados ou informações, sem autorização prévia, praticando conduta ilícita conscientemente e no uso de seu livre arbítrio, com a intenção de obter vantagem ilícita. Da mesma forma, se verificada a ausência de dolo do agente, a conduta será atípica. Deve-se, em todos os casos, considerar qual a finalidade do agente invasor (MALAQUIAS, 2015).

Nesse sentido, Malaquias (2015, p. 94) afirma que

> [...] o legislador pátrio deixou expressamente determinada a condição de violação indevida a fim de criar respectiva exceção à regra penal e proteger atos decorrentes do cumprimento de ordens e perícias judiciais ou também originados em manutenção do equipamento a serem executadas por técnicos e especialistas autorizados pelo proprietário, caracterizando acessos ou violações excepcionalmente permitidas.

Observa-se que o legislador penal estabeleceu como condição para a prática do delito, que o dispositivo informático invadido esteja protegido por mecanismo de segurança, sendo que a ausência total deste caracteriza a atipicidade do fato, em razão da impropriedade do objeto. Deste modo, considera-se mecanismo de segurança a barreira entre o invasor e os dados e informações guardados no dispositivo (JESUS; MILAGRE, 2016).

> A locução “mecanismo de segurança” deve ser interpretada como perfil mínimo que um aparelho utiliza em seu funcionamento, tendo em vista que a grande maioria dos usuários não instala sofisticados aplicativos de segurança de rede e nem implantam *firewall* complexos para o uso doméstico e também em pequenas empresas (MALAQUIAS, 2015, p. 93). (Grifo original)

No delito em tela, promove-se a proteção à liberdade individual, o direito à intimidade e a segurança da informação, com o objetivo de proteger os dados e informações pertencentes à pessoa proprietária do dispositivo informático (JESUS; MILAGRE, 2016).

A pena prevista na norma penal é de 3 meses a 1 ano de detenção, cumulada com pena de multa, visto que se trata de conduta de menor potencial ofensivo, na qual a pena deve servir de caráter socioeducativo, bem como forma de

punição imposta pelo Estado ao agente que pratica o crime cibernético. Ainda, o parágrafo segundo do artigo 154-A prevê hipótese de aumento pena de um sexto a um terço se da invasão resulta prejuízo econômico (MALAQUIAS, 2015).

Da mesma forma, o parágrafo quinto traz o aumento de pena de um terço à metade se o delito for cometido contra o Presidente da República, Governadores, Prefeitos, Presidente do Supremo Tribunal Federal, entre outros agentes públicos do alto escalão. Observa-se que o referido aumento de pena tem o objetivo de tornar mais grave o delito cometido contra tais figuras, em razão da importância dos cargos que ocupam, os quais trazem inúmeras informações e dados sigilosos que poderão comprometer a segurança do Estado.

Cabe, ainda, constatar que

> [...] a maioria das condenações nos crimes cibernéticos margearão a impunidade, até porque ainda poderá o magistrado optar pela pena alternativa que apenas restringe direitos, conforme preceitua cumulativamente o art. 44, do CP, e as diversas possibilidades de enquadramento do agente infrator (MALAQUIAS, 2015, p. 95).

A consumação do crime de invasão de dispositivo informático ocorre com a constatação da invasão, que deverá ser comprovada por prova pericial, na qual serão avaliados os artefatos e evidências como data e hora de início e fim da conexão. Deste modo, conforme afirmam Jesus e Milagre (2016, p. 97), “basta a invasão com intenção para que a conduta do agente faça subsunção perfeita ao tipo penal”.

Logo, trata-se de crime formal, no qual se exaure com a mera conduta de invadir dispositivo informático, não dependendo das consequências e resultados advindos da invasão. Temos como exemplo a situação em que o criminoso está planejando a invasão em um *smartphone* para obter fotos íntimas de determinada pessoa e, posteriormente, exigir uma certa quantia em dinheiro para não as divulgar. Se o agente invadir o *smartphone*, porém, por circunstâncias alheias a sua vontade, não conseguir obter as fotos pretendidas, o crime será consumado mesmo sem a obtenção, adulteração ou destruição dos arquivos (MALAQUIAS, 2015).

Em casos concretos, normalmente, o infrator invade com a finalidade de cometer outros crimes, tais como o estelionato, o dano, a difamação, a extorsão, entre outros. Nessas situações, sempre que o antefato (invasão) for menor que o pós-fato, o autor deverá ser punido apenas pelo crime mais grave.

Importante destacar que

> [...] não poderá haver concurso do delito do art. 154-A com o crime de dano (art. 163), nem com o crime de divulgação de segredo (art. 153) e com a violação de segredo profissional (art. 154), podendo se cogitar em concurso envolvendo delitos de propriedade imaterial, nos termos art. 195 da Lei n. 9.279/96, bem como envolvendo delitos ofensivos à honra, como difamação, injúria e calúnia (JESUS; MILAGRE, 2016, p. 105).

A norma penal trouxe, ainda, a forma qualificada do crime de invasão de dispositivo informático, prevista no artigo 154-A, §3º, do Código Penal, que impõe pena de reclusão de 6 meses a 2 anos e multa, se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas ou o controle remoto não autorizado do dispositivo invadido.

A ação penal será pública e condicionada à representação, sendo necessária a autorização da vítima para que haja a propositura da ação penal pelo Ministério Público. Entretanto, no caso de crime cibernético de invasão de dispositivo informático cometido contra a Administração Pública, indireta e direta, a ação é incondicionada, nos termos do artigo 154-B do Código Penal (JESUS; MILAGRE, 2016).

Por fim, considerando a pena inferior a 2 anos, o delito de invasão de dispositivo móvel será processado em face do Juizado Especial Criminal. Não obstante, considerando que os delitos desta natureza exigem comprovação probatória de alta complexidade, a competência poderá ser deslocada para a Justiça Comum (JESUS; MILAGRE, 2016).

3.1.2 Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública

Um dos principais crimes próprios perpetrados no âmbito cibernético é a indisponibilização de serviços, isto é, ataques realizados com o objetivo de interromper serviço de tecnologia da informação, sendo que a principal técnica utilizada para concretização desses ataques é a chamada DoS (*Denial of Service*) ou ataque de negação de serviços (JESUS; MILAGRE, 2016).

Um ataque de negação de serviço caracteriza-se por uma tentativa de "tornar recursos de um sistema indisponíveis para quem os utiliza, sendo os alvos mais comuns os servidores *Web*" (JESUS; MILAGRE, 2016, p. 109). Isto posto, cabe destacar que não se trata de invasão de dispositivo informático, mas sim de

invalidação de serviços pela sobrecarga.

Além da tipificação do crime de invasão de dispositivo informático, a Lei nº 12.737, de 30 de novembro de 2012, promoveu uma complementação ao artigo 266 do Código Penal, que anteriormente não era expresso ao tratar da possibilidade de sistemas informáticos serem objeto do ataque envolvendo a interrupção (JESUS; MILAGRE, 2016). Dessa forma, o dispositivo passou a vigorar com a seguinte redação:

> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
> Pena - detenção, de um a três anos, e multa.
> § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
> § 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.

Observa-se que a reforma do delito em comento teve por finalidade promover a proteção de serviço telemático ou de informação de utilidade pública, ou seja, “aqueles que objetivam facilitar a vida do indivíduo na sociedade, colocando a disposição deste, utilidades que lhe proporcionarão mais conforto e bem-estar” (JESUS; MILAGRE, 2016, p. 110).

Dessa forma, é fundamental que o ordenamento jurídico brasileiro estabeleça uma sanção para o indivíduo que cause tumulto nas comunidades através da interrupção de serviços públicos essências ou que tragam facilidades à vida em sociedade. Inclusive, no caso de tragédias acentuadas, que causam calamidade pública, a lei prevê a aplicação em dobro da pena cominada (MALAQUIAS, 2015).

O delito do artigo 266 do Código Penal é considerado como crime instantâneo, já que uma vez interrompido o serviço, a conduta não pode mais ser cessada pelo agente, não importando se essa interrupção acontecer por apenas alguns segundos ou durante inúmeras horas. Por conseguinte, a consumação do delito acontece com a efetiva invasão ou perturbação, que deverá ser corroborada por laudo pericial, sendo, assim, considerado crime material, pois exige para a consumação o resultado previsto no tipo penal (JESUS; MILAGRE, 2016).

Em análise aos casos concretos, deve-se observar, também, a progressão criminosa

> [...] em que o agente será punido pelo delito mais grave em casos que, por exemplo, o agente precisou invadir os servidores antes de “interromper” as

> atividades, ou mesmo no caso em que, após a interrupção, ocorre o dano ou mesmo o acesso indevido a dados. Lembrando que os fatos deverão se dar, para a progressão criminosa, sempre no mesmo contexto, o que poderá restar provado da prova técnica. Pode ser de acordo com o caso concreto, crime exaurido, na medida em que, após praticado o delito do § 1º do art. 266 do Código Penal, pode o agente levar a consequências mais lesivas. O juiz deverá considerar tais circunstâncias na aplicação da pena (JESUS; MILAGRE, 2016, p. 113). (Grifo original)

O crime de Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático é de ação penal pública incondicionada, portanto, independe de representação dos ofendidos e é de competência do juízo comum (JESUS; MILAGRE, 2016).

3.2 Crimes cibernéticos impróprios

Os crimes cibernéticos impróprios são aqueles em que o computador e a internet são usados como instrumentos para a prática do delito, isto é, caracterizam-se pela agressão a bens jurídicos já protegidos pelo Código Penal Brasileiro. Tais crimes podem ser cometidos tanto da forma tradicional quanto por intermédio de computadores (MALAQUIAS, 2015). Portanto, “se é possível o encaixe da conduta antissocial a um dispositivo legal em vigor, não deve o aplicador do Direito quedar-se em omissão” (JESUS; MILAGRE, 2016, p. 25).

A rede mundial de computadores se constitui apenas como um meio de execução de delitos conhecidos e que já encontram respaldo na legislação penal brasileira, dentre os quais destacam-se o estelionato (art. 171 do CP), a ameaça (art. 147 do CP), os crimes contra a honra (arts. 138-140 do CP) e a pornografia infantil (FIORILLO; CONTE, 2016).

