UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE - UFRN
CENTRO DE CIÊNCIAS JURÍDICAS SOCIAIS E APLICADAS - CCSA
DEPARTAMENTO DE DIREITO PÚBLICO
CURSO DE GRADUAÇÃO EM DIREITO

OS CIBERCRIMES E O DIREITO BRASILEIRO: AS LIMITAÇÕES DA LEGISLAÇÃO EM VIGOR, CONSIDERANDO A REALIDADE TECNOLÓGICA

MATHEUS PIERRE FERNANDES

NATAL - RN

2021

MATHEUS PIERRE FERNANDES

OS CIBERCRIMES E O DIREITO BRASILEIRO: AS LIMITAÇÕES DA LEGISLAÇÃO EM VIGOR, CONSIDERANDO A REALIDADE TECNOLÓGICA

Monografia apresentada ao Curso de Direito sob a orientação da Professora Drª. Mariana de Siqueira como requisito parcial para obtenção do título de Bacharel em Direito, do Centro de Ciências Sociais Aplicadas, da Universidade Federal do Rio Grande do Norte.

Orientadora: Profª. Drª. Mariana de Siqueira.

NATAL - RN

2021

Universidade Federal do Rio Grande do Norte - UFRN
Sistema de Bibliotecas - SISBI
Catalogação de Publicação na Fonte. UFRN - Biblioteca Setorial do Centro Ciências Sociais Aplicadas - CCSA

Fernandes, Matheus Pierre.
Os cibercrimes e o direito brasileiro: as limitações da legislação em vigor, considerando a realidade tecnológica / Matheus Pierre Fernandes. - 2021.
88f.: il.

Monografia (Graduação em Direito) - Departamento de Direito, Centro de Ciências Sociais Aplicadas, Universidade Federal do Rio Grande do Norte, Natal, 2021.
Orientadora: Profa. Dra. Mariana de Siqueira.

1. Direito penal - Monografia. 2. Crime cibernético - Monografia. 3. Lei Carolina Dieckmann - Monografia. 4. Invasão de dispositivos informáticos - Monografia. I. Siqueira, Mariana de. II. Título.

RN/UF/CCSA CDU 343.4:004

Elaborado por Shirley de Carvalho Guedes - CRB-15/440

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
DEPARTAMENTO DE DIREITO PUBLICO - DIPUB

ATA Nº 8/2021 - DPU/CCSA (16.17)

Nº do Protocolo: 23077.043577/2021-51

Natal-RN, 30 de abril de 2021.

ATA DE DEFESA DE TRABALHO DE CONCLUSÃO DE CURSO

Aos vinte e nove dias do mês de abril de 2021, às 09:30, na Plataforma Virtual Google Meet, realizou-se a sessão pública para a defesa oral do Trabalho de Conclusão do Curso de Graduação em Direito intitulado: "OS CIBERCRIMES E O DIREITO BRASILEIRO: AS LIMITAÇÕES DA LEGISLAÇÃO EM VIGOR, CONSIDERANDO A REALIDADE TECNOLÓGICA", de MATHEUS PIERRE FERNANDES, matrícula nº 2016051167. A Comissão Examinadora, designada pela Portaria-TCC nº 05/2021-DPU, foi composta pelos professores Mariana de Siqueira, matrícula nº 1753047 (DPU/UFRN), Lidianne Araújo Aleixo de Carvalho, matrícula nº 2314286 (DPU/UFRN) e Karoline Lins Câmara Marinho de Souza, matrícula nº 2578062 (DPU/UFRN). Realizada a defesa oral e a arguição, em conformidade com os procedimentos regulares, a Comissão considerou a monografia APROVADA, atribuindo-lhe a nota 10,0 e a menção COM DISTINÇÃO.

(x) Este TCC é um trabalho de excelência e considero-o INDICADO a concorrer ao prêmio de melhor TCC do Curso neste semestre

(Assinado digitalmente em 30/04/2021 11:42)
KAROLINE LINS CAMARA MARINHO DE SOUZA
PROFESSOR DO MAGISTERIO SUPERIOR
DPU/CCSA (16.17)
Matrícula: 2578062

(Assinado digitalmente em 30/04/2021 10:13)
LIDIANNE ARAUJO ALEIXO DE CARVALHO
PROFESSOR DO MAGISTERIO SUPERIOR
DPU/CCSA (16.17)
Matrícula: 2314286

(Assinado digitalmente em 30/04/2021 11:04)
MARIANA DE SIQUEIRA
PROFESSOR DO MAGISTERIO SUPERIOR
DPU/CCSA (16.17)
Matrícula: 1753047

RESUMO

O presente trabalho tem o objetivo de identificar e analisar as lacunas que existem na Legislação Penal Brasileira, quando considerado a realidade atual dos cibercrimes, é dizer, como eles ocorrem, qual seu atual potencial, etc. Para isso é preciso explicar todo o contexto fático, que já deixa muito claro que legislação brasileira de crimes cibernéticos, a Lei nº 12.737/2012, que foi apelidada de Lei Carolina Dieckmann, nasceu ultrapassada. O principal problema identificado na pesquisa é que a legislação brasileira trata os cibercrimes como se este se resumisse à conduta de invadir dispositivos informáticos. Essa visão é muito equivocada e remonta aos primórdios do surgimento do termo hacker. Para encontrar as respostas para os problemas desta pesquisa e atingir seus objetivos, foi feita uma pesquisa exploratória, por meio de levantamento bibliográfico e com a aplicação de dois métodos científicos: o método dedutivo e o método hipotético dedutivo. Com a redação dada ao art. 154-A do Código Penal, uma série de ataques cibernéticos são penalmente atípicos no Brasil, quando puramente considerados, pois tecnicamente não envolvem a invasão de dispositivos informáticos, o que não faz com que tenham resultados menos lesivos às vítimas e a sociedade. É o que ocorre com o *phishing*, o vazamento de dados pessoais, o ataque de *ransomware* e o ataque de *spoofing*, condutas que já são praticadas há algum tempo, causam danos vultosos a um grande número de pessoas, mas há verdadeiras brechas que permitem que as condutas passem impunes. Alguns desses problemas e lacunas podem ser resolvidas pela aprovação do PL 236 do Senado, que se trata do projeto de Novo Código Penal, que na sua redação original tipifica o ataque de *ransomware*, diminui as hipóteses de atipicidade do ataque *spoofing* e acaba com a visão de que todo os cibercrimes se resume à invasão de dispositivos informáticos. Mas esse não é único propósito da pesquisa, que também cuida de analisar os desafios envolvidos na investigação e repressão dos crimes cibernéticos, como a transnacionalidade da rede e a multiplicidade de jurisdições, a existência de serviços de *Proxies* que dificultam a identificação do endereço IP dos hacker, além do fim da estratégia *follow the money*, ocasionada pelo surgimento das criptomoedas irrastreáveis, como a Bitcoin. Ademais, a base legal da repressão penal não é a única preocupação do presente trabalho, que também aponta possíveis estratégias de prevenção, principalmente estratégias baseadas na informação contra as principais fraudes e crimes praticados na internet.

Palavras-chave: cibercrimes; Lei Carolina Dieckmann; invasão de dispositivos informáticos; lacunas.

ABSTRACT

This work has the objective of identifying and analyzing the gaps that exist in the Brazilian Criminal Law, when considering the current reality of cybercrimes, it is to say, how they occur, what is its current potential, etc. For this, it is necessary to explain the entire factual context, which already makes it very clear that Brazilian cybercrime legislation, Law No. 12,737 / 2012, which was dubbed Carolina Dieckmann Law, was born outdated. The main problem identified in the research is that Brazilian legislation treats cybercrimes as if it were reduced to the conduct of breaking into computer devices. This vision is very wrong and goes back to the beginning of the term hacker. To find the answers to research issues e to reach all its goals, was made an exploratory research, through bibliographic survey and with the application of two scientific methods: the deductive method and the hypothetical-deductive method. With the redaction given to the art. 154-A of the Criminal Code, a series of cyber attacks are criminally atypical in Brazil, when they are purely considered, because they technically do not involve the invasion of computer devices, which does not result in less harmful results for victims and society. This is what happens with phishing, the leakage of personal data, the ransomware attack and the spoofing attack, conducts that have been practiced for some time, cause huge damage to a large number of people, but there are real gaps that allow conducts to go unpunished. Some of these problems and gaps can be solved by the approval of the Senate's PL 236, which is the New Penal Code project, which in its original wording typifies the ransomware attack, reduces the chances of atypicality of the spoofing attack and ends the vision that all cybercrimes comes down to the invasion of computer devices. But this is not the only purpose of the research, which also takes care of analyzing the challenges involved in the investigation and repression of cyber crimes, such as the transnationality of the network and the multiplicity of jurisdictions, the existence of Proxies services that make it difficult to identify the IP address of hackers, in addition to the end of the follow the money strategy, caused by the emergence of untraceable cryptocurrencies, as Bitcoin. In addition, the legal basis of criminal repression is not the only concern of the present work, which also points out possible prevention strategies, mainly strategies based on information against the main frauds and crimes practiced on the internet.

Keywords: cybercrimes; Carolina’s Dickmann Law; invasion of computer devices; gaps.

AGRADECIMENTOS

Agradeço primeiramente aos meus pais por toda educação que me deram e todo o suporte para que pudesse chegar até esse momento.

Agradeço à minha orientadora Mariana de Siqueira, que através do Grupo de Estudos de Direito Público da Internet e das Inovações Tecnológicas (GEDI-UFRN) me despertou o interesse por pesquisar na área de Direito e Tecnologia.

Agradeço a Vargner de Paula, colega de trabalho durante meu estágio no Ministério Público Federal, que fez crescer substancialmente o meu interesse pelo Direito Penal.

Agradeço também a minha namorada Selly, que me deu todo o suporte emocional para enfrentar os árduos anos dessa graduação.

Por fim, agradeço aos meus amigos do curso, em especial a Vanessa Lopes, João Victor, João Luís e Emanuelle Campbell, que foram mais próximos e contribuíram ouvindo minha idéias e dando opiniões.