É inegável que as novas tecnologias e, especialmente, a internet trouxeram inúmeros avanços e facilidades para a vida em sociedade, ampliando o acesso à informação e facilitando a comunicação entre os indivíduos. Apesar disso, fato é que o uso dos meios eletrônicos e o acesso à internet acabaram por facilitar, também, a perpetração de crimes comuns, considerando que os criminosos cibernéticos encontraram novas formas de praticar crimes já conhecidos, aperfeiçoando, cada vez mais, suas técnicas.

Constata-se, ainda, que embora a técnica pela qual o agente concretiza a ação criminosa seja diferente no meio virtual, não há a necessidade de conhecimentos técnicos específicos para praticar tais crimes. Qualquer usuário da

rede mundial de computadores pode cometer o crime de ameaça ou estelionato, por exemplo, mesmo sem dominar técnicas aprofundadas na área da informática (SILVA, 2015).

De acordo com Jesus e Milagre (2016, p. 50):

> Fato é que a maior parte dos crimes eletrônicos está relacionada a delitos em que o meio para a realização da conduta é virtual, mas o crime em si não. A exemplo, tem-se como crimes mais comuns praticados na rede o estelionato e a pornografia infantil e os ataques mais comuns os praticados por meio de vírus de computador ou *malware,* seguido de invasão de perfis nas redes sociais e por ataques de *phising*.

Desse modo, para melhor elucidar tema, torna-se necessário aprofundar o estudo sobre os crimes cibernéticos impróprios mais praticados no ambiente virtual, a fim de compreender os motivos pelos quais são tão reincidentes.

3.2.1 Crime de pornografia infantil

A pornografia infantil é um grave problema de abrangência mundial e está em constante crescimento com o auxílio da internet, já que as informações e imagens são compartilhadas na *web* com milhares de pessoas em poucos minutos. O uso ilimitado da internet nas últimas décadas possibilitou a ampliação da divulgação de imagens e vídeos que reproduzem imagens pornográficas envolvendo crianças e adolescentes.

Sobre o assunto, Malaquias (2015, p. 82) afirma:

> A pornografia infantil transformou-se em verdadeira calamidade social. O índice de páginas geradas e ampliadas na Internet é alarmante e os delinquentes virtuais se sentem protegidos pelo anonimato propiciado pela *web*, favorecendo a produção desenfreada de *sites* que exploram a nudez de crianças e adolescentes em cenas de sexo explícito, inclusive possibilitando o assédio em salas de conversação (*chat*) ou grupos de relacionamentos.

Nesse contexto, impende lembrar que não existe crime de pedofilia, como os meios de comunicação em massa, especialmente a mídia televisiva, insistem em divulgar erroneamente. Trata-se de utilização incorreta de termos técnicos. A pedofilia se caracteriza como um transtorno sexual ou parafilia, isto é, um transtorno psíquico que “leva um indivíduo adulto a se sentir sexualmente atraído por crianças ou prática efetiva de atos sexuais com crianças” (FIORILLO; CONTE, 2016, p. 235).

Por sua vez, a pornografia infantil se constitui por

> [...] qualquer meio de retratar ou promover o abuso de uma criança, incluindo meios impressos ou de áudio, centrados nos atos sexuais ou nos órgãos genitais das crianças. Cumpre esclarecer que o crime de pornografia infanto-juvenil nem sempre é praticado por pedófilos, pois há quem pratique o delito de consumo, em suas diversas formas, como trocar, adquirir, possuir, pelo fato de ter essa preferência sexual, mas há quem pratique o crime por curiosidade, oportunidade, bem como no objetivo de obter ganhos financeiros, havendo organizações criminosas dedicadas à produção e vende de material pornográfico envolvendo crianças e adolescentes (SILVA, 2017, p. 87).

Diante desta triste realidade, é imprescindível que o ordenamento jurídico brasileiro seja rigoroso ao criminalizar e punir qualquer tipo de ato relacionado à divulgação, aquisição, produção ou posse de material com conteúdo de pornografia infantil, tendo em vista que esta e o abuso sexual de menor tem crescido assustadoramente e, por consequência, ganhado grande destaque no noticiário do Brasil e do mundo (FIORILLO; CONTE, 2016).

Nesse contexto, com o intuito de ampliar e promover o combate à produção, venda e distribuição de pornografia infantil, inclusive criminalizando inúmeras condutas relacionadas à aquisição e posse do referido material, ocorreu a promulgação da Lei 11.829 de 25 de novembro de 2008, que alterou a Lei 8.069/1990 (Estatuto da Criança e do Adolescente) e tipificou inúmeras condutas criminosas associadas à pedofilia, que utilizam como meio de divulgação e consumação do crime a rede mundial de computadores, assim como as redes locais e os equipamentos de informática dos indivíduos (MALAQUIAS, 2015).

Portanto, “a integridade física, a liberdade sexual, a dignidade e a honra da criança ou do adolescente são os objetos jurídicos a serem tutelados pelos tipos penais” (MALQUIAS, 2015, p. 82). Os dispositivos incriminadores das condutas relacionadas à pornografia infantil visam proteger a formação moral da criança e do adolescente, a fim de proporcionar a convivência saudável em sociedade e garantir o seu desenvolvimento.

O artigo 240 do Estatuto da Criança e do adolescente prevê como fato criminoso as condutas de “produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente”. Trata-se, assim, de crime de ação múltipla, visto que apresenta diferentes formas de execução, considerando-se consumado o delito com a concretização de qualquer das condutas descritas no tipo penal (FIORILLO; CONTE, 2016).

Constata-se que o §2º do referido dispositivo, ampliado pela Lei nº 11.829/2008, indica situações em que ocorrerá o aumento de pena, as quais se destaca àquelas pertinentes às relações em que o agente exerça autoridade sobre a vítima ou possua relações de parentesco consanguíneo ou afim até o terceiro grau (FIORILLO; CONTE, 2016).

Outro dispositivo da Lei nº 8.069, de 13 de julho de 1990, que merece destaque é o artigo 241-A, que prevê:

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
> § 1º Nas mesmas penas incorre quem:
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
> § 2º As condutas tipificadas nos incisos I e II do § 1º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo.

O delito traz inúmeros verbos nucleares, tratando-se, mais uma vez, de crime de ação múltipla, que engloba diversas práticas que são perpetradas por meio da internet. Em uma análise do tipo penal acima descrito, Silva (2017, p. 96) afirma:

> A primeira hipótese está expressa pelo verbo *oferecer*, que tem o sentido de apresentar ou propor para que seja aceito. *Trocar* é permutar uma coisa por outra. *Disponibilizar,* ainda que guarde semelhança de significado com oferecer, para os fins do artigo sob exame, amolda-se mais especificamente a casos de hospedagem e compartilhamento de arquivos, como em serviços P2P (*peer-to-peer*), como, *v.g*, o E-Mule, em que o agente disponibiliza arquivos com material pornográfico para que terceiros façam cópias ou *download*. A ação de *transmitir* refere-se à remessa de material com conteúdo pornográfico entre usuários de *Internet* ponto a ponto, como ocorre com o envio de *e-mails* e a programas de mensagens como *Whatsapp, Telegram, Skype* ou *msn*. *Distribuir* é uma conduta que se amolda ao envio de *e-mails* na forma de *spams*, em que o conteúdo pornográfico é levado a uma multiplicidade de destinatários. *Publicar* é condizente com a hipótese em que a prática delitiva se procede de forma direta, com a exposição da cena incriminada, mediante a utilização de redes sociais (*Orkut, Facebook*), blogs (*blogspot, fotolog, tumblr*), *webpages*. Por fim, *divulgar*, por qualquer meio, é propalar, tornar conhecido, mas não propiciar acesso ao material pornográfico de forma direta – diferentemente do que ocorre com a conduta publicar – podendo funcionar, a nosso ver, como uma espécie de recurso de tipificação residual, com a utilização, *v.g*, de links que direcionem o usuário para *webpages, twitter,* redes sociais. (Grifo original)

Observa-se que o §2º traz uma condição objetiva de punibilidade,

relacionada às condutas previstas nos incisos I e II do §1º, na qual o responsável legal pela prestação do serviço, devidamente comunicado, deixa de desabilitar o acesso ao conteúdo ilícito de pornografia infantil, e, assim, constitui pressuposto material de aplicação da pena (SILVA, 2017).

Conclui-se, dessa forma, que a inclusão do art. 241-A pela Lei 11.829/2008 ampliou consideravelmente a abrangência do crime de pornografia infantil, punindo de forma ampla inúmeras condutas que estejam, ainda que minimamente, relacionadas à propagação de conteúdo ilícito de cenas de sexo explícito ou pornográfico envolvendo crianças e adolescentes.

O artigo 241-B do Estatuto da Criança e do Adolescente possui a seguinte redação:

> Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
> § 1º A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo.
> § 2º Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por:
> I – agente público no exercício de suas funções;
> II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo;
> III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário.
> § 3º As pessoas referidas no § 2º deste artigo deverão manter sob sigilo o material ilícito referido.

O tipo penal acima descrito menciona três verbos, quais sejam, adquirir, possuir e armazenar, sendo que o primeiro se trata de crime instantâneo, no qual a consumação acontece em determinado momento, sem continuidade no tempo. Por outro lado, nas modalidades possuir e armazenar, trata-se de crime permanente, em que a consumação se prolonga no tempo (SILVA, 2017).

O *quantum* da pena é influenciado pela quantidade do material pornográfico encontrado, já que o §1º nos aponta hipótese de redução da pena de um a dois terços se a quantidade do material for pequena. Não obstante, essa previsão demonstra-se criticável, considerando que, mesmo que a quantidade do material de pornografia apreendido seja pequena, ainda sim haverá uma lesão significativa à dignidade da criança e do adolescente, ou seja, ao bem jurídico que se quer tutelar (FIORILLO; CONTE, 2016). Ou seja, não é a quantidade de material que irá definir a

gravidade do crime, mas sim o conteúdo do material. Ademais, o que seria considerado “pequena quantidade” de material pornográfico não está definido na lei.

Por fim, o §2º prevê causa de excludente de ilicitude o fato de a posse ou armazenamento ter por objetivo a comunicação às autoridades competentes da ocorrência das condutas descritas nos artigos 240, 241, 241-A e 241-C, quando a comunicação ocorrer pelas pessoas elencadas nos incisos I a II do §2º. Tal previsão demonstra a preocupação do legislador com eficácia da persecução criminal, a fim de garantir a investigação e punição das condutas descritas nos tipos penais em análise (FIORILLO; CONTE, 2016).

O artigo 241-C da Lei no 8.069/1990 incrimina o indivíduo que simular a participação de criança ou adolescente em “cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual”.

O tipo penal descrito no artigo 241-C do Estatuto da Criança e do Adolescente está intimamente ligado ao mundo cibernético, visto que é bastante comum encontrar na internet *sites* que permitem o download de programas como o *Photoshop, Avid, After Effects* e *Adobe Premiere*, que permitem a manipulação e edição de vídeos e imagens, facilitando adulterações e montagens. Dessa forma, por muitas vezes, os criminosos cibernéticos se utilizam de imagens de crianças para fazer montagens utilizando-as em cenas de pornografia infantil para divulgação na *web* (FIORILLO; CONTE, 2016).

Cabe destacar que a simulação deve envolver crianças ou adolescentes reais, não com um simulacro de pessoa que não seja, efetivamente, alguém real. Quando não se tratar de criança, e sim de boneco ou algum tipo de simulação, o fato não se enquadra à hipótese prevista no artigo 241-C (SILVA, 2017).

Já o artigo 241-D do Estatuto da Criança e do Adolescente, por sua vez, prevê:

> Art. 241-D. Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso:
> Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.
> Parágrafo único. Nas mesmas penas incorre quem:
> I – facilita ou induz o acesso à criança de material contendo cena de sexo explícito ou pornográfica com o fim de com ela praticar ato libidinoso;
> II – pratica as condutas descritas no caput deste artigo com o fim de induzir criança a se exibir de forma pornográfica ou sexualmente explícita.

O diploma legal pretende coibir o “aliciamento, o assédio, o constrangimento ou qualquer forma de sedução do menor que, pode ocorrer de modo dissimulado e

sub-reptício em salas de conversação digital (*chat*)" (MALAQUIAS, 2015, p. 86).

A instigação e o aliciamento de criança para prática de atos libidinosos, infelizmente, têm se configurado como uma prática comum na internet. As condutas são praticadas através de salas de bate-papo *online*, *sites* de relacionamento, jogos interativos e simuladores de vida, como, por exemplo, o *Second Life.* Levando em consideração que as crianças e os adolescentes passam inúmeras horas dos seus dias em ambientes virtuais como os citados acima, os pedófilos se aproveitam da facilidade de comunicação que o meio virtual lhes proporciona para realizar as mais diferentes formas de assédio (FIORILLO; CONTE, 2016).

Trata-se de crime formal, pois não depende que a prática do ato libidinoso se concretize para que ocorra a consumação do delito, basta que o criminoso tenha a finalidade de aliciar, assediar, instigação ou constranger a criança ou o adolescente para a prática de ato libidinoso. Entretanto, caso aconteça, de fato, o estupro, o agente deverá responder em concurso pelo dano praticado (SILVA, 2017).

Por fim, a Lei nº 11.829/2008, para facilitar a interpretação dos tipos penais introduzidos ao Estatuto da Criança e do Adolescente, trouxe a definição de "cena de sexo explícito ou pornografia":

> Art. 241-E. Para efeito dos crimes previstos nesta Lei, a expressão "cena de sexo explícito ou pornográfica" compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais.

Apesar do uso da internet ter ampliado a divulgação de conteúdos de sexo explícito envolvendo crianças e adolescentes, por outro lado, ela também serve de instrumento para o combate à pedofilia e à pornografia infantil. O uso da *web* permitiu a criação de uma central unificada de denúncias contra a pedofilia praticada via rede mundial de computadores.

> Resultante de um acordo firmado entre a Secretaria Especial de Direitos Humanos, a Polícia Federal e a ONG SaferNet, a central de informações permite que a Polícia Federal tenha acesso imediato ao banco de dados para apurar as informações sobre os crimes, abreviando o início das investigações e a remoção de páginas impróprias da Internet. A central serve também para alimentar a base de dados do governo federal, permitindo identificar onde há mais delitos, se as vítimas são crianças brasileiras e, assim, orientar a elaboração das políticas públicas de combate à pedofilia (FIORILLO; CONTE, 2016).

Diante da análise dos tipos penais acima expostos, verifica-se que a legislação penal brasileira atende de forma satisfatória o combate à pornografia infantil, uma vez que tipifica inúmeras condutas relacionadas a esse tema, punindo desde as ações mais simples até as mais complexas.

Entretanto, considerando que o crime de pornografia infantil é um dos delitos cibernéticos mais comuns no Brasil, é essencial que o combate a esse tipo de crime se torne cada vez mais eficiente e rigoroso, pois o abuso infantil causa danos morais e psicológicos irreparáveis, que acabam acompanhando a criança e ao adolescente violentado pelo resto de suas vidas.

Além disso, não basta apenas criar tipos penais prevendo punições para o crime de pornografia infantil, para o seu efetivo combate é fundamental que a investigação criminal seja eficaz ao identificar os autores e comprovar a materialidade do delito, pois, somente assim, será possível, de fato, punir os delinquentes cibernéticos que praticam esse tipo de infração desumana.

Dessa forma, o Estado tem o dever de proteger a dignidade das crianças e adolescentes brasileiros, garantindo o seu desenvolvimento em uma sociedade segura e saudável, que pune com rigor qualquer tipo de abuso, violência, exploração sexual e divulgação de cenas pornográficas com a participação de crianças e adolescentes.

3.2.2 Crimes contra a honra e crime de racismo

O Código Penal de 1940 trata dos crimes contra a honra, identificados como aqueles delitos que ofendem bem imateriais da pessoa humana, a sua honra pessoal. São eles: a calúnia, a difamação e a injúria, respectivamente previstos nos artigos 138, 139 e 140 do Código Penal. Logo, objetiva-se a defesa de um bem imaterial, relacionado à personalidade humana (CAPEZ, 2012).

Toda pessoa tem o direito de não ser ultrajada em sua honra e dignidade, tal proteção é garantida pela Constituição Federal de 1988, que em seu artigo 5º, X, prevê que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”.

Inegável o uso da internet diariamente na vida de grande parte da população brasileira, as formas de comunicação no ambiente digital evoluem e se ampliam em uma velocidade inacreditável. Nesse contexto, as redes sociais adquiriram destaque,

pois surgiram da necessidade da interação social entre as pessoas no ambiente digital. Apenas o *Facebook*, uma dentre as inúmeras redes sociais da internet, possui cerca de 1,6 bilhão de usuários em todo o mundo (MURARD, 2014).

Portanto, com evolução da comunicação após o surgimento da internet, os indivíduos passaram a experimentar uma liberdade nunca antes vista para poder expor sua imagem, privacidade e pensamentos na *web.* Assim sendo, verifica-se que os usuários da rede mundial de computadores, seja por publicações em redes sociais, seja por comentários em sites ou postagens em blogs, acabam exagerando ao usar essa liberdade, o que acaba tornando cada vez mais comum a prática de crimes contra a honra no ambiente digital. Ofender e ser ofendido se tornou uma rotina na vida de alguns usuários da rede (MASI, 2016).

O crime de calúnia é tipificado no artigo 138 do Código Penal, cuja redação é a seguinte:

> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime:
> Pena - detenção, de seis meses a dois anos, e multa.
> § 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.
> § 2º - É punível a calúnia contra os mortos.

No caso do delito acima descrito, o agente deve atribuir a alguém fato qualificado como crime, sabendo ser essa imputação falsa, apontando circunstâncias capazes de identificar o fato criminoso. Assim, a prática do crime de calúnia, no meio virtual, verifica-se, por exemplo, quando o usuário de uma rede social faz uma postagem afirmando que determinada pessoa furtou objetos de sua casa, sabendo que tal furto jamais aconteceu. Acontece que o usuário que pratica tal delito, em diversas ocasiões, sabe que a postagem pode ser visualizada por milhares de pessoas em um curto período de tempo e usa desse método rápido de propagação como forma de atingir a honra de outrem.

Destaca-se, ainda, que a “falsidade da imputação é sempre presumida e a ofensa à honra só deixa de existir se ficar provada a veracidade do crime atribuído ao ofendido” (CAPEZ, 2012, p. 293). Trata-se da exceção da verdade, que se constitui como uma forma que o sujeito possui de provar que o que afirmou é verdade, pois quando o fato for verdadeiro, não há que se falar em crime de calúnia (CAPEZ, 2012).

Cita-se como exemplo o caso do *youtuber* Nando Moura que foi condenado por ter acusado falsamente Tico Santa Cruz, vocalista da banda Detonautas, de ter

recebido dinheiro da Lei Rouanet para financiar projetos de sua banda. Em um de seus vídeos publicados no *youtube,* Moura afirmou que Tico Santa Cruz recebia dinheiro da Lei Rouanet para defender opiniões políticas em suas redes sociais (2016, <https://penseegratis.org>).

Já o crime de difamação tem como objetivo proteger a reputação, a boa fama do indivíduo no meio social. A difamação difere-se da calúnia, uma vez que naquela o fato imputado não é criminoso e a falsidade não é exigida pelo tipo penal, logo, o fato poderá ser verdadeiro ou não (CAPEZ, 2012). O delito encontra-se previsto no artigo 139 do Código Penal de 1940:

> Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
> Pena - detenção, de três meses a um ano, e multa.
> Parágrafo único - A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções.

O crime configura-se quando o agente atribui a alguém fato desonroso, ou seja, fato ofensivo à sua reputação, que deve, necessariamente, chegar ao conhecimento de terceiros, uma vez que é a reputação que o imputado ostenta na comunidade que deve ser lesada. Consequentemente, o delito se consuma no exato momento em que terceiro, que não o ofendido, toma ciência da afirmação que ofende a imagem do imputado (MURARD, 2014).