ÍNDICE DE IMAGENS

SUMÁRIO

1 INTRODUÇÃO

1.1 CONTEXTUALIZAÇÃO

Não há dúvidas que o avanço tecnológico seja um processo benéfico e venha facilitar o dia a dia da humanidade. Entretanto, historicamente, as ferramentas tecnológicas, que surgem como propósitos lícitos e benéficos, são apropriadas pelo crime e empregadas de forma nociva em relação à sociedade.

Quanto a isso, exemplos não faltam. O automóvel, que foi um grande avanço e revolucionou a forma de locomoção do ser humano, não demorou para ser empregado pelo crime, em roubos e fugas. O dinamite, que foi inventada por Alfred Nobel em 1867 (ARAÚJO, c2021), hoje em dia é fortemente empregada para furtar valores em caixas eletrônicos. Sendo assim, com o advento e a popularização dos microcomputadores e com o advento da rede mundial de computadores (internet), não é estranho que o mesmo processo aconteça.

Os primeiros computadores, quando foram inventados, eram máquinas enormes, que ocupavam uma sala inteira e pesavam toneladas para possuir uma capacidade de cálculo incrivelmente inferior à de um smartphone da atualidade. A mudança veio com a invenção do microcomputador, que só foi possível graças a invenção do microprocessador, pela Intel Corporation, que criou o Intel 4004 (TRÓIA, 2020). Os microcomputadores, ou computadores pessoais, que surgiram no final da década de 80, com o Apple I, Apple II e o IBM PC foram se popularizando e ficando cada vez mais potentes (TRÓIA, 2020).

A internet, conforme matéria do site Rocket Content (2020), foi criada como um projeto de defesa militar dos Estados Unidos, denominada Arpanet, teve sua primeira comunicação ponto a ponto em 1969 e nos anos seguintes foram conectados computadores ao redor dos Estados Unidos. Em 1989 surgiu a *World Wide Web* (rede mundial de computadores) e a rede foi passando a conectar computadores em escala global. Nos anos seguintes se deu a popularização e o uso comercial da internet, além da criação da famosa ferramenta de pesquisa Google, em 1997.

Se a internet e os computadores não escapam à tendência de serem subvertidas para o uso no crime, o que representa esse processo, sem dúvidas, é a figura do hacker ou cracker.

O termo hacker não surgiu como sinônimo de cibercriminoso. Conforme matéria do jornalista Mark Ward (2011) da BBC News Brasil, o termo hacker surgiu nos anos 50 no MIT (Instituto de Tecnologia de Massachusetts), onde os *hacks* eram sinônimos de brincadeiras. Essa primeira geração de hackers era marcada por jovens que queriam demonstrar suas habilidades e domínio sobre a tecnologia e a palavra hacker ainda não tinha um aspecto negativo.

De acordo com o documentário *The Secret History of Hacking*, de Ralph Lee (2001), entre os primeiros hackers estão os chamados piratas do telefone, hackers do telefone ou *phreakers* (*phone crackers* - crackers de telefone). Na década de 60, o norte americano John Thomas Draper, ou Capitão Crunch, como era conhecido, descobriu como burlar o sistema de telefonia dos Estados Unidos apenas emitindo sons na frequência de 2600 Hz e, com isso, criou um aparelho conhecido como caixa azul, ou cracker de telefone, que possibilitava ao usuário fazer ligações sem pagar.

Essa invenção ficou bem conhecida no Vale do Silício e inspirou Steve Wozniak, cofundador da Apple Inc. na sua jornada para construir o computador pessoal Apple I, em 1976 (LEE, 2001). Com o advento do computador pessoal e da popularização da internet, começaram a surgir os primeiros hackers de computador, que a princípio eram hackers como passatempo, brincadeira ou forma de demonstrar suas habilidades, mas quando a sociedade começou a fazer negócios pela internet, o foco mudou.

O documentário de Ralph Lee (2001) ainda fala sobre Kevin Mitnick, talvez um dos maiores hackers de todos os tempos, que fez fama nos anos 90 e chegou a ser considerado inimigo público nos Estados Unidos. Aos 17 anos, Kevin foi preso por obter indevidamente os manuais de uma empresa telefônica. Aos 18 anos, solto após cumprir pena de 1 ano, Kevin invadiu o sistema de defesa aérea dos Estados Unidos. Em 1988, Mitnick foi acusado e condenado por embaralhar os arquivos de uma empresa de tecnologia, causando-lhe prejuízos na cifra de 5 milhões de dólares. Após anos ludibriando as autoridades, Mitnick foi preso em 1995 e cumpriu pena de 5 anos de prisão, mais 3 anos de proibição de encostar em um computador.

Outro dos maiores hackers de todos tempos é o americano Kevin Poulsen (TERRA, c2021), que tinha expertise em controlar redes telefônicas e em 1990 controlou as linhas telefônicas de uma rádio de Los Angeles para garantir que seria a ligação ganhadora de um Porsche. A fraude foi descoberta e o hacker foi preso pelo FBI. Atualmente, Poulsen é jornalista e editor da revista Wired.

Assim como Mitnick e Poulsen, existem inúmeros outros hackers talentosos. A questão é que os hackers, na atualidade, direcionam seu talento de diferentes formas e boa parte emprega em atividades criminosas. Rik Ferguson (2011 *apud* WARD, 2011), pesquisador na área de segurança, fala que os hackers se dividem entre os “chapéus brancos”, aqueles que se direcionam para atividades lícitas e informam empresas e sites sobre falhas de segurança e os “chapéu pretos”, que são os cibercriminosos que tem o interesse de lucrar com roubos de informações confidenciais, extorsões e outras atividades ilícitas na internet. Há ainda, segundo Ferguson, os "chapéus cinza”, que são hackers por passatempo, fazem brincadeiras e causam pequenos danos. Além desses, mas não se encaixando claramente em nenhuma definição dessas, existem também os hacktivistas, ativistas hackers que atuam em prol de alguma causa.

Um grande exemplo de hacktivismo é o grupo Anonymous. O grupo é descentralizado e sem hierarquia, o que dificulta que seja combatido por autoridades. Desde 2003 a comunidade de hacktivistas conhecida como Anonymous protagonizou uma série de ataques contra sites sob a justificativa de defesa da liberdade de expressão. Em 2010 o grupo tirou do ar todos os sites de organizações que promovessem alguma sanção contra o site WikiLeaks. Dentre esses alvos estavam os sites da Visa e Mastercard, administradoras de cartões de crédito que bloquearam doações ao site WikiLeaks (EXAME, 2011).

No século XXI a atividade hacker deixou de ser uma brincadeira, não é mais para provar que é possível, como o Kevin Mitnick, ou para mudar o resultado de um sorteio como Kevin Poulsen, agora os são principalmente motivados por dinheiro. Diversas técnicas são empregadas para arrancar dinheiro de vítimas por meio da internet.

Dentre essas técnicas há o *phishing*, que é um ardil perpetrado por meio da internet para capturar informações das vítimas, como informações bancárias e de

cartão de crédito, e empregá-las em outras fraudes, por meio dessa técnica, as vítimas, ludibriadas, fornecem as informações voluntariamente. Não menos importante, existem também os *softwares*[1] maliciosos (*malwares*[2]) com as duas diversas variantes e espécies que são fabricados e distribuídos na internet em um ritmo impressionante.

Pesquisa realizada pela Kaspersky Lab (2013) identificou que mais 315 mil novos *softwares* maliciosos surgem todos os dias apenas para computadores e dispositivos móveis. O impacto desses *malwares* pode ser percebido no estudo publicado na revista Consumer Reports que revelou que o ataque de *malwares* custam 2,3 bilhões de dólares a consumidores americanos por ano. Pesquisa realizada pela BCD Travel (2019) revelou que fraudes em cartões de créditos custam 28 bilhões de dólares a empresas por ano. Uma matéria do programa Fantástico da Globo (2021) noticiou que 60 milhões de brasileiros já sofreram algum tipo de fraude financeira na internet, dentre propagandas enganosas, *phishing*, boletos falsos, clonagem de cartão de crédito e golpes por aplicativo de mensagem (clonagem de WhatsApp). Se a pequena cibercriminalidade só cresce, não passa despercebido que começam a surgir também grandes crimes dignos de filmes de Hollywood.

Em 2016, conforme matéria do jornalista Kim Zetter (2016), na revista Wired, hackers a serviço do governo da Coréia do Norte protagonizaram um dos maiores roubos da história quando subtraíram o incrível valor de 81 milhões de dólares do Banco de Bangladesh. De acordo com a matéria, os hackers tiveram acesso à rede interna da instituição financeira se utilizando da técnica de *phishing* e obtiveram credenciais da rede SWIFT *(Society for Worldwide Interbank Financial Telecommunication*), uma rede comunicação bancária internacional que processa transferências bancárias internacionais, e no dia 4 de fevereiro os hackers utilizaram as credenciais do Banco de Bangladesh para transferir 850 milhões de dólares do Federal Reserve Bank (FED) de Nova York para contas nas Filipinas, Sri Lanka e outras contas na Ásia. A fraude foi descoberta pelo FED de Nova York, que conseguiu bloquear a maior parte do valor, mas ainda assim 80.931.644 milhões de dólares foram pulverizados em contas na Ásia, resultando em um dos maiores assaltos a banco da história.

[1] Palavra da língua inglesa que significa programa de computador.
[2] Programas de computador maliciosos, voltados para danificar os sistemas das vítimas.

No momento atual, os hackers, ou crackers, já não são nenhuma novidade. O que há de novo é um mundo extremamente conectado, onde sistemas informáticos a tudo controlam e cada vez mais estes sistemas estão conectados à rede mundial de computadores. Esse processo tem nome, se chama internet das coisas (*Internet of things* – IOT) e corresponde ao processo de que cada vez mais eletrônicos e eletrodomésticos estão se tornando computadores e passando a se conectar com a internet. Foi o que aconteceu com os *smartphones, smart tvs,* geladeiras inteligentes e até os carros estão entrando passando a se conectar com a internet.

Se o resultado deste processo por um lado é a possibilidade sem precedentes de se coletar dados e processar dados do ambiente, por outro lado, mais um sistema conectado é mais um sistema vulnerável a ataques de hackers.

Nesse contexto, não é difícil imaginar golpes de criptografia, ou *ransomwares*[3], em seus eletrodomésticos e outros dispositivos que se tornaram conectados à internet. Um hacker pode lançar um ataque de *ransomware* contra sua geladeira inteligente e exigir um pagamento em criptomoedas não rastreáveis para liberar o funcionamento dela. O carro autônomo conectado à internet pode sofrer ataque semelhante ou se tornar uma arma mortal ao ter seus freios desabilitados por um hacker em pleno movimento. Não é demais lembrar que, se há um sistema, ele pode ser invadido e quanto mais conectado, mais vulnerável e ainda há muito mais a temer. Esse é o futuro mais visível da tecnologia que estará presente em muitas casas num futuro próximo e é também o futuro previsível dos cibercrimes.

No ano de 2008, na cidade de Lodz, na Polônia, como conta matéria de John Leyden (2008), no site britânico The Register, um jovem de apenas 14 anos utilizou um controle remoto modificado, com sistema infravermelho, para alterar a rota de um bonde, o que causou seu descarrilhamento. No acidente, 20 pessoas ficaram feridas, mas felizmente ninguém morreu.

[3] De acordo com a empresa de cibersegurança Karspersky Lab (c2021), Ransomware é um software malicioso que infecta seu computador e exibe mensagens exigindo o pagamento de uma taxa para fazer o sistema voltar a funcionar. Essa classe de malware é um esquema de lucro criminoso, que pode ser instalado por meio de links enganosos em uma mensagem de e-mail, mensagens instantâneas ou sites. Ele consegue bloquear a tela do computador ou criptografar com senha arquivos importantes predeterminados.

O episódio faz refletir o risco e o potencial destrutivo que sistemas informáticos podem representar para a sociedade, talvez um risco ainda não compreendido pelas autoridades estatais ao redor do mundo. No descarrilhamento do bonde na Polônia, o jovem utilizou um controle modificado e foi presencialmente até o trilho para causar o acidente, mas essa não é a única forma de causar um acidente dessa magnitude.

Muitos desses sistemas estão conectados à rede mundial de computadores e muitos outros estarão conectados no futuro. Isso significa dizer que um hacker mal intencionado pode causar um acidente de trem, de avião, de automóveis, entre outros, estando a milhares de quilômetros das vítimas.

Os sistemas que controlam esses trens, automóveis e tráfego aéreo são exemplos de sistemas críticos, tema que será melhor explorado no desenvolvimento desta pesquisa. De acordo com definição dada pela tecnóloga de sistemas Celina Ferreira Ribeiro (2010), os sistemas críticos são aqueles cuja falha pode ocasionar danos físicos, econômicos, ambientais e até acidentes com vítimas fatais.

Esses sistemas recebem esse nome porque controlam infraestruturas críticas, o que em outras palavras quer dizer que são infraestruturas capazes de causar verdadeiras catástrofes, de tamanhos variados, que pode ser de um pequeno acidente, com alguns feridos, até o caos generalizado em um país ou região. São exemplos dessas infraestruturas críticas, como já falado, a malha ferroviária, o tráfego aéreo, o sistema financeiro, os sistemas governamentais, dos tribunais, etc.

De acordo com Marc Goodman (2014, p. 27), especialista em cibersegurança, essas infraestruturas críticas estão cada vez mais se conectando à internet. O problema é que grande parte desses sistemas utilizam o sistema SCADA[4], um sistema que apresenta muitas falhas de segurança e, portanto, são mais vulneráveis do que se imagina.

Pode até parecer difícil de imaginar um sistema crítico sendo invadido, exceto pelo fato de que já aconteceu. Conforme matéria de Elinor Mills (2011) no site de tecnologia CNET, hackers invadiram os sistemas do departamento de água e esgoto de

[4] Sigla para *Supervisory Control And Data Acquisition*, que pode ser livremente traduzido como sistema de supervisão e aquisição de dados. Dito de forma resumida, se trata de um software de supervisão de processos ou sistemas.

South Houston, no Texas, Estados Unidos. Como explica Marc Goodman (2014, p. 27), o sistema que controla o tratamento de esgoto é um sistema SCADA, que mede e ajusta os produtos químicos responsáveis por tratar a água e revertê-la para consumo humano. Acontece que a medida errada de produtos químicos pode oferecer riscos à saúde humana e um hacker que invadir esse sistema SCADA, já dito inseguro, pode fazer isso acontecer. No ataque ao departamento de água e esgoto de South Houston o hacker, que de acordo com a matéria foi localizado na Rússia pelo seu endereço eletrônico, apenas ligou e desligou uma bomba, não causando mais danos. Apesar de não ter acontecido algo mais grave, o potencial já foi anunciado.

Não faltam exemplos de pequenas alterações em sistemas críticos que possam causar grandes danos. Os mesmos Estados Unidos, muitas vezes vítima de ciberataques, utilizou um ataque hacker para sabotar o programa nuclear iraniano. Consoante matéria do jornalista David E. Sanger (2012), no jornal The New York Times, o presidente dos Estados Unidos, à época, Barack Obama ordenou uma série de ciberataques ao programa nuclear iraniano. Para o ataque, foi utilizado um *worm*[5] desenvolvido pelas agências de inteligência dos Estados Unidos e de Israel, chamado de Stuxnet.

O Stuxnet é um *worm* de computador projetado especificamente para atacar sistemas SCADA. Com o objetivo de sabotar o programa nuclear iraniano, um pendrive infectado com o Stuxnet foi contrabandeado para o Irã e inserido nos sistemas da usina de enriquecimento de urânio da cidade de Natanz.

Marc Goodman (2014, p. 135), autor já citado nesta introdução, detalhou como foi o ataque à usina de Natanz. Em uma primeira fase o Stuxnet apenas atuou silenciosamente, captando informações para entender o funcionamento das centrífugas de enriquecimento de urânio e gravar os dados. Na segunda fase do ataque, o *worm* começou a manipular o funcionamento dos motores da centrífugas durante meses, fazendo os rotores falharem e o rendimento do urânio despencar. Enquanto isso acontecia, as telas da sala de controle da usina apontavam um funcionamento normal, pois o Stuxnet repassava informações pré-gravadas. Com esse ataque silencioso,

[5] O *worm* é um software malicioso, que é como um vírus, sendo que mais perigoso, visto que ele se multiplica sozinho pela rede de computadores, independente de qualquer ação da vítima.

enquanto centenas de centrífugas começavam a falhar, os iranianos não faziam ideia do que estava acontecendo.

O jornalista Kim Zetter (2014), da revista Wired, chamou o Stuxnet, responsável pelo ataque às centrífugas de Natanz, de primeira arma digital. Não é por acaso, sabendo que boa parte das infraestruturas críticas do mundo são controladas por sistemas SCADA, ter um *worm* como o Stuxnet à solta na rede mundial de computadores é um perigo global.

Embora muitos dos citados exemplos de ataques hackers tenham ocorrido em outros países, o Brasil também já foi alvo de ciberataques. No dia 3 de novembro de 2020 o Superior Tribunal de Justiça foi alvo de uma ataque hacker, o que fez o tribunal suspender os prazos processuais, visto que os sistemas do tribunal só voltaram a operar no dia 9 de novembro. De acordo com matéria do site Consultor Jurídico (2020), o hacker não teve acesso aos arquivos e processos guardados em nuvem, bloqueando apenas os dados dos computadores do tribunal.

Poucos dias depois, no dia 15 de novembro de 2020, em pleno primeiro turno das eleições municipais brasileiras, conforme matéria do UOL (2020), um grupo de hackers brasileiros e portugueses, liderados por um cidadão português realizaram um ataque de negação de serviço contra os servidores do TSE, com o objetivo de tirá-los do ar. O ataque foi neutralizado, mas, ainda assim, os resultados do primeiro turno atrasaram consideravelmente. Um hacker conhecido como Zambrius assumiu a autoria do ataque e se desconfia que a motivação tenha sido a de desacreditar o sistema eletrônico de votação brasileiro.

Em ambos os casos, as autoridades garantiram que não houve maiores danos e que dados de processos não foram perdidos e o resultado da eleição não foi maculado, contudo, mais uma vez, o potencial já foi demonstrado e certamente não será a última vez que esse tipo de ataque acontece.

É neste contexto histórico que se insere esta pesquisa. O presente trabalho tem o objetivo de analisar alguns ciberataques mais praticados na internet, confrontando-a com as leis penais referentes aos cibercrimes no Brasil, sob a luz dos princípios constitucionais aplicáveis e com auxílio de tratados internacionais existentes, em busca de lacunas que surgiram com a nova realidade tecnológica.

Os crimes informáticos, conforme Carla Rodrigues Araújo de Castro (2003 *apud* VELLOZO, 2015), são classificados em próprios e impróprios. Os crimes informáticos próprios são aqueles praticados contra sistemas informacionais em si, enquanto nos crimes informacionais impróprios são aqueles em que o sistema informáticos são meras ferramentas para atingir outro bem jurídico, como por exemplo, quando se pratica um estelionato por meio da internet. Para atingir o objetivo do trabalho, será analisada a Lei nº 12.737/2012, a lei delitos informáticos, além das demais leis penais que tipificam delitos informáticos, próprios ou impróprios.

Além disso, serão analisados os principais - e mais praticados - ilícitos informáticos próprios, ou seja, contra sistemas, praticados por meio digital, que podem ou não ser crimes no Brasil, a depender da tipificação.

O recorte se justifica pelo fato de que os ilícitos informáticos próprios possuem a tipificação penal mais limitada, enquanto os crimes informáticos impróprios já gozam de vasta tipificação.

É importante que se diga, contudo, que o presente trabalho não pretende esgotar todos os crimes ou condutas contrárias ao Direito praticadas na internet, uma vez que há uma vasta lista de crimes que não é possível tratar de todos eles no âmbito de um trabalho de conclusão de graduação.