A internet é um espaço que reúne todos os tipos credos e pensamentos e, em razão de sua amplitude, acaba sendo considerada como um ambiente seguro para a propagação de qualquer tipo de comentário. Logo, o crime de difamação ocorre em peso no ambiente virtual, como, por exemplo, no caso em que o agente repassa para inúmeras pessoas, através do aplicativo de celular *Whataspp*, mensagens com o intuito de degradar a reputação de determinada pessoa, atribuindo a esta fato prejudicial à sua imagem.

Por outro lado, a injúria é a ofensa à dignidade ou decoro de outrem e está prevista no artigo 140 do Código Penal:

> Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:
> Pena - detenção, de um a seis meses, ou multa.
> § 1º - O juiz pode deixar de aplicar a pena:
> I - quando o ofendido, de forma reprovável, provocou diretamente a injúria;
> II - no caso de retorsão imediata, que consista em outra injúria.
> § 2º - Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se considerem aviltantes:
> Pena - detenção, de três meses a um ano, e multa, além da pena correspondente à violência.

> § 3º Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência:
> Pena - reclusão de um a três anos e multa.

Diferentemente dos crimes de calúnia e difamação, que tutelam a honra objetiva, o bem protegido pela normal penal acima descrita é a honra subjetiva, que se constitui “pelo sentimento próprio de cada pessoa acerca de seus atributos morais (chamados de honra-dignidade), intelectuais e físicos (chamados de honra-decoro)” (CAPEZ, 2012, p. 306). A consumação do delito acontece no momento em que a vítima toma conhecimento do teor da ofensa, não necessitando que esta seja proferida na presença do ofendido, bastando que chegue ao seu conhecimento, por intermédio de terceiro, através da internet ou qualquer outro meio (CAPEZ, 2012).

Observa-se que o §1º do artigo 140 prevê duas hipóteses de perdão judicial, existe a configuração do crime de injúria, porém, o juiz poderá deixar de aplicar a pena. Na primeira hipótese, a vítima de maneira reprovável provoca injustamente a injúria, dando causa à ofensa sofrida. A segunda hipótese, por sua vez, trata da retorsão imediata, que se caracteriza pela injúria como resposta à injúria proferida pela vítima. O retruque deve acontecer no mesmo instante, sem intervalo de tempo, caso contrário, não será possível aplicar o perdão judicial. Portanto, “aquele que é injuriado em primeiro lugar pode ser isentado de pena desde que pratique o crime imediatamente após ser ofendido” (MURARD, 2014, <anabmurard.jusbrasil.com.br>).

Destaca-se que a ação penal nos crimes contra a honra (calúnia, difamação e injúria) é de iniciativa privada, na qual o Estado transfere a legitimidade para a propositura da ação penal para a vítima ou a seu representante legal, conforme dispõe o artigo 145 do Código Penal. A vítima possui a responsabilidade de dar início à ação penal privada, através da queixa, razão pela qual, frequentemente, os crimes contra a honra cometidos na *web* acabam não chegando ao judiciário.

O legislador trouxe, ainda, a tipificação da injúria qualificada por preconceito de raça, cor, etnia, religião, origem ou condição de pessoa idosa ou portadora de deficiência, que está prevista no §3º do artigo 140, inserida no Código Penal pela Lei nº 9.459, “que impôs penas de reclusão, de 1 a 3 anos, e multa, se a injúria for cometida mediante utilização de elementos referentes a raça, cor, religião ou origem” (CAPEZ, 2012, p. 314).

Nesse passo, verifica-se necessário destacar a distinção entre o crime de

racismo e o crime de injúria racial. O último é referente ao uso de palavras pejorativas em relação à raça ou cor, com a intenção de ofender vítima específica. Já no caso do crime de racismo, previsto na Lei nº 7.716/1989, trata-se de conduta discriminatória dirigida a um grupo ou coletividade. O racismo é delito mais amplo do que o de injúria racional, já que vista atingir uma coletividade indeterminada de indivíduos, promovendo a discriminação de toda uma raça (2015, <http://www.cnj.jus.br>).

No que diz respeito à propagação de mensagens com conteúdo racista pela rede mundial de computadores, Filho (2017, p. 130) disserta:

> [...] o racismo acompanha a história da humanidade e foi a justificativa usual para a prática da escravidão e do genocídio por diversas sociedades. Nos tempos atuais, uma nova forma de praticar esse odioso crime vem se destacando: mensagens racistas são frequentemente divulgadas pela internet. Uma jornalista negra da TV brasileira foi vítima de diversos crimes de racismo por meio das redes sociais, somente pelo fato de ser negra. A divulgação desses fatos foi exponencial e o caso repercutiu nacional e internacionalmente. Estimulados pelo aparente anonimato da internet e pela instantaneidade de comunicação e de retirada das mensagens *online*, muitos crimes de racismo e de "injúria racial" são praticados por usuários brasileiros, todos os dias, por meio de *sites* diversos e das redes sociais. Não obstante, as demais formas de racismo existentes na sociedade brasileira, o racismo é precipuamente relacionado à discriminação dos negros. Além disso, deficientes físicos, homossexuais e mulheres também são vítimas constantes de discriminação social pela Internet. (Grifo original)

Crime de racismo se caracteriza por todo comportamento discriminatório, com correspondência na Lei. 7.716, de 5 de janeiro de 1989, motivado por preconceito de raça, cor ou etnia e que atinge, ao mesmo tempo e solidariamente, toda coletividade. (FILHO, 2017). O artigo 20 da aludida lei trouxe a tipificação penal das seguintes condutas:

> Art. 20. Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional.
> Pena: reclusão de um a três anos e multa.
> § 2º Se qualquer dos crimes previstos no caput é cometido por intermédio dos meios de comunicação social ou publicação de qualquer natureza:
> Pena: reclusão de dois a cinco anos e multa.

Dessa forma, a conduta de postar mensagens discriminatórias, sejam elas por motivo de cor, raça, sexo, orientação sexual ou qualquer outro tipo de intolerância ou ódio, poderá se encaixar ao tipo penal do artigo 20, §2º, da Lei nº 7.716/89, o qual se trata de crime imprescritível. Observa-se que o §2º do tipo penal acima descrito traz uma pena maior quando a discriminação for divulgada através

dos meios de comunicação, tal previsão foi introduzida no ordenamento jurídico brasileiro em uma época que sequer existia a internet (FILHO, 2017).

Por muitas vezes, os indivíduos que propagam ideias preconceituosas pela internet utilizam do argumento de que a Constituição Federal assegura a liberdade de pensamento. Apesar disso, é importante advertir que a liberdade de expressão não é uma garantia constitucional absoluta, uma vez que sofre limitações de natureza ética e de caráter jurídico. Quando se verificar abusos no exercício da liberdade da manifestação de pensamento, tal como quando alguém posta em suas redes sociais declarações de cunho nazista, deverá ocorrer a reação estatal, expondo àquele indivíduo sanções jurídicas de índole penal (2003, <www.conjur.com.br/>).

Atualmente, há uma enorme dificuldade em assegurar o direito de esquecimento em relação às mensagens, imagens e vídeos que circulam pela internet. Dessa maneira,

> [...] mesmo que o autor das mensagens racistas postadas na Internet se arrependa posteriormente e procure “deletar” o conteúdo divulgado, não estará absolutamente a salvo de ser processado e eventualmente responsabilizado criminalmente. É que as mensagens racistas podem ser imediatamente replicadas por outros usuários do mundo inteiro, razão pela qual torna-se praticamente impossível a posterior retirada daquilo que foi compartilhado na rede. Pense-se, por exemplo, na divulgação de uma fotografia montada com uma mensagem racista. Mesmo que o autor da montagem apague posteriormente a postagem inicial, nada impedirá que a fotografia seja instantaneamente compartilhada por diversos usuários do mundo inteiro que tiveram acesso à foto. Assim, se a vítima do crime de racismo está sujeita a reviver indefinidamente situações que diminuíram sua dignidade como pessoa, e o autor do delito, por sua vez, pode ser responsabilizado por crimes que jamais prescreverão (FILHO, 2017, p. 146). (Grifo original)

Infelizmente, os discursos de ódio e a divulgação de mensagens racistas na internet possuem números exorbitantes no Brasil. No ano de 2015, a SaferNet, instituição que recebe queixas de violações de direitos na Internet, recebeu cerca de 55.000 denúncias de casos de racismo *online* no país, sendo que no decorrer de nove anos ocorreram mais de 469.000 denúncias (2016, <www.brasil.elpais.com>).

Números exorbitantes como os relatados anteriormente demonstram que o Brasil ainda é um pais extremamente racista, fato que evidencia a necessidade de promover o combate a qualquer tipo de discriminação, inclusive no ambiente virtual. É essencial para que haja a punição dos crimes cometidos na rede mundial de computadores que as pessoas e, especialmente, as vítimas desses crimes odiosos

denunciem e busquem o auxílio do judiciário para garantir que os criminosos cibernéticos sejam devidamente punidos, na forma da lei.

3.2.3 Estelionato

A internet se tornou um meio de comunicação, informação e interação social, fato que possibilitou o surgimento da sociedade da informação. Nesse passo, é inquestionável o valor que a internet assumiu no cotidiano tanto da vida pessoal quanto profissional dos brasileiros. Paralelo ao sucesso da rede mundial de computadores, surgiram problemas preocupantes como os crimes informáticos, tendo como exemplo as fraudes *online* (WENDT; JORGE, 2012).

O Direito Penal Brasileiro prevê inúmeros tipos de fraude, entretanto, nota-se que o estelionato é a principal delas e se encontra previsto no artigo 171 do Código Penal de 1940:

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
> Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis.
> § 1º - Se o criminoso é primário, e é de pequeno valor o prejuízo, o juiz pode aplicar a pena conforme o disposto no art. 155, § 2º.

O dispositivo penal tutela a inviolabilidade do patrimônio e visa, especialmente, reprimir fraudes que causem dano ao patrimônio do indivíduo. Trata-se de delito em que o criminoso, ao invés de utilizar a violência ou a grave ameaça, emprega uma armadilha, um ardil, o engodo com o intuito de induzir em erro a vítima, levando-a a ter uma visão equivocada dos fatos, a fim de obter vantagem ilícita (CAPEZ, 2012).

O estelionato é praticado com uma grande frequência no ambiente virtual, sobretudo, no âmbito do *e-commerce* (comércio eletrônico), no qual inúmeras pessoas acabam sendo vitimadas ao realizarem compras em *sites* criados com a finalidade de fraudar. A vítima efetua o pagamento corretamente, porém, acaba não recebendo a mercadoria (WENDT; JORGE, 2012).

Os *sites* fraude possuem algumas características específicas: criação de domínios e hospedagem no Brasil ou no exterior, indexação em sites de pesquisa de preços, suposta confiabilidade inicial à condição e credibilidade do site, preço abaixo da média oferecida por outros sites de *e-commerce*, exigência de pagamento através de boleto ou depósito bancário, a falta de Política de Privacidade e Termos

de Uso, assim como poucas formas de contato com os responsáveis pela empresa (WENDT; JORGE, 2012).

Os *sites* fraudes poderão ser encontrados, por muitas vezes, em páginas da internet conhecidas como buscadores de preço, tais como o Buscapé ou o Mercado Livre, promovendo a inserção, inclusive, de qualificações positivas dadas por usuários falsos, afirmando que a loja virtual é confiável e entrega os produtos corretamente. Ainda, é possível verificar que os preços oferecidos pelas lojas virtuais falsas são consideravelmente mais baratos do que nas lojas virtuais tradicionais. Assim, o *site* fraude passa uma falsa aparência de confiabilidade, induzindo a vítima em erro (WENDT; JORGE, 2012).

A prática desse tipo de crime também é frequentemente perpetrada por meio de *e-mail*, como no caso em que a vítima recebe mensagem de correio eletrônico supostamente enviada por um banco renomado, solicitando a confirmação e atualização de seus dados. Assim, o estelionatário virtual envia um *e-mail* a uma certa vítima, fazendo-a presumir que se trata de um banco, visando obter seus dados pessoais e utiliza-los para obter vantagem indevida.

Dessa forma, nota-se que os delinquentes cibernéticos utilizam técnicas para ludibriar a vítima, a fim de convence-la a fornecer dados pessoais, pagar uma certa quantia em dinheiro ou executar determinada tarefa. Esse método de ataque é chamado de engenharia social, que se caracteriza pelo

> [...] uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações. Exemplo: você recebe uma mensagem de *e-mail*, cujo remetente é o gerente ou alguém em nome do departamento de suporte do seu banco. Na mensagem ele diz que o serviço de Internet Banking está apresentando algum problema e que tal problema pode ser corrigido se você executar o aplicativo que está anexado à mensagem. A execução deste aplicativo apresenta uma tela análoga àquela que você utiliza para ter acesso à conta bancária, aguardando que você digite sua senha. Na verdade, este aplicativo está preparado para furtar sua senha de acesso à conta bancária e enviá-la para o atacante (WENDT; JORGE, 2012, p. 21).

O que chama atenção nesse tipo de ação é a criatividade do criminoso e sua capacidade de ludibriar a vítima a fazer o que ele deseja, sendo que esse tipo de prática não possui procedimentos definidos, podendo se modificar de acordo com a originalidade do delinquente cibernético (WENDT; JORGE, 2012).

Sendo assim, na engenharia social, as principais técnicas utilizadas pelos agentes se baseiam na manipulação da emoção dos seus alvos. As emoções mais

manipuladas pelos delinquentes cibernéticos são o medo, a ganância, a simpatia e a curiosidade. O usuário da *web,* motivado por essas sensações, acaba executando código malicioso em seu computador e até fornecendo senhas ou realizando pagamentos de quantias significativas em favor do estelionatário (WENDT; JORGE, 2012).

Por muitas vezes, o criminoso se aproveita de alguma notícia ou assunto de destaque na mídia mundial, nacional ou regional, com o intuito de chamar atenção de suas potenciais vítimas, usando, por exemplo, ataque terrorista ou acidente aéreo de grandes proporções. Esse tipo de prática é chamada de efeito saliência (WENDT; JORGE, 2012).

O mundo virtual oferece inúmeras vantagens para os seus usuários, facilitando a prática de serviços sem que o indivíduo necessite sair de casa, o que era impossível antes do surgimento da internet. As pessoas podem fazer todos os tipos de compras no *e-commerce* e, inclusive, realizar transações bancárias através dos aplicativos e *sites* dos bancos.

Todavia, tais facilidades despertaram o interesse dos estelionatários, que visualizaram no meio virtual uma oportunidade única de criar novas táticas para enganar suas vítimas. Além disso, a sensação de impunidade que predomina no âmbito da internet também auxilia para que o estelionato continue sendo frequentemente executado por meio de dispositivos informáticos.

Nesse contexto, é essencial que as vítimas de fraudes *online* comuniquem a ocorrência do delito às autoridades, pois, apenas assim, será possível iniciar a persecução penal e promover uma diminuição na incidência desse tipo de delito no ambiente cibernético.

4 PROCEDIMENTOS DE INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS

Apenas a tipificação penal de condutas danosas cometidas no ambiente cibernético não garante um combate eficaz aos crimes virtuais, é essencial que o Estado possua aparatos que possibilitem uma investigação criminal forte no âmbito virtual, fazendo uso de técnicas aprimoradas de perícia e de cooperação internacional. Percebe-se dificultosa a efetiva punição dos crimes cibernéticos sem que existam peritos especializados em todos aspectos técnicos do mundo digital.

Nas palavras de Malaquias (2015, p. 80),

> [...] a aplicação da sanção penal exige mais do que a simples dedução, inferência ou conhecimento superficial sobre a identidade do acusado. É necessária a comprovação de que o indivíduo que figura como imputado realmente tenha praticado a conduta que levou ao resultado configurado como crime cibernético. Assim, a eficiência da investigação criminal deverá comprovar por intermédio de perícias oficiais ou outros meios de provas válidas que o *sujeito ativo* A que está sob investigação no *crime cibernético* B ingressou no *ambiente virtual* C por meio da *chave de identificação* D ou E, utilizando-se do *código de acesso* F ou G, descritos e inequivocamente identificados no *laudo pericial* H, apresentados como *prova 1* nos autos do *processo* J, em que tais instrumentos foram utilizados pelo indivíduo sobre o qual recai a imputação penal. (Grifo original)

Para que a persecução penal seja bem sucedida, é essencial que as provas digitais sejam claras e possibilitem a comprovação da materialidade e da autoria dos delitos praticados através da rede mundial de computadores. As provas digitas apresentam traços específicos que permitem sua verificação, ou seja, elas deixam marcas e se caracterizam como o rastro dos crimes cibernéticos (DOMINGOS, 2017).

Nesse contexto, é fundamental enfatizar que quando uma informação é registrada na internet ou em algum dispositivo informático, tal informação poderá ser recuperada dentro de um certo período, ainda que tenha sido apagada. Isso possibilita que a perícia forense analise as provas digitais, verificando sua autenticidade e integridade, propiciando a determinação do seu grau de confiabilidade (DOMINGOS, 2017).

Primeiramente, a prova digital deve ser admissível, isto é,

> [...] como qualquer outra prova, sua aquisição deve ser correta para que possa ser admissível. O segundo requisito, dessa vez específico a sua natureza, é que coleta e preservação devem ser realizadas observando-se os princípios da ciência computacional a fim de garantir sua autenticidade e integridade. Essas características podem ser verificadas pela análise das

> provas digitais pela perícia forense que poderá determinar então o seu grau de confiabilidade. Dessa forma, a prova somente será convincente em juízo se bem esclarecido no laudo pericial o grau de confiabilidade dessa prova, pois na parte das vezes é a prova determinante para a indicação de autoria do delito (DOMINGOS, 2017, p. 245).

Independente do motivo, seja para boas ou más finalidades, quando alguém se conecta à internet, o faz através de ISP (*Internet Protocol Provider*), ou provedor de acesso à internet, sendo que este atribui ao usuário um endereço de IP (*Internet Protocol*), “em uma determinada faixa de data e horário, comumente enquanto durar a conexão à internet. Tal atribuição pode ficar no provedor de conexão (registro de conexão associados a dados cadastrais)” (JESUS; MILAGRE, 2016, p. 170).

Na fase de investigação criminal, é essencial que seja dada a devida importância às evidências deixadas pelo criminoso cibernético através do número identificativo IP que toda estação de trabalho ou computador pessoal recebe ao se conectar com a grande rede mundial. O endereço de IP pode ser “estático (número fixo que pertence a determinado usuário) ou dinâmico (uma faixa de reserva que é atribuída a cada estação de trabalho de modo distinto)” (MALAQUIAS, 2015, p. 105).

Existe a possibilidade, ainda, de se obter informações acerca do acesso à internet através do registro do servidor do *proxy*. Há situações em que o delinquente cibernético faz uso de conexão direta, oportunidade na qual os *logs* de registro de navegação identificam quais os locais que o usuário esteve e os serviços utilizados por ele (MALAQUIAS, 2015).

Além disso, os *cookies*, pequenos registros de informações, são armazenados cada vez que o usuário acessa os *sites* da internet. Através dessas informações “é possível traçar o *user profile* (perfil do usuário) que se consolida em determinado espaço de tempo em virtude de comparação de dados estatísticos comparativos de suas preferências” (MALAQUIAS, 2015, p. 121).

Consequentemente, a investigação criminal e a instrução processual exigem procedimentos técnicos para que seja possível

> [...] dar legitimidade à prova produzida mediante o crime cibernético que será executada por intermédio do exame de corpo de delito e dos exames periciais, a fim de apontar a veracidade do fato, sendo elaborado por profissionais especializados em *hardware, software,* tráfego e segurança de rede. Esses mencionados profissionais poderão definir sobre a existência de vestígios da atividade criminosa desenvolvida e efetivada no ambiente cibernético, por exemplo, indicando a origem de um *e-mail*, sua autoria, integralidade, adulteração, destinatário, itinerário utilizada para chegar ao destino final, endereços virtuais envolvidos, protocolo de comunicação (*Internet Protocol – IP*) que identificará sua tramitação e propriedades

> físicas (MALAQUIAS, 2015, p.110).