Não escapa do conhecimento do autor que crimes contra a honra e contra a dignidade sexual de adultos, crianças e adolescentes são praticados em larga escala por meios informáticos. No entanto, esses não são delitos informáticos próprios e além disso, já gozam de boa tipificação.

É por isso, que o recorte de condutas analisadas pelo presente trabalho se volta para as que podem (ou não) serem consideradas crimes informáticos próprios. Isso porque a pesquisa como um todo inicia diante de uma suspeita de que boa parte destes não são tipificados como crime ou que existem lacunas que permitem que a conduta não se amolde aos tipos penais existentes. O que provavelmente ocorre por uma questão de desconsideração da realidade técnica dos cibercrimes.

Todavia, não se trata apenas de uma investigação quanto à previsão legal desses injustos como crime. Princípios constitucionais serão usados para analisar a legislação infraconstitucional em busca de lacunas.

Para completar este trabalho, serão analisados projetos de lei em tramitação no congresso nacional, para aferir a possibilidade de mudança na realidade encontrada com a pesquisa.

1.2 JUSTIFICATIVA

Inicialmente, é importante que se diga que o autor do presente trabalho integra o Grupo de Estudos de Direito Público da Internet e das Inovações Tecnológicas (GEDI) da UFRN e pesquisa cibercrimes, o que por si só, justifica o interesse por pesquisar nesta área.

Mas para além disso, a ideia para escrever sobre essa temática veio após a leitura do livro *Future Crimes*[6], do Marc Goodman, um especialista em cibersegurança segurança que trabalhou para o FBI e foi consultor da interpol. No livro, o autor proporciona um choque de realidade ao explorar tudo o que os cibercriminosos podem fazer nos dias atuais, com a tecnologia atual e como tudo ainda pode piorar quanto mais vivemos em um mundo mais conectado.

O livro *Future Crimes* não é um livro da literatura jurídica. É, na verdade, virado para a área tecnológica. Foi então que surgiu a ideia trazer os crimes do futuro do livro do Marc Goodman para o contexto jurídico pátrio, para analisar se o legislador braisleiro está ciente do potencial atual dos cibercrimes e se isso se reflete em uma legislação preparada para reprimir adequadamente, à luz de parâmetros constitucionais, essas práticas nocivas à sociedade.

De forma semelhante ao livro, este trabalho tem a intenção de chocar, é dizer, fazer o alerta quanto ao potencial destrutivo que a evolução tecnológica entregou nas mãos de hackers mal intencionados, enquanto analisa se esse problema se reflete na legislação penal referente aos cibercrimes no Brasil.

[6] O título do livro pode ser traduzido para o português simplesmente como Crimes do Futuro.

1.3 OBJETIVOS

1.3.1 Geral

Como foi adiantado na introdução, o objetivo principal da pesquisa é analisar a legislação penal brasileira referente a crimes cibernéticos para averiguar se ela é adequada para lidar com alguns dos mais praticados crimes essencialmente praticados por meios cibernéticos do presente e os que poderão ser comuns no futuro, com a dinâmica de surgimento de novas tecnologias, tendo em vista os princípios constitucionais que orientam o Direito Penal pátrio. Em outras palavras, o objetivo é analisar se as leis penais que tipificam cibercrimes no Brasil oferecem o suporte jurídico adequado para reprimir os delitos informáticos próprios de forma constitucionalmente adequada.

A hipótese lançada inicialmente é de que o Direito pátrio não dá o tratamento adequado aos crimes cibernéticos. Essa hipótese tem como premissa a noção de que a maioria das condutas antijurídicas praticadas na internet não estão devidamente tipificadas como crime na legislação penal brasileira e as que já têm tipificação como crime, não atendem aos princípios previstos na Constituição. Além disso, lança-se também a hipótese de que os crimes cibernéticos impõem novos desafios para a investigação de crimes dessa natureza e que há como adotar estratégias de prevenção, paralelamente à repressão penal dos crimes cibernéticos, para reduzir a sua ocorrência.

1.3.2 Específicos

Para alcançar-se esse objetivo principal, será necessário, como objetivos específicos: a) identificar as práticas nocivas na internet, contrárias ao direito e analisar se constituem ilícitos penais, ou seja, são tipificadas como crime no Brasil; b) analisar a legislação existente em relação aos crimes cibernéticos, à luz dos princípios constitucionais aplicáveis, como o princípio da individualização da pena (art. 5º, XLVI da CRFB), considerando as condutas nocivas identificadas e tipificadas como crime no

Brasil; c) analisar os problemas relacionados à investigação dos crimes cibernéticos; d) analisar projetos de lei em tramitação no congresso nacional relacionadas ao tema; e) por fim, analisar possíveis estratégias de prevenção aos crimes cibernéticos.

1.4 METODOLOGIA DA PESQUISA

Trata-se de subseção para delinear como a pesquisa será executada e quais procedimentos técnicos serão empregados.

Como já foi dito, analisar a legislação penal brasileira referente a crimes cibernéticos para averiguar se ela é adequada para lidar com os crimes cibernéticos do presente e do futuro, tendo em vista a realidade tecnológica e princípios constitucionais que orientam o Direito Penal pátrio.

Logo, é possível observar que se trata de uma pesquisa exploratória, pois nas palavras de Antônio Carlos Gil (2002, p. 42):

> Estas pesquisas têm como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a constituir hipóteses. Pode-se dizer que estas pesquisas têm como objetivo principal o aprimoramento de idéias ou a descoberta de intuições. Seu planejamento é, portanto, bastante flexível, de modo que possibilite a consideração dos mais variados aspectos relativos ao fato estudado.

Ademais, a pesquisa será operada por meio de levantamento bibliográfico - que como explica Antônio Carlos Gil (2002, p. 44) “é [a pesquisa] desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos” - tendo em vista que não há melhor forma de analisar o fenômeno tomando como base a ordem jurídica nacional. Será, portanto, analisado todo o material referente ao tema até então produzido, como livros e artigos científicos, além da letra da lei propriamente.

Além disso, o que também não pode deixar de ser mencionado é o método ou métodos que serão empregados.

Como explica Marina de Andrade Marconi e Eva Maria Lakatos (2003, p. 106):

> Método e métodos situam-se em níveis claramente distintos, no que se refere à sua inspiração filosófica, ao seu grau de abstração, à sua formalidade mais ou menos explicativa, à sua ação nas etapas mais ou menos concretas da investigação e ao momento em que se situam. Com uma contribuição às

> tentativas de fazer distinção entre os termos, diríamos que o método se caracteriza por uma abordagem mais ampla, em nível de abstração mais elevado, dos fenômenos da natureza e da sociedade. Assim teríamos, em primeiro lugar, o **método de abordagem** [método indutivo, dedutivo, hipotético-dedutivo e dialético]. (...) Por sua vez, os **métodos de procedimento** seriam etapas mais concretas da investigação, com formalidade mais restrita em termos de explicação geral dos fenômenos e menos abstratas. (grifo nosso).

Quanto ao método de abordagem, o presente trabalho utilizar-se-á de dois métodos: dedutivo (pois se pretende partir de conceitos gerais e aplicá-las às premissas levantadas) e o hipotético-dedutivo (vez que para identificar se há realmente lacunas legislativas, serão lançadas hipóteses, seguidas do processo de eliminação de erros ao apontar as falhas das hipóteses).

Pelo método dedutivo, como explica Marconi e Lakatos (2003, p. 91): “Se todas as premissas são verdadeiras, a conclusão deve ser verdadeira. Toda informação ou conteúdo fatual da conclusão já estava, pelo menos implicitamente, nas premissas”.

Isso quer dizer, se as leis penais seguem certos parâmetros definidos pela Constituição e as leis referentes aos cibercrimes são leis penais, elas devem seguir certos parâmetros definidos pela Constituição. A pesquisa busca investigar e definir que parâmetros são esses e analisar se as leis penais referentes aos crimes cibernéticos cumprem esse parâmetro. Diferente das ciências naturais, o Direito é uma ciência do *dever ser* e não do *ser*, logo, se premissas são verdadeiras, a conclusão deveria ser verdadeira, não quer dizer que é verdadeira. Assim, a conclusão do trabalho busca apontar como as leis deveriam ser, caso elas não já o sejam, o que faz parte do resultado da pesquisa.

O método hipotético-dedutivo de Karl Popper se resume da seguinte forma:

> O método científico parte de um problema (P1), ao qual se oferecesse uma espécie de solução provisória, uma teoria-tentativa (TT), passando-se depois a criticar a solução, com vista à eliminação do erro (EE) e, tal como no caso da dialética, esse processo se renovaria a si mesmo, dando surgimento a novos problemas (P2). (MARCONI; LAKATOS, 2003, p. 95).

Na pesquisa esse método será utilizado quando se quer saber se uma conduta é ou não abarcada por algum tipo penal no ordenamento jurídico braisleiro. Assim, quando se quer saber se um ataque cibernético é crime no Brasil, o primeiro passo é lançar a teoria-tentativa de que ele é tipificado pela lei de cibercrimes, passando a se criticar essa teoria, até chegar a uma conclusão.

Sabendo disso, a pesquisa se desenvolverá da seguinte forma:

a) Relato introdutório do assunto a ser tratado e delimitação do problema;
b) Desenvolvimento dos conceitos teóricos envolvidos;
c) Apresentação da legislação em vigor;
d) Levantamento das premissas, ou apresentação dos crimes cibernéticos;
e) Aplicação do método dedutivo, tendo como premissa maior a base teórica desenvolvida;
f) Aplicação do método hipotético-dedutivo;
g) Apresentação da(s) conclusão(ões).

2 EMBASAMENTO TEÓRICO

O Direito Penal é regido pelo princípio da legalidade, é dizer, não há crime sem uma lei anterior que tipifique a conduta como crime, ou o postulado da *nullum crimen nulla poena sine previa lege.* Tal princípio tem status constitucional, está previsto no art. 5º, XXXIX da Constituição da República Federativa do Brasil (CRFB), além de previsão infraconstitucional, no art. 1º do Código Penal (CP).