A perícia forense possui papel essencial na análise das provas obtidas na investigação criminal, sendo, inclusive, indispensável a presença de perito nas ações de busca e apreensão, a fim de garantir a correta coleta das provas digitais, para que nenhuma informação se perca ou seja corrompida. Outro fator importante é o tempo na obtenção das evidencias deixadas pelo agente, uma vez que a prova digital é extremamente volátil (DOMINGOS, 2017).

A perícia judicial pode ser até mesmo efetuada no computador pessoal, *smartphone* ou qualquer outro dispositivo que seja objeto de investigação e possa ter sido usado, por exemplo, para postar mensagens de ameaça, difamação, calúnia ou imagens de pornografia infantil, necessitando, para isso, de ordem judicial de busca e apreensão de natureza cautelar, com o intuito de verificar a procedência ou improcedência de *e-mail*, arquivo ou programa que possa ter sido objeto do crime (MALAQUIAS, 2015).

Após a promulgação da Lei nº 12.850, de 2 de agosto de 2013, a infiltração de agentes poderá ser utilizada como forma de investigação nos crimes de pornografia infanto-juvenil via internet, considerando a transnacionalidade envolvida no delito, bem como a existência de tratado internacional que obriga o Brasil a promover a sua erradicação (WOLFF, 2017).

No caso concreto, o agente policial infiltrado tenta criar uma relação de confiança para que seja possível desvendar as ações criminosas ou introduzir-se no universo da organização criminosa, para que seja possível compreender seu funcionamento. Essa tarefa pode ser extremamente perigosa, razão pela qual necessita de agentes treinados para a sua execução (WOLFF, 2017).

Porém, o uso de agente infiltrado é procedimento de investigação excepcionalíssimo, sendo imprescindível a autorização judicial, que deverá ser circunstanciada, motivada e sigilosa, estabelecendo os limites a serem respeitados pelo agente infiltrado, nos termos do artigo 10 da Lei nº 12.850/13. Ainda, observa-se que o §2º estabelece os requisitos para que a infiltração seja cabível: “será admitida a infiltração se houver indícios de infração penal de que trata o artigo 1º e se a prova não puder ser produzida por outros meios disponíveis”. Nesse contexto, o artigo 1º da aludida Lei possui a seguinte redação:

> Art. 1º Esta Lei define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal a ser aplicado.
> § 1º Considera-se organização criminosa a associação de 4 (quatro) ou mais pessoas estruturalmente ordenada e caracterizada pela divisão de tarefas, ainda que informalmente, com objetivo de obter, direta ou indiretamente, vantagem de qualquer natureza, mediante a prática de infrações penais cujas penas máximas sejam superiores a 4 (quatro) anos, ou que sejam de caráter transnacional.

Desse modo, é possível o uso de infiltração de agentes para investigar o crime cibernético de pornografia com envolvimento crianças e adolescentes em razão da caracterização da internacionalidade da conduta. Por óbvio, para que se possa utilizar desse método de investigação, deverá ser comprovada a impossibilidade de produzir a prova por outros meios. Afinal, “o uso de ardil por parte do Estado não deverá ser a regra, mas sim a última opção” (WOLFF, 2017, p. 221).

Cabe destacar que a validade da infiltração dependerá da verificação se os limites fixados pelo juiz e a finalidade da investigação foram respeitados pelo agente infiltrado, uma vez que os excessos cometidos no andamento da investigação poderão causar a nulidade da prova obtida (WOLFF, 2017).

Interessante trazer à baila as formas de guarda de prova e registros dos dados da internet, a fim de que tais dados possam auxiliar no processo investigativo. Assim, existem procedimentos simples e usuais que podem ser usados para preservar as informações publicadas na internet, antes que sejam modificadas (WENDT; JORGE, 2012).

A vítima poderá fazer o uso da tela *print screen*, que copia a imagem que estiver aparecendo na tela. Após a cópia da imagem da tela, o usuário poderá colar o conteúdo em programas de edição de imagens, como o *Paint*. Posteriormente, será possível utilizar a imagem salva em relatório de investigação inicial ou, até mesmo, em petição inicial elaborada por advogado da área criminal. Entretanto, o uso somente do *print screen* não é recomendado, considerando que há a possibilidade de manipulação da imagem, que poderá ser questionada judicialmente (WENDT; JORGE, 2012).

Outra opção é o registro de uma Ata Notarial, que se conceitua como

> [...] instrumento público através do qual o tabelião ou seu preposto – a pedido de pessoa interessada ou por quem a ela represente – autentica em forma narrativa os fatos, se estado, e tudo aquilo que atesta por seus próprios sentidos sem a emissão de opinião, juízo de valor ou conclusão, portando por fé (pública) que tudo aquilo presenciado e relatado representa a verdade com consignação nos livros de notas (WENDT; JORGE, 2012, p.

72).

Portanto, a Ata Notarial poderá ser utilizada como meio de prova em ambiente virtual, em relação à *sites* e documentos eletrônicos, fixando data e existência de arquivos como imagens, vídeos, logotipos, mensagens, entre outros. A parte interessada poderá, por exemplo, imprimir o site relacionado ao delito e registrar uma Ata Notarial, que poderá ser utilizada como meio de prova em eventual processo criminal (WENDT; JORGE, 2012).

Além das formas acima relatadas, destaca-se que a certidão elaborada pela Polícia Civil também representa importante instrumento para salvaguardar dados eletrônicos. O Escrivão poderá acessar uma página internet, promover sua impressão e certificar data e a existência desta, uma vez que seus atos possuem fé pública. Nesse contexto, a vítima de crime cibernético poderá se dirigir à uma Delegacia de Polícia e, após a elaboração do boletim de ocorrência, poderá solicitar que seja feita a impressão das mensagens ou postagens do *site* que contenha os fatos criminosos (WENDT; JORGE, 2012).

Observa-se, inclusive, que houve um avanço em relação ao combate os crimes digitais com a promulgação da Lei nº 12.735, de 30 de novembro de 2012, que prevê, em seu artigo 4º, que os órgãos da polícia judiciária poderão estruturar, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

4.1 Marco civil da internet e a investigação no ambiente virtual

A Lei nº 12.965, de 23 de abril 2014, conhecida como o Marco Civil da Internet, estabeleceu inúmeros direitos aplicáveis ao ambiente virtual, reconhecendo direitos fundamentais já previstos na Constituição Federal de 1988, bem como em documentos internacionais dos quais o Brasil é signatário, como, por exemplo, o Pacto de São José da Costa Rica. O Marco Civil da Internet é considerado a “Constituição da Internet”, assegurando direitos e deveres aos usuários e provedores da internet brasileira (FIORILLO; CONTE, 2016).

Além de estabelecer princípios, garantias, direitos e deveres para os usuários brasileiros, a Lei 12.965/2014 serve como forma de complementação nas atividades de repressão aos crimes cibernéticos. Apesar de não tratar da estrutura

investigativa, tampouco dos deveres dos provedores de internet e serviços quanto à cooperação para com as autoridades que investigam os delitos digitais, o Marco Civil da Internet tipifica fatos cibernéticos (JESUS; MILAGRE, 2016).

Segundo Jesus e Milagre (2016, p. 170),

> [...] sabe-se que o provedor dos serviços (pago ou gratuito) registra os dados de acesso à aplicação (em alguns casos até mesmo as atividades realizadas – embora muitos afirmem que não), porém tais registros só são fornecidos com ordem judicial. Obtendo-se os dados de acesso ás aplicações daquele que utilizou o serviço para más finalidades, pode-se, através do IP (*Internet Protocol*), que será fornecido, descobrir qual o Provedor de Acesso associado ao IP (caso o usuário não tenha mascarado a conexão), e, com isto, oficiá-lo, para que apresente os dados físicos (nome, endereço, RG, CPF, CNPJ, dentre outros) da pessoa responsável pela conta de Internet a qual estava atribuído o referido IP, na exata data e hora da atividade maliciosa. Por meio desta correlação, pode-se chegar à autoria de delitos cometidos por meio da internet. Nesse contexto, como fica evidenciado, sem a cooperação dos provedores de Internet ou de serviços, em muitos casos, é praticamente impossível apurar a autoria de delitos cibernéticos, e a questão se agrava quando um destes provedores não está no Brasil.

O Marco Civil da Internet, nos termos do seu artigo 7º, inciso I, assegura aos usuários o direito à inviolabilidade e ao sigilo de suas comunicações no meio digital. Conforme o inciso V, o usuário possui, inclusive, o direito de não fornecer a terceiros seus registros de conexão e de acesso à internet, salvo nas hipóteses previstas em lei ou mediante consentimento (JESUS; MILAGRE, 2016).

A Lei nº 12.965/2014 esclarece que os provedores somente serão obrigados a fornecer os registros e informações que permitem a identificação de usuário mediante ordem judicial. Da mesma forma, a remoção de conteúdo só é possível com mandado judicial, com exceção aos casos envolvendo imagens de nudez, situação na qual poderá ser solicitada a remoção da foto por meio de notificação extrajudicial, que deverá ser atendida pelos provedores (JESUS; MILAGRE, 2016).

Além disso, os artigos 13 e 15 da Lei nº 12.965/2014 trazem as seguintes redações:

> Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.
> Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

Assim, verifica-se que os provedores de acesso têm o dever de manter os registros de conexão pelo prazo de um ano, enquanto os provedores de aplicações ou serviços de internet deverão conservar os registros de acesso a aplicações pelo prazo de seis meses. Todavia, destaca-se que a autoridade policial ou administrativa e o Ministério Público poderão requerer aos provedores a manutenção dos registros por tempo superior ao previsto em lei, através de requerimento judicial dos dados, nos termos do §2º do artigo 15 da lei em comento (JESUS; MILAGRE, 2016).

Em relação ao exposto acima, Fiorillo e Conte (2016, p. 228) afirmam que

> [...] o Marco Civil da Internet teve por objetivo, nesse aspecto, solucionar um dos grandes impasses no tocante à responsabilidade sobre o conteúdo postado e, principalmente, na contribuição com investigações criminais sobre crimes cibernéticos. Ocorre que, até então, a responsabilidade sobre o armazenamento dos dados dos usuários não era regulamentada por lei e cada empresa fazia, quando fazia, a seu modo.

A norma é clara ao prever que o fornecimento de registros de conexão ou de acesso a aplicações só poderá ocorrer mediante autorização de autoridade judiciária, ou seja, mediante ordem de um Juiz de Direito. Por outro lado, o Marco Civil permitiu às autoridades policiais e ao Ministério Público o acesso de dados cadastrais de usuários sem necessidade de autorização judicial, sendo suficiente o simples requerimento. Importante destacar que não se deve confundir dados cadastrais com dados de conexão, pois aqueles podem ser obtidos via requerimento direto aos provedores, enquanto estes somente via ordem judicial (JESUS; MILAGRE, 2016).

Conclui-se, portanto, que o Marco Civil da Internet trouxe previsões relevantes que influem diretamente na investigação criminal dos delitos cibernéticos, prevendo, por exemplo, tempo mínimo para a manutenção de registros de conexão e acesso, o que, visivelmente, auxilia no êxito das investigações que necessitam, especificamente, dos dados de conexão e acesso do investigado.

4.2 Cooperação internacional

O avanço da tecnologia integrou o mundo em uma grande teia, na qual todos possuem acesso aos mais diferentes tipos de conteúdo em todo o planeta, não importando o local físico em que esteja armazenado tal conteúdo. Entretanto, para a Justiça, “o local físico da prática de um ato digital tem relevância para

determinar a competência judiciária” (JESUS; MILAGRE, 2016, p. 179).

Como consequência dessa interligação virtual entre usuários de diversos países, é comum que os criminosos cibernéticos busquem praticar delitos por meio de sistemas hospedados no exterior. Quando tal situação ocorre, a investigação, no Brasil, necessita da cooperação de provedores de serviço ou conexão situados fora do país (JESUS; MILAGRE, 2016).

No entanto, na prática verifica-se uma resistência muito grande por parte dos provedores estrangeiros em cumprir ordens judiciais brasileiras, sob a alegação de que não estão sujeitos às ordens do Poder Judiciário brasileiro e que somente poderiam cumprir ordens dos países que consideram capazes para tais atos, como, por exemplo, o Estado onde estão armazenados os dados pretendidos (DOMINGOS, 2017).

Ocorre que é indiscutível que a cooperação internacional é imensamente importante para o combate aos crimes digitais, podendo ser usada para a obtenção de dados essenciais para a investigação criminal ou até como meio de prova no processo penal (JESUS; MILAGRE, 2016).

As principais medidas de cooperação internacional são a carta rogatória e o auxílio mútuo em matéria penal, sendo que cada país utiliza o método de cooperação internacional que entende adequado. As cartas rogatórias são pedidos expedidos pelas autoridades judiciárias brasileiras aos juízos de outros países, para que cumpram ato instrutório em conformidade com a lei daquele país. Já o auxílio mútuo em matéria penal, também conhecido por auxílio direto, exerce a função de obter provas para a investigação e o processo criminal, se caracterizando como um instrumento estatal para o combate à criminalidade transnacional (DOMINGOS, 2017).

> Em alguns casos, autoridades se valem do chamado DRCI do Ministério da Justiça, o Departamento de Recuperação de Ativos e Cooperação Internacional da entidade, que faz a intermediação entre órgãos judiciais dos países envolvidos. Nesse caso, o delegado que está conduzindo a investigação representa ao juiz, e de posse da resposta do juiz autorizando a quebra, ele entra em contato com o DRCI. Este, por sua vez, pode devolver a solicitação ao delegado, para que ela seja adaptada às necessidades do país que receberá a solicitação, ou, caso esteja tudo em ordem e na língua do Estado de destino, encaminha ao país onde se buscam os dados de um criminoso digital ou a remoção de um conteúdo ilícito. Os dados, então, caso haja a cooperação, voltam ao DRCI, que comunica nos autos a informação, ou caso em fase de inquérito, diretamente à delegacia de polícia. Esta cooperação é possível por ser o Brasil signatário do MLAT. A possibilidade do uso das cartas do chamado MLAT (*Mutual Legal Assistance Treaty*), não deve ser desconsiderada (JESUS; MILAGRE, 2016, p. 179).

Convém apontar, ainda, que o principal organismo para a cooperação internacional é a INTERPOL (*International Criminal Police Organization*), que, por meio da administração de um serviço universal de comunicações e gerenciamento de informações, auxilia e capacita forças policiais nacionais em suas investigações. No combate aos crimes cibernéticos de disseminação de pornografia infantil, por exemplo, se na fase de investigação forem identificados IPs e dados de conexão pertencentes a outro país, poderá ocorrer a troca de informações relevantes às investigações entre as autoridades competentes daqueles países, sendo que essa troca acontece, geralmente, por intermédio da INTERPOL (DOMINGOS, 2017).

É essencial que se promova o conhecimento e o aperfeiçoamento dos mecanismos de cooperação internacional, no sentido de tornar possível a obtenção de provas digitais dos provedores estrangeiros de uma forma desburocratizada e célere, representando, assim, o verdadeiro auxílio direto, a fim de facilitar a persecução penal dos crimes praticados no ambiente virtual (DOMINGOS, 2017).

Dessa forma, a cooperação internacional, bem como a harmonização das legislações penais dos países se caracterizam como solução eficiente no combate aos crimes informáticos, tendo em vista que permitem maior agilidade e efetividade nas investigações e punições (FIORILLO; CONTE, 2016).

5 CONCLUSÃO

O presente trabalho monográfico teve como principal objetivo promover uma análise sobre os crimes cibernéticos mais comumente praticados no ambiente virtual, bem como verificar quais os procedimentos de investigação que poderão ser utilizados na persecução criminal.

Uma maior conscientização acerca da tipificação dos delitos informáticos e das formas de guarda de prova e dados da internet poderá auxiliar no combate à este tipo de delito, considerando que tais informações poderão ser usadas na investigação criminal. Em razão disso, necessário destacar que os crimes cibernéticos carecem de maior atenção do mundo jurídico, pois, mesmo que se verifiquem números assustadores de crimes praticados na *web*, os estudos e a prevenção em relação à essas infrações ainda são significativamente pequenos.

Através da pesquisa sobre a origem da internet e das primeiras infrações cometidas no ambiente virtual, verifica-se que os delitos cibernéticos surgiram concomitantemente com o advento da rede mundial de computadores, o que demonstra que os delinquentes enxergaram, desde logo, o ambiente virtual como propício para a perpetração de delitos, uma vez que se sentem protegidos pela falsa sensação de anonimato que a internet lhes propicia.

Por outro lado, a legislação penal informática evolui em velocidade consideravelmente inferior ao surgimento de novos crimes cibernéticos, o que se demonstra justificável uma vez que a evolução tecnológica acontece com uma rapidez incrível e difícil de acompanhar. Entretanto, o Direito tem o dever de promover a punição aos agentes que praticam delitos cibernéticos, para que a internet não se torne um ambiente sem regras, onde pessoas mal intencionadas possam prejudicar terceiros sem a devida repreensão estatal.

Em relação a tipificação dos crimes digitais, observa-se que uma grande parte dos delitos perpetrados no ambiente virtual já se encontram tipificados pelo Código Penal de 1940, sendo que as infrações penais estão sendo praticadas através da internet e das novas tecnologias, estas que são usadas apenas como um novo instrumento para a execução de delitos já conhecidos, como, por exemplo, o estelionato, os crimes contra a honra, entre outros. Estes são os chamados crimes cibernéticos impróprios.

Ocorre que, a internet proporciona inúmeras formas de propagação de mensagens, notícias e imagens que podem ser postadas por qualquer usuário,

facilitando, assim, a ação de estelionatários virtuais e delinquentes que visam ofender ou difamar suas vítimas.

Conclui-se, portanto, que os crimes cibernéticos estão muito mais presentes no ambiente virtual do que poderíamos imaginar, pois, por muitas vezes, o usuário da *web* se sente protegido pela ideia do anonimato que a rede lhe proporciona e age de formas que não teria coragem fora dela.

Além disso, as inovações tecnológicas oferecerem infinitas possibilidades para aperfeiçoar o *modus operandi* dos criminosos, que se utilizam da criatividade e da eficiência das novas tecnologias para ludibriar suas vítimas, assim como para propagar informações falsas, com o intuito de obter vantagem ilícita ou causar danos a terceiros.

Destaca-se, ainda, que um dos maiores problemas que a internet ocasionou é a propagação desenfreada de pornografia infantil. O uso da rede mundial de computadores ampliou assustadoramente o consumo de imagens e vídeos pornográficos envolvendo crianças e adolescentes, considerando que o download deste tipo de arquivo é simples e poderá ser feito por um enorme números de usuários ao mesmo tempo.

Os crimes envolvendo pornografia infantil acontecem em dimensão ainda maior em áreas de difícil acesso na internet, como a *deep web,* fato que dificulta a identificação dos autores destes delitos e a remoção do conteúdo ilícito da rede. Portanto, é essencial que se promova o combate a esse tipo de crime, considerando que se caracterizam como uma afronta aos direitos fundamentais da criança e do adolescente, estes que necessitam de uma proteção integral e especial por parte do Estado e da sociedade.

Diante do estudo realizado, pode-se concluir que inúmeras infrações perpetradas através da internet já se encontram tipificadas no Código Penal Brasileiro, as novas tecnologias apenas representam um novo instrumento utilizado para conduta criminosa, possibilitando, assim, a aplicação da legislação já existente. Dessa forma, o espaço cibernético é relativamente protegido pelas normas penais brasileiras.

Não obstante, em relação aos crimes cibernéticos próprios, ou seja, aqueles vinculados com a utilização das novas tecnologias para a consumação do delito, a legislação penal demonstra-se omissa. A Lei nº 12.737, de 30 de novembro de 2012, de maneira inovadora, trouxe a tipificação de crimes cibernéticos próprios, criminalizando condutas cibernéticas que ainda não encontravam amparo no

ordenamento jurídico brasileiro.

Observa-se que o legislador restringiu a aplicação do crime de invasão de dispositivo informático impondo como condição para o enquadramento na norma penal que o dispositivo informático esteja protegido por mecanismos de segurança, tais como senhas e softwares. A previsão de condições para que a conduta seja considerada crime tem como objetivo restringir o âmbito de atuação da lei e evitar a criminalização excessiva de condutas realizadas cotidianamente na internet, o que poderia criar entraves para a inovação no meio digital.