O princípio da legalidade, ou da reserva legal, como ensina o professor Cezar Roberto Bitencourt (2012, p. 24), é uma limitação ao poder punitivo estatal em prol do cidadão, fruto de um longo processo de conquistas. Conforme o autor (BITENCOURT, 2012, p. 24):

> Em termos bem esquemáticos, pode-se dizer que, pelo princípio da legalidade, a elaboração de normas incriminadoras é função exclusiva da lei, isto é, nenhum fato pode ser considerado crime e nenhuma pena criminal pode ser aplicada sem que antes da ocorrência desse fato exista uma lei definindo-o como crime e cominando-lhe a sanção correspondente. A lei deve definir com precisão e de forma cristalina a conduta proibida.

É por esse princípio que a lei deve prever com precisão e de forma clara a conduta que é proibida. Trata-se de uma questão de segurança jurídica, pois garante que ninguém será submetido a punição estatal, se não pelas regras previamente estabelecidas por lei (BITENCOURT, 2021, p. 24).

Assim sendo, ao se analisar crimes cibernéticos, ou condutas nocivas reprováveis da era digital e o seu reflexo no Direito é necessário, primeiramente, que se investigue se há um tipo penal incriminador que preveja a conduta como crime, em outras palavras, se o fato já é previsto como crime, pois não sendo, não há que se falar em crime, pelo princípio *nullum crimen nulla poena sine previa lege*.

Há de se lembrar que o crime, nas palavras de Assis Toledo (1994 apud GRECO, 2015, p. 195):

> Substancialmente, crime é um fato humano que lesa ou expõe a perigo bens jurídicos (jurídico-penais) protegidos. Essa definição é, porém, insuficiente para a dogmática penal, que necessita de outra mais analítica, apta a pôr à mostra o s aspectos essenciais ou os elementos estruturais do conceito de crime. E dentre as várias definições anal íticas que têm sido propostas por importantes penalistas, parece-nos mais aceitável a que considera as três notas fundamentais do fato-crime, a saber: ação típica (tipicidade), ilícita ou antijurídica (ilicitude) e culpável (culpabilidade). O crime, nessa concepção que adotamos, é, pois, ação típica, ilícita e culpável.

Dito isso, se o fato não for previsto por um tipo penal incriminador, falta-lhe já o primeiro elemento da teoria analítica do crime: a tipicidade. É por esse motivo que, na pesquisa, a primeira circunstância a ser analisada é se a conduta já é prevista como crime.

Até pouco tempo, a atipicidade era a situação dos atuais crimes informáticos próprios, visto que apenas crimes informáticos impróprios eram tipificados até 2012. O que mudou essa realidade foi a aprovação da Lei nº 12.737/2012, que inovou ao inserir no Direito Penal a figura do crime de invasão de dispositivos informáticos.

A Lei nº 12.737/2012 é um marco para a pesquisa na área dos cibercrimes e será melhor tratada no próximo tópico. Além disso, serão igualmente tratados princípios Constitucionais aplicáveis ao presente trabalho.

2.1 LEI DE CRIMES INFORMÁTICOS

A Lei nº 12.737/2012, que pode ser chamada de Lei de Crimes Informáticos, ou Lei Carolina Dieckmann, apelido que ganhou a lei em referência ao caso da atriz brasileira que teve fotos íntimas vazadas na internet por hackers em 2012. O episódio chamou atenção pelo fato de que a atividade dos hackers não recebia a devida atenção do Direito Penal, aliás, não fosse a extorsão praticada pelos hackers no caso Carolina Dieckmann, o fato poderia ter passado impune, visto que a invasão de dispositivos informáticos não era prevista como crime.

Nesse contexto histórico, foi aprovada em 30 de novembro de 2012 a Lei nº 12.737, que inseriu os arts. 154-A, 154-B, 266, §§1º e 2º e art. 298, parágrafo único no Código Penal (CP). A principal inovação que a lei trouxe foi, sem dúvidas, o art. 154-A, que tipificou o delito de invasão de dispositivos informáticos (art. 154-A, *caput* do CP) e a figura equiparada (art. 154-A, §1º do CP) que consiste no crime de venda e distribuição de programas de computador destinados à invasão de dispositivos informáticos.

A lei não se limitou a criar o tipo penal, mas também previu causas de aumento e uma forma qualificada do crime, o que, a primeira vista, atende ao princípio da

individualização da pena, princípio constitucional previsto no art. 5º, XLVI da CRFB e que será melhor discutido.

Pelo art. 154-B do CP, também incluído na Lei n 12.737/2012, os crimes do art. 154-A são de ação penal pública condicionada à representação, a não ser que tenha como vítima a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos. O art. 154-B, bem como as baixas penas previstas para os crimes do art. 154-A levam a concluir que o crime de invasão de dispositivos informáticos é um crime de baixo potencial ofensivo, nos termos do art. 61 da Lei nº 9099/95.

O art. 154-A não foi a única inovação importante da Lei Carolina Dieckmann, a alteração no art. 266 do CP criou o crime de interrupção de serviço telemático ou de informação de utilidade pública, ao qual prevê uma pena superior ao previsto para os crimes do art. 154-A.

Esse tipo penal merece menção visto que, embora possa ser praticado mesmo que não se utilizando de meios informáticos, prevê a primeira hipótese de pena diferenciada ao agente que invade sistemas críticos, tema a ser melhor discutido. Entretanto, como os núcleos do tipo falam em interromper, impedir ou dificultar o restabelecimento do serviço, pode-se concluir que caso o agente invada um sistema de crítico telemático ou de informação de utilidade pública e não pratique nenhuma dessas condutas (interromper, impedir ou dificultar o restabelecimento), não estará incurso no art. 266, §1º, mas no art. 154-A *caput* do Código Penal.

Com isso, vê-se que a Lei nº 12.737/2012 inovou e criou novos tipos penais que contemplam condutas antijurídicas praticadas por meio digitais, sendo a principal lei que tipifica cibercrimes. A pergunta que será o ponto de partida do trabalho é: a Lei nº 12.737/2012 é suficiente e, portanto, tipificou os principais injustos praticados na por meios digitais?

2.2 O PRINCÍPIO DA INDIVIDUALIZAÇÃO DA PENA

O art. 5º, XLVI da CRFB institui, no Direito Penal, o princípio da individualização da pena, princípio que rege a valoração das condutas desde o momento legislativo até

a dosimetria da pena aplicada pelo juiz na sentença condenatória, como explica professor Rogério Greco (2015, p. 119):

> Interpretando o texto constitucional, podemos concluir que o primeiro momento da chamada individualização da pena ocorre com a seleção feita pelo legislador, quando escolhe para fazer parte do pequeno âmbito de abrangência do Direito Penal aquelas condutas, positivas ou negativas, que atacam nossos bens mais importantes. Destarte, uma vez feita essa seleção, o legislador valora as condutas, cominando-lhes penas que variam de acordo com a importância do bem a ser tutelado.

O mencionado tem significativa importância para a análise que se pretende fazer no presente trabalho, pois se analisará, para além da tipificação dos injustos cibernéticos estudados, se a Lei de Crimes Informáticos individualiza devidamente as condutas, aplicando penas mais severas para os fatos cujas circunstâncias sejam mais graves, ou penas mais brandas para fatos menos reprováveis.

Esse princípio é muito importante para nortear o legislador brasileiro na aprovação de leis penais e está amplamente refletido na legislação, tanto no Código Penal, quanto nas Lei Penais Extravagantes.

A título de exemplo, os crimes de furto e roubo, previstos no arts. 155 e 157 do Código Penal, são, ambos, delitos praticados ao subtrair coisa alheia móvel de outrem, com a diferença que o crime de roubo se pratica mediante o uso de violência ou grave ameaça contra a vítima, essa circunstância faz com o crime de roubo seja punido de forma bem mais severa que o crime de furto. Mas não para por aí a individualização da pena nesses crimes patrimoniais, se o agente emprega uma arma branca para perpetuar a violência ou grave ameaça, a pena aumenta em um terço, pela previsão do inciso VII, §2º do art. 157 do CP. Se a violência ou grave ameaça se fizer por meio de uma arma de fogo o aumento é de dois terços da pena base (art. 157, §2º-A, I do CP).

Assim, vê-se que se o agente, ao praticar o crime de roubo com circunstâncias tais que aumentem o risco para a vida da vítima, como o uso de armas, o legislador, orientado pelo princípio da individualização da pena, entendeu que sua pena deve ser mais gravosa. Fica claro que as circunstâncias agravantes, causas de aumento, causas de diminuição e qualificadoras previstas no tipos penais, ou na parte geral do código existem em razão deste princípio, bem como que surgem quando o legislador, orientado por tal princípio e dando lógica ao sistema, impõe que a pena se mais branda ou mais grave que a prevista no *caput* sempre que as circunstâncias dos fatos sejam

mais ou menos reprováveis que a simplesmente prevista no *caput*, por motivos de risco, perigo, motivação, resultado, etc.

Tal princípio não é utilizado como parâmetro por acaso neste trabalho. Como já foi dito aqui, o art. 154-A do Código Penal prevê como crime o ato de invadir dispositivos informáticos alheios, contudo, será que o diploma penal prevê uma pena diferenciada para aqueles que invadem um sistema crítico, que como dito na introdução, pode oferecer riscos não dimensionáveis à sociedade? São perguntas como essa que a pesquisa busca responder.

2.3 O DIREITO À SEGURANÇA PÚBLICA

Como ensina o professor Walter Nunes da Silva Júnior (2015, p. 126), o Estado é uma criação humana que tem como finalidade básica a imposição de sua autoridade para garantir a manutenção da segurança pública, que é um dos pilares que possibilitam a convivência em sociedade.

A Constituição da República Federativa do Brasil usa a palavra segurança por diversas vezes para atribuir direitos ao cidadão, tomando como exemplos os termos segurança jurídica, social e pública, sempre como um sinônimo de garantia e proteção.

No caso da segurança pública, a Constituição atribui um capítulo exclusivamente para tratar do assunto e traz a seguinte redação no seu art. 144: “A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos”.

Deste modo, o art. 144 da CRFB revela um direito fundamental à segurança pública, cujo conteúdo é o dever de preservação da ordem pública e da incolumidade das pessoas e seu patrimônio por parte do Estado, o qual cumpre esse dever através dos seus órgãos de segurança pública discriminados no rol do art. 144. Como explica José Afonso da Silva (2006, p. 778), a segurança pública é a manutenção da ordem pública interna, que em outras palavras é a manutenção ou preservação de uma paz social que garanta a todos o gozo de seus direitos e exerçam suas atividades sem perturbação ilegítima de outrem. O autor ainda fala que na sua dinâmica, o direito à

segurança pública, é uma atividade de vigilância, prevenção e repressão de condutas delituosas (SILVA 2006, p. 778).

Assim, não restam dúvidas, que pelo direito à segurança pública, que atos ilícitos praticados pela internet, como todos os demais, devem ser alvos da atividade de vigilância, prevenção e repressão do poder público, uma vez que essas condutas maculam a incolumidade das pessoas e de seus patrimônios e perturbam a ordem pública.

Entretanto, como disse Afonso da Silva (2006, p. 778), as condutas alvo de vigilância, prevenção e repressão são as condutas delituosas, ou crimes. Como mencionado, o art. 1º do Código Penal estabelece que não há crime sem lei anterior que defina o fato como crime. Dessa forma, os contornos deste direito são definidos pelas leis penais infraconstitucionais, mas o âmbito de abrangência deste direito constitucional é mais amplo e não se limita a normas hierárquicas mentes inferiores.

Se, por exemplo, uma conduta nociva à incolumidade das pessoas, assim compreendidas com seus direitos da personalidade, ou do seu patrimônio e não há uma lei que tipifique a conduta como crime, temos uma lacuna, que não pode ser preenchida por qualquer recurso integrativo, se não pela edição de um tipo penal incriminador.

2.4 O PRINCÍPIO DA INTERVENÇÃO MÍNIMA

Como leciona o jurista alemão Claus Roxin (2006, p. 1), o Direito Penal é uma importante instituição social, que garante a paz e a convivência entre os cidadãos, mas ele submete as pessoas, sempre que suspeitos de crime, ainda que inocentes, medidas persecutórias graves do ponto de vista social e psíquico. O condenado, nesse ramo do Direito, é estigmatizado e pode ser excluído pela sociedade, o que não deveria existir em um país democrático. É nesse contexto, que Roxin (2006, p. 2) fala que o Direito Penal é um mal necessário, mas continua sendo um mal.

Tendo em vista esse peso das consequências que o Direito Penal impõe sobre os cidadãos, existe o princípio da subsidiariedade ou da intervenção mínima do Direito Penal. Nas palavras de Roxin (2006, p. 13):

> Este princípio fundamenta-se na ideia de que o direito penal, em virtude das suas acima expostas desvantagens, somente pode ser a *ultima ratio* da política social. Isso significa que só se deve cominar penas a comportamentos socialmente lesivos se a eliminação do distúrbio social não puder ser obtida através de meios extrapenais menos gravosos.

Não é porque a conduta de certa forma é nociva à paz social, que ela deva ser tipificada como crime. Neste sentido, há no ordenamento jurídico brasileiro o princípio da intervenção mínima do Direito Penal, que se traduz para o legislador pátrio da seguinte forma, nas palavras do Professor Rogério Greco (2015, p 97):

> O legislador, por meio de um critério político, que varia de acordo com o momento em que vive a sociedade, sempre que entender que os outros ramos do direito se revelem incapazes de proteger devidamente aqueles bens mais importantes para a s ociedade, seleciona, escolhe as condutas, positivas ou negativas, que deverão merecer a atenção do Direito Penal.

Assim, o princípio da intervenção mínima orienta que o Direito Penal deve ser o último ramo do Direito que o Estado deve lançar mão para tratar de condutas que lesam bens jurídicos, somente devendo este ramo agir quando a lesão for a um bem jurídico importante, e a lesão for muito grave, além disso, os outros ramos do direito devem ser ineficazes na resposta a essa conduta. Além disso, a proibição da conduta com consequências penais deve ser necessária para a manutenção da paz social (ROXIN, 2006, p. 12).

Esse princípio não está invocado por acaso neste trabalho, pois as condutas a serem elencadas, caso não sejam ainda previstas como crime, devem ser analisadas à luz deste princípio para responder se tal conduta deveria ser criminalizada.

2.5 O PRINCÍPIO DA PROPORCIONALIDADE E A VEDAÇÃO À PROTEÇÃO DEFICIENTE

Na antiguidade, bem como na idade média, não tinha muita força a ideia de proporcionalidade entre crime e castigo, essa ideia veio surgir no período do iluminismo, sobretudo tendo como expoente o iluminista italiano Cesare Beccaria, que viveu no século XVIII. Beccaria (1764, p. 44), em “Dos delitos e das penas”, fala da necessidade de haver uma proporcionalidade entre os delitos praticados e as penas impostas para se prevenir que os homens pratiquem os crimes mais graves, ao mesmo

tempo que se evite a impunidade. No livro, Beccaria (1764, p. 44) dá um exemplo interessante:

> Se dois crimes que atingem desigualmente a sociedade recebem o mesmo castigo, o homem inclinado ao crime, não tendo que temer uma pena maior para o crime mais monstruoso, decidir-se-á mais facilmente pelo delito que lhe seja mais vantajosos; e a distribuição desigual das penas produzirá a contradição, tão notória quando freqüente, de que as leis terão de punir os crimes que tiveram feito nascer. Se se estabelece um mesmo castigo, a pena de morte por exemplo, para quem mata um faisão e para quem mata um homem ou falsifica um escrito importante, em breve não se fará mais nenhuma diferença entre esses delitos.

O princípio da proporcionalidade, para parte da doutrina, trata-se de um princípio implícito, não previsto expressamente na Constituição, mas que deriva necessariamente de outros princípios constitucionais importantes (GRECO, 2015, p. 126). Para outros doutrinadores, com influência do pensamento jurídico alemão, a proporcionalidade é, na verdade, um critério para analisar a constitucionalidade de atos infraconstitucionais (DIMITRI; MARTINS, 2014, P. 189). Gilmar Ferreira Mendes (2004, p. 47) fala que no Direito Alemão, o princípio da proporcionalidade ou da proibição do excesso, tem natureza de norma constitucional não escrita derivada do Estado de Direito e a sua violação se trata de um excesso praticado pelo Poder Legislativo.

Esse princípio, quando aplicado no Direito Penal tem relação íntima com o comentado princípio da individualização da pena, pois nas palavras do jurista Alberto Silva Franco (2000, p. 67):

> O princípio da proporcionalidade exige que se faça um juízo de ponderação sobre a relação existente entre o bem que é lesionado ou posto em perigo (gravidade do fato) e o bem de que pode alguém ser privado (gravidade da pena). Toda vez que, nessa relação, houver um desequilíbrio acentuado, estabelece-se, em consequência, inaceitável desproporção. O princípio da proporcionalidade rechaça, portanto, o estabelecimento de combinações legais (proporcionalidade em abstrato) e a imposição de penas (proporcionalidade em concreto) que careçam de relação valorativa com o fato cometido considerado em seu significado global. Tem, em consequência, um duplo destinatário: o poder legislativo (que tem de estabelecer penas proporcionadas, e m abstrato, à gravidade do delito) e o juiz (as penas que os juízes impõem ao autor do delito têm de ser proporcionadas à sua concreta gravidade).

Como foi dito, esse princípio tem clara ligação com o princípio da individualização das penas, esse positivado (art. 5º, XLVI da CRFB), mas, deve-se dizer, guarda ligação com princípio da intervenção mínima, pois ambos são desdobramentos lógicos do princípio da proporcionalidade.

O princípio da proporcionalidade, quando aplicado ao Direito Penal, gera ainda duas conclusões lógicas imediatas direcionadas ao legislador na hora de aprovar leis penais: a proibição do excesso e a proibição à proteção deficiente (GRECO, 2015, p. 127).

Rogério Greco (2015, p. 127) dá uma luz neste tópico, ao explicar que a proibição do excesso se dirige ao legislador e ao julgador, protegendo o direito à liberdade dos cidadãos, para evitar, no caso legislativo, que sejam punidos desnecessariamente condutas que não tem a gravidade necessária para se tornarem penalmente relevantes ou para evitar que se puna excessivamente uma conduta penalmente relevante. Como se pode ver, a proibição do excesso tem ligação direta com os princípios da intervenção mínima e da individualização da pena.

O autor explica ainda a proibição da proteção deficiente, ao dizer que se não pode haver punição em excesso, pela mesma lógica também não pode haver deficiência na proteção de um direito fundamental, o que pode ocorrer pela falta de figuras típicas, a exclusão dessas, cominação de penas mais brandas que o suficiente para reprimir a conduta típica ou pela aplicação de benefícios que beneficiem indevidas os responsáveis (GRECO, 2015, p. 127).

O jurista gaúcho Lênio Streck (2004) resume de forma brilhante os desdobramentos do princípio da proporcionalidade no Direito Penal:

> Trata-se de entender, assim, que a proporcionalidade possui uma dupla face: de proteção positiva de proteção de omissões estatais. Ou seja, a inconstitucionalidade pode ser decorrente de excesso do Estado, caso em que determinado ato é desarrazoado, resultando desproporcional o resultado do sopesamento (Abwägung) entre fins e meios; de outro, a inconstitucionalidade pode advir de proteção insuficiente de um direito fundamental-social, como ocorre quando o Estado abre mão do uso de determinadas sanções penais ou administrativas para proteger determinados bens jurídicos. Este duplo viés do princípio da proporcionalidade decorre da necessária vinculação de todos os atos estatais à materialidade da Constituição, e que tem como consequência a sensível diminuição da discricionariedade (liberdade de conformação) do legislador.

Assim, o princípio da proporcionalidade é suma importância para o que se pretende analisar no trabalho, sobretudo pelo seu desdobramento da proibição à proteção deficiente, uma vez que os a legislação penal brasileira referente aos crimes cibernéticos serão analisados sob essa ótica ao serem confrontados com as principais condutas nocivas praticadas por meios informáticos.

3 OS CIBERCRIMES E AS DEFICIÊNCIAS DA LEGISLAÇÃO PENAL BRASILEIRA

Após a devida discussão acerca das bases teóricas que orientam a pesquisa e a guiam para os seus objetivos, cabe agora analisar as condutas nocivas praticadas por meios informáticos e confrontá-los com a legislação penal em vigor, com o auxílio dos princípios que foram elencados no embasamento teórico.

3.1 A INVASÃO DE SISTEMAS OU DISPOSITIVOS INFORMÁTICOS

Invadir, conforme definição do dicionário Michaelis (2021), significa entrar à força, penetrar hostilmente em determinado lugar, apoderar-se, conquistar, ou tomar. Invadir um sistema informático, portanto, é o ato de forçar nesse sistema, ou se apoderar dele, geralmente ultrapassando algum sistema de segurança, contra a vontade do proprietário do sistema.

Não há apenas uma forma de invadir um sistema, mas o meio mais utilizado é algum programa malicioso que reproduz algumas linhas de código e consegue subverter o sistema da vítima à vontade do invasor.

Matéria de Jonathan Strickland (2007) no site HowStuffWorks explica algumas estratégias utilizadas: a) roubo de senhas para acessar o sistema através programas, como os *Log Keystrokes*[7]*,* instalados na máquina da vítima, que registram todas as senhas utilizadas pelo usuário e as enviam para o invasor, ou simplesmente pela força bruta, com programas que tentam senhas até conseguir acertar; b) o uso de vírus, *worms* e outros *malwares*, que se infiltram nos sistemas e causam uma série de problemas; e c) acessar o sistema por meio de *backdoors*[8], que basicamente são portas desprotegidas no computador da vítima, geralmente uma vulnerabilidade deixada por um programa malicioso.

Como já foi dito, desde de 2012, com a edição da Lei nº 12.737, a invasão de dispositivos informáticos é crime tipificado no Brasil. O art. 154-A do CP atribui pena de 3 meses a 1 ano de detenção para quem invadir dispositivo informático mediante violação de mecanismo de segurança ou sem a devida permissão do titular do

[7] Os Log Keystrokes são programas maliciosos que, uma vez instalados no computador, gravam todas as teclas pressionadas (KASPERSKY, c2021).
[8] Pode ser livremente traduzido para o português como porta de trás, mas no âmbito da tecnologia da informação esse termo significa uma vulnerabilidade que permite que um invasor burle os sistemas de segurança da máquina invadida (POSEY, Brian, 2021).

dispositivo, com a intenção obter, adulterar ou destruir dados ou para nele instalar vulnerabilidades.

Assim, a invasão de dispositivos informáticos por qualquer dos meios acima descritos está tipificada no art. 154-A do CP, seja pelo fato do invasor violar dispositivo de segurança (senhas), seja pela falta de autorização do proprietário e com a finalidade especial de agir obter, adulterar ou destruir dados (roubo de senhas, informações bancárias, mídias, etc.) e instalar vulnerabilidades (como a abertura de *backdoors*), o que geralmente é a finalidade de um hacker malicioso.

Pela grande importância para o presente trabalho, não é demais esclarecer o termo “dispositivos informáticos” e nas palavras de Rogério Sanches Cunha (2016, p. 344):

> Por dispositivo informático entende-se qualquer aparelho (instrumento eletrônico) com capacidade de armazenar e processar automaticamente informações/programas (notebook, netbook, tablet, Ipad, Iphone, Smartphone, pendrive etc.). Importante observar ser indiferente o fato de o dispositivo estar ou não conectado à rede interna ou externa de computadores (intranet ou internet).

A definição é muito útil e oportuna para demonstrar que a proteção dada pelo art. 154-A do CP, que tipifica o crime de invasão de dispositivos informáticos está muito além dos computadores e *smartphones*, mas abarca qualquer dispositivo eletrônico capaz de processar informações (composto por circuitos integrados). Também foi oportuna a nomenclatura adotada pelo legislador, uma vez que abrangente o suficiente para prever evoluções tecnológicas. Vale dizer, se o legislador tivesse fechado demais o tipo penal, utilizando as palavras computador, celular, etc. estaria condenado o tipo penal a ficar ultrapassado com o surgimento de novos equipamentos eletrônicos que podem igualmente sofrer invasão, expondo os bens juridicamente protegidos (a liberdade individual e o direito à intimidade, além da proteção da inviolabilidade dos dados e informações existentes em dispositivo informático) a uma deficiência de proteção.

Em atenção ao princípio da individualização da pena e da proporcionalidade, pelo menos no que diz respeito a dispositivos informáticos não críticos, o §2º do art. 154-A do CP prevê aumento de pena se da invasão resultar prejuízo econômico. Além disso, o §3º do mesmo artigo prevê uma qualificadora se da invasão resultar a

obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido, além de um aumento de pena se essas informações forem repassada para terceiros (art. 154-A, §4º do CP). Para mais, se a vítima for presidente do STF, chefe do poder executivo ou presidente da casa legislativa de qualquer esfera da república, a pena é aumentada de um terço até metade.

Com isso, pode-se dizer que a invasão de dispositivos informáticos é crime, tipificado no Código Penal, além de atender, pelo menos no caso da invasão de sistemas informáticos que não oferecem maiores riscos à sociedade, a critérios de proporcionalidade e de individualização da pena, prevendo penas diferenciadas de acordo as circunstâncias do fato (consequências da conduta ou características das vítimas da invasão).

3.1.1 A invasão de sistemas críticos

Os sistemas críticos, como explicado na introdução do trabalho, são aqueles cuja falha pode ocasionar danos físicos, econômicos, ambientais e até acidentes com vítimas fatais. Com isso dito, é possível perceber que esses sistemas estão por todos os lugares.

Eles, inclusive, já foram introduzidos no começo do trabalho, mas vale retomar dizendo que são exemplos de sistemas críticos os sistemas que controlam tráfego aéreo, sistemas que controlam barragens e usinas, sistemas militares, sistemas de distribuição de energia elétrica, de telecomunicações, sistemas financeiros, etc.

Não é difícil de perceber que esses exemplos mencionados – que, vale dizer, não esgotam nem de perto os tipos de sistemas que podem ser classificados como críticos – têm algo em comum: uma capacidade de causar grandes estragos se falharem ou apresentarem mal funcionamento. Por exemplo, não é difícil de imaginar que um *worm* como o Stuxnet, que sabotou o projeto nuclear iraniano, se instale no sistema que controla uma usina nuclear e altere seus parâmetros de controle a ponto de causar um acidente aos moldes da explosão do reator de Chernobyl.

Com esse exemplo, dá para entender os riscos que esses sistemas críticos representam para a sociedade, sobretudo se considerarmos a possibilidade de serem subvertidos por hackers mal intencionados. É possível até dizer que são uma grande oportunidade para hackers protagonizarem o máximo potencial destrutivo e lesivo que a tecnologia moderna pode oferecer, como ocorreu no assalto virtual de 81 milhões de dólares ao banco de Bangladesh, sendo também uma grande oportunidade para ciberterroristas, além de cibercriminosos que querem extorquir pessoas, empresas e governos sob a ameaça de lançar o caos através de sistemas críticos.

Com isso, não é difícil de imaginar que num futuro próximo, hackers realizarão ataques contra sistemas críticos como um carro autônomo e exigir da vítima um resgate em criptomoedas não rastreáveis para que seus freios não sejam desabilitados em pleno movimento.

Apesar da classificação adotada, os sistemas críticos nada mais são do que dispositivos informáticos que trabalham com graves riscos e por serem sistemas informáticos, a invasão destes configura, em tese, o crime previsto no art. 154-A do CP, desde que haja violação de mecanismos de segurança ou acesso não autorizado, o que certamente ocorrerá nesses casos, além do dolo especial dirigido a obter, adulterar ou excluir dados, ou instalar vulnerabilidades. Um ataque hacker dessa natureza geralmente tem uma dessas intenções.

Assim, a invasão de sistemas críticos não deixa de ser tipificada como crime pela legislação penal, mas também não quer dizer que a legislação seja satisfatória.

Como já foi tratado, a legislação penal infraconstitucional deve obediência ao princípio da proporcionalidade e da individuação da pena (art. 5º, XLVI da CRFB), o que se traduz em penas diferenciadas de acordo com as circunstâncias especiais do fato.

Pois bem, uma tecla bem batida neste trabalho é que a invasão de sistemas críticos oferece um risco muito superior a toda sociedade, quando comparado a um sistema de um dispositivo informático de uma pessoa comum, cujos riscos de dano geralmente se limitam a esfera pessoal. Assim, por obrigação expressa nos princípios constitucionais mencionados, o artigo deveria prever um aumento de pena ou um agravante para aquele que invade sistemas críticos, o que não ocorre.

A circunstância especial de risco maior é utilizada em outros tipos penais do Código Penal para agravar a pena do *caput*, então não seria algo inédito. O crime de incêndio, previsto no art. 250 do CP, define em seu §1º, II que a pena prevista no *caput* aumenta de um terço, dentre outras circunstâncias, se o incêndio for provocado em: a) casa habitada ou destinada a habitação; b) em depósito de explosivos, combustível ou inflamável; c) em poço petrolífero ou galeria de mineração.

Rogério Sanches Cunha (2016, p. 559), comentando sobre o agravante de incêndio provocado em depósito de explosivo, combustível ou inflamável, fala que "a majoração é justificada em razão da maior (e evidente) periculosidade a que a ação expõe a incolumidade pública". Mas para além desta alínea, nas demais citadas o risco maior a vidas humanas e outros danos também é a razão por trás do agravamento da pena.

Sendo assim, é uma questão de coerência sistêmica e de atenção aos princípios da proporcionalidade e da individualização da pena que o invasor de sistemas crítica receba uma repressão maior que o invasor de dispositivos informáticos mais simples.

Nesse sentido, há um dispositivo no Código Penal, também inserido pela Lei nº 12.737/2012, que atende parcialmente a essa obrigação legislativa, o art. 266, §1º e §2º do CP. Que tipificou a conduta de interromper, perturbar, impedir ou dificultar o restabelecimento de serviço telemático ou de informação de utilidade pública.

O crime previsto no art. 266 já existia, mas a Lei nº 12.737/2012 adicionou seus §§1º e 2º. Com essa inovação passou a prever uma possibilidade de pena diferenciada – notavelmente mais grave – para aqueles que invadem sistemas críticos. No entanto, há dois problemas envolvidos.

O primeiro problema é que a abrangência do tipo penal se limita aos sistemas críticos envolvidos nos serviços telemáticos (serviços de transmissão de dados pela rede, como a internet) ou de informação de utilidade pública. Com isso, para além do problema gerado por não dar uma definição do que seria um serviço de utilidade pública, exclui de plano uma ampla gama de sistemas críticos que não estão envolvidos em serviços dessa natureza. Se o sistema crítico invadido não está empregado em um serviço telemático ou de informação de utilidade pública, o ato de

invadi-lo incorrerá, em tese, no art. 154-A *caput* do CP, tendo pena mais branda e não havendo a aludida individualização.

O segundo problema é que o tipo penal não prevê a invasão do sistema como um dos seus núcleos, mas a interrupção, o impedimento ou a dificultação do restabelecimento do serviço. Assim, se o hacker invade um sistema crítico envolvido em serviço telemático ou de informação de utilidade pública, mas não interrompe o serviço, ou se o serviço já tiver sido interrompido, não impede-lhe ou dificulta-lhe o restabelecimento, ainda que instale vulnerabilidades para fazê-lo posteriormente, o hacker incorrerá no art. 154-A *caput* e não no art. 266, §1º do CP, com pena mais branda e sem a individualização da pena que o sistema determinaria para esse tipo de circunstância.

Deste modo, embora o art. 266 do Código Penal preveja algumas hipóteses em que a invasão de sistemas críticos será punida de forma mais gravosa que a invasão de sistemas comuns, mas como visto, essas hipóteses são muito limitadas e se pode concluir que, em atenção aos princípios da proporcionalidade e da individualização da pena, a legislação penal é lacunosa em relação aos sistemas críticos, havendo uma desproporcionalidade na repressão do crime nessas circunstâncias, pela deficiência na proteção ao bem jurídico.

3.2 FABRICAÇÃO E DISSEMINAÇÃO DE MALWARES

Malwares são programas maliciosos que causam uma série de problemas em equipamentos computacionais, podendo danificar o sistema, roubar informações, apagar informações, etc. Joseph Regan (2019), em matéria no site da empresa de cibersegurança AVG, resume de forma interessante o que é um malware:

> O termo malware se refere a software que danifica dispositivos, rouba dados e causa o caos. Existem muitos tipos de malware, vírus, cavalos de Troia, spyware, ransomware, etc. (...) Frequentemente um malware é desenvolvido por times de hackers que, na maioria das vezes, estão apenas buscando uma forma de fazer dinheiro, seja pela proliferação do próprio malware ou por meio de leilão na Dark Web. De qualquer forma, podem haver outras razões para a criação de malwares. Esses softwares maliciosos podem ser usados como ferramentas de protesto, uma forma para testar a segurança de uma rede ou até mesmo como armas de guerra entre governos.

Assim, o *malware* é uma classificação para programas criados com propósitos danosos e se dividem vários subtipos de *malwares*, como os vírus, que geralmente precisam ser executados pela vítima e que geralmente não sabem que estão executando um vírus. Como um vírus biológico, eles infectam um sistema, se replicam, corrompem arquivos, entre outras ações danosas.

Os cavalos de tróia (*trojan horse*) são programas maliciosos que se escondem em programas legítimos para serem executados juntos com o programa legítimo. Suas ações são parecidas com a do vírus, mas são comumente usados para deixar vulnerabilidades, como um *backdoor*. Outro software malicioso de ampla utilidade para cibercriminosos são os *spywares* que são *malwares* que espionam suas ações na máquina, gravando senhas, cartões de crédito, etc.

Existem ainda os *worms, ransomwares* e *botnets*[9]. Os *worms* são como os vírus, mas eles não precisam do comando executar para realizar suas ações lesivas e se espalham com muita velocidade, basta lembrar do exemplo do *worm* Stuxnet.

Para completar a lista de *malwares*, podemos citar os *ransomwares*, que são programas maliciosos usados para ataque de criptografia, eles geralmente agem criptografando as informações presentes na máquina, ou ameaçando apagá-las, em mensagens que exigem um resgate para evitar o transtorno de perder dados importantes.

Por muito tempo os hackers produziram, espalharam e realizaram ataques com *malwares* com total tranquilidade e esse fato se quer era crime no Brasil. Essa realidade mudou, pelo menos no âmbito legislativo, a lei apelidada de Lei Carolina Dieckmann (Lei nº 12.737/2012) trouxe o §1º do art. 154-A do Código Penal, que traz a seguinte redação: “§1º na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput”.

Com isso, aqueles que produzem, oferecem, distribuem, vendem ou difundem softwares maliciosos que tem a função de invadir outros dispositivos informáticos, ou

[9] Os botnets, palavra formada pela junção dos termos em inglês *bot* e network, que significam em português, respectivamente, robô e rede, são máquinas infectadas por malwares que permitem que um terceiro as controle remotamente (AVAST, c2021).

seja, que produzem e disseminam vírus, *worms, trojans, spywares* incorrem na pena definida no art. 154-A *caput* do CP.

A inovação foi muito oportuna e necessária, haja vista os *malwares* são a principal ferramenta utilizada por cibercriminosos e dessa forma o legislador buscou punir aquele que participa de alguma forma do crime de invasão de dispositivos informáticos. Fazendo uma rápida comparação, é como se o §1º do art. 154-A do CP tivesse punindo os traficantes de armas, visto que os *malwares* são verdadeiras armas cibernéticas. É como foi dito por Joseph Regan (2019), os *malwares* são produzidos por equipes de hackers que formam verdadeiras organizações cibercriminosas e a maioria dos pequenos cibercriminosos não alteram uma linha de código, apenas adquirem esses *malwares* em cantos obscuros da internet para realizar os mais diversos ataques.

Desta forma, a fabricação e disseminação de *malwares* é crime no Brasil e também cumpre os demais quesitos da pesquisa, pois não necessita de diferenciadores de pena para individualização, uma vez que a conduta não se torna mais grave a depender do programa que foi fabricado ou disseminado, se um vírus ou um trojan, todos são programas maliciosos, a forma como são utilizados é que podem adicionar circunstância penalmente relevantes ao fato.

3.3 PHISHING

O *phishing* é um ardil virtual para enganar as vítimas e fazê-las entregar informações importantes voluntariamente. Com essas informações, os praticantes de *phishing* realizam outras fraudes, como fraudes de cartão de crédito, empréstimos fraudulentos, etc. Ivan Belsic (2020), em matéria no site da empresa de cibersegurança AVAST resume bem do que se trata o *phishing*:

> O phishing é um dos golpes mais antigos e conhecidos da internet. Podemos definir phishing como qualquer tipo de fraude por meios de telecomunicação, que usa truques de engenharia social para obter dados privados das vítimas. (...) Por isso phishing recebe seu nome: O cibercriminoso vai “pescar” (em inglês, “fishing”) com uma atraente “isca” para fisgar as vítimas do vasto “oceano” dos usuários da internet. O ph em "phishing" vem de “phreaking de telefone” que surgiu em meados de 1900, no qual os “phreaks”, ou seja, entusiastas, faziam experimentos com as redes de telecomunicações para descobrir como elas funcionavam. Phreaking + fishing = phishing.

Assim, o *phishing* é um meio empregado pelos cibercriminosos para obter dados das vítimas, geralmente dados que possam ser usados para praticar fraudes financeiras, sem a necessidade de utilizar uma malware, visto que a vítima ludibriada entrega os dados voluntariamente.

Pode-se pensar que o *phishing* atraia a aplicação do art. 154-A do CP, mas ocorre que nesta técnica não há invasão de dispositivo que atraia a aplicação do art. 154-A do CP, uma vez que, como dito, o cibercriminoso nessa modalidade não invade a máquina de vítima, ele solicita as informações por mensagem ou outros meios, a vítima as envia. Funciona da seguinte forma: o golpista envia uma mensagem (pode ser por SMS, *e-mail*, pelas redes sociais, páginas fraudulentas na internet, etc.) se passando por pessoa de confiança da vítima, gerente de banco, empresa que a vítima seja cliente, etc. para solicitar informações que a vítima envia por confiar no aparente interlocutor, mas acaba enviando para um cibercriminoso que utiliza seus dados para realizar compras fraudulentas no seu cartão de crédito ou realizar outras fraudes de ordem financeira.

Não havendo aplicação por nenhum tipo trazido pela Lei Carolina Dieckmann (Lei nº 12.737/2012), resta saber se o *phishing* poderia se encaixar no crime previsto no art. 171 do Código Penal, o estelionato. O art. 171 do CP fala que é crime “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”.

À primeira vista, parece solucionado, uma vez que o *phishing* é uma prática onde se utiliza um meio fraudulento para obter alguma vantagem em informações da vítima. No entanto, o problema reside na natureza dessa vantagem indevida obtida para caracterizar o crime de estelionato. Nesse ponto, não há um consenso na doutrina. Na visão do penalista Heleno Cláudio Fragoso (1958 *apud* CUNHA, 2016, p. 342), “por vantagem ilícita deve entender-se qualquer utilidade ou proveito de ordem patrimonial, que o agente venha a ter em detrimento do sujeito passivo sem que ocorra justificação legal”.

O professor César Roberto Bitencourt (entre 2003 e 2020 *apud* CUNHA, 2016**,** p. 342) tem outra visão:

> O argumento de que a natureza econômica da vantagem é necessária, pelo fato de o estelionato estar localizado no Título que disciplina os crimes contra