Conforme já debatido no presente trabalho, existem inúmeras condutas prejudiciais praticadas por usuários mal intencionados que ainda não se encontram tipificadas no ordenamento jurídico brasileiro, permitindo que as vítimas de tais condutas arquem com os danos que sofreram sem nenhum tipo de proteção e punição do Estado, tais como a disseminação de vírus de computador ou o envio de mensagens não solicitadas, o *spam*. Dessa forma, infrações cibernéticas próprias ainda necessitam de um maior amparo do Direito Penal Brasileiro.

No que diz respeito aos procedimentos de investigação dos crimes cibernéticos, é possível concluir que as provas virtuais são essenciais para que haja a efetiva punição aos delinquentes virtuais, pois apenas será possível a comprovação da materialidade e autoria se as provas obtidas na fase investigatória forem claras e confiáveis.

Dessa forma, torna-se indispensável detectar às evidências deixadas pelo criminoso cibernético, como o endereço de IP, através do exame de corpo de delito e exames periciais. A perícia forense é essencial na análise das provas obtidas, razão pela qual é crucial que peritos sejam devidamente qualificados e possuam amplo conhecimento técnico informático.

Outro fator que poderá influir positivamente na investigação criminal é o uso de agente infiltrado, assim como a criação de equipes especializadas no combate e repreensão aos crimes cibernéticos.

Por fim, considerando que vivemos em um mundo globalizado, em que os países se encontram interligados por meio da internet, a cooperação internacional é ferramenta fundamental para a devida punição dos crimes cibernéticos, sendo, para tanto, necessária uma atuação satisfatória por parte do Estado, promovendo o aperfeiçoamento dos mecanismos de cooperação internacional e, consequentemente, ampliando o combate e prevenção aos crimes digitais.

Sendo assim, concluo que os infrações perpetradas no ambiente virtual

estão parcialmente amparadas pelo ordenamento jurídico brasileiro, havendo, especialmente, uma lacuna considerável na tipificação dos delitos cibernéticos próprios. Quanto aos métodos de investigação, entendo que é fundamental que se promova uma melhoria no aparelhamento policial, o aperfeiçoamento dos profissionais que atuam no âmbito investigativo, bem como o uso da cooperação internacional para que seja possível a efetiva punição dos crimes cibernéticos já tipificados na legislação penal.

REFERÊNCIAS

BRASIL. Código Penal (1940). *Código Penal Brasileiro*. Brasília, DF: Senado Federal, 1940.

_____. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Diário Oficial da República Federativa do Brasil, Brasília, DF, 16 jul. 1997. Disponível em: <http://www.planalto.gov.br/ccivil_ 03/Leis/L8069Compilado.htm>. Acesso em: 16 out 2017.

_____. Lei nº 9.609, de 19 de fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no país, e dá outras providências. *Diário Oficial [da] República Federativa do Brasil,* Brasília, DF, 19 fev. 1998. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9609. htm>. Acesso em: 18 maio 2017.

_____. Lei nº 9.983, de 14 de julho de 2000. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências. *Diário Oficial [da] República Federativa do Brasil,* Brasília, DF, 14 jul. 2000. Disponível em: <http://ww w.planalto .gov.br/ccivil_03/leis/L9983.htm>. Acesso em: 23 maio 2017.

_____. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. *Diário Oficial [da] República Federativa do Brasil,* Brasília, DF, 30 nov 2012. Disponível em: <http://www.planalto. gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 20 set 2017.

CAPEZ, Fernando. *Curso de Direito Penal.* 12. ed. São Paulo: Saraiva, 2012.

_____. *Curso de Direito Penal.* 17. ed. São Paulo: Saraiva, 2013.

CARVALHO, Ana Cristina Azevedo P. *Marco Civil da Internet no Brasil:* análise da Lei 12.965/14 e do Direito da Informação. Rio de Janeiro: Alta Books, 2014.

CASTELLS, Manuel. *A Galáxia da Internet:* reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar, 2003.

_____. *A Sociedade em Rede.* 8. ed. atual. São Paulo: Paz e Terra, 2005.

CAVALCANTE, Ana Mary. Crimes cibernéticos: o Brasil é o 5º do mundo em fraudes digitais. *O Povo,* [S.l.], 24 jan. 2016. Disponível em: <http://www20.opovo.com.br/app /opovo/dom/2016/01/23/noticiasjornaldom,3565860/crimes-ciberneticos-brasil-e-o-5-do-mundo-em-fraudes-digitais.shtml>. Acesso em: 27 maio 2017.

CONFIRA alguns crimes virtuais que viraram notícia. *Folha de São Paulo*, São Paulo, 07 jan. 2006. Disponível em: <http://www1.folha.uol.com.br/folha/informatica /ult124u194 60.shtml>. Acesso em: 26 maio 2017.

CRIMES virtuais afetam 42 milhões de brasileiros. *Estadão*, São Paulo, 27 jan. 2017. Disponível em: <http://economia.estadao.com.br/noticias/releases-ae,crimes-virtuais-afetam-42-milhoes-de-brasileiros,70001644185>. Acesso em: 22 maio 2017.

DOMINGOS, Fernanda Teixeira Souza. A obtenção de provas digitais na investigação dos delitos de violência e exploração sexual infantil online. In: SILVA, Ângelo Roberto Ilha da. *Crimes Cibernéticos*. Porto Alegre: Livraria do Advogado, 2017. p. 235-254.

D'URSO, L. F. F.; D'URSO, L. A. F. Ataque cibernético mundial é a comprovação da insegurança na internet. *Conjur,* [S.l.], 17 maio 2017. Disponível em: <http://www.conjur.com.br/2017-mai-17/ataque-cibernetico-mundial-comprova-inseguranca-internet>. Acesso em: 25 maio 2017.

FIORILLO, C. A. P.; CONTE, C. P. *Crimes no Ambiente Digital e a Sociedade da Informação*. 2. ed. São Paulo: Saraiva, 2016.

INTERNET chegou para provar que somos um dos países mais racistas do mundo. *El Pais,* Rio de Janeiro, 15 jun 2016. Disponível em: <https://brasil.elpais.com/brasil/2016/05/10/politica/1462895132_579742.html>. Acesso em: 20 set 2017.

JESUS, D. D.; MILAGRE, J. A. *Manual de Crimes Informáticos.* São Paulo: Saraiva, 2016.

KNIGHT, Peter T. *A Internet no Brasil:* origens, estratégia, desenvolvimento e governança. Indiana: Author House, 2014.

LEIA o segundo voto de Celso de Mello no HC do editor nazista. *Conjur,* [S.l.], 1 out 2003. Disponível em: <https://www.conjur.com.br/2003-out-01/liberdade_expressao_nao_absoluta_afirma_ministro>. Acesso em: 20 set 2017.

MALAQUIAS, Roberto Antônio Darós. *Crime Cibernético e Prova:* a investigação criminal em busca da verdade. 2. ed. Curitiba: Juruá, 2015.

MASI, Carlo Velho. Crime contra a honra pela internet. *Canal Ciências Criminais,* [S.l.], 3 set 2016. Disponível em: <https://canalcienciascriminais.com.br/crimes-contra-honra-pela-internet/>. Acesso em: 5 out 2017.

MURARD, Ana Beatriz Conte. Crimes contra a honra na internet. *Jusbrasil,* [S.l.], 2 out 2014. Disponível em: <https://anabmurard.jusbrasil.com.br/artigos/169528179/crimes-contra-a-honra-na-internet>. Acesso em: 5 out 2017.

NETO, Pedro Rodrigues. Condenação de Nando Moura mostra que a internet não é "terra de ninguém". *Pense*, [S.l.], 23 ago 2017. Disponível em: < https://penseegratis org/2017/08/23/condenacao-de-nando-moura-mostra-que-internet-nao-e-terra-de-ninguem/>. Acesso em: 5 out 2017.

OLIVEIRA JUNIOR, Eudes Quintino. A nova lei Carolina Dieckmann. *Jusbrasil,* [S.l.], dez. 2012. Disponível em: <https://eudesquintino.jusbrasil.com.br/artigos/121823244/a-nova-lei-carolina-dieckmann>. Acesso em: 25 maio 2017.

PRESSE, France. Ataque de hackers sem precedentes provoca alerta no mundo. *G1,* [S.l.], 13 maio 2017. Disponível em: < http://g1.globo.com/tecnologia/noticia/ataque-de-hackers-sem-precedentes-provoca-alerta-no-mundo.ghtml>. Acesso em: 26 maio 2017.

QUESADA, J. D.; CANO, R. J. O ciberataque: apertar um botão e desligar o mundo. *El País,* Madri, 21 maio 2017. Disponível em: <http://brasil.elpais.com/brasil/2017/05/20/internacional/1495291083_920693.html>. Acesso em: 25 maio 2017.

SILVA, Ângelo Roberto Ilha da. Pedofilia, pornografia infantil e os tipos penais previstos no Estatuto da Criança e do Adolescente. In: SILVA, Ângelo Roberto Ilha da. *Crimes Cibernéticos*. Porto Alegre: Livraria do Advogado, 2017. p. 85-102.

SILVA, Patrícia Santos. *Direito e Crime Cibernético*: análise da competência em razão do lugar no julgamento de ações penais. Brasília: Vestnik, 2015.

TESTA CÔRREA, Gustavo. *Aspectos Jurídicos da Internet.* São Paulo: Saraiva, 2000.

VIEIRA, Eduardo. *Os Bastidores da Internet no Brasil:* as histórias de sucesso e fracasso que marcaram a web brasileira. Barueri, SP: Manole, 2003.

WENDT, E.; JORGE, H. V. N. *Crimes Cibernéticos:* ameaças e procedimentos de investigação. Rio de Janeiro: Brasport Livros e Multimídia, 2012.

WOLFF, Rafael. Infiltração de agentes por meio virtual. In: SILVA, Ângelo Roberto Ilha da. *Crimes Cibernéticos*. Porto Alegre: Livraria do Advogado, 2017. p. 215-234.

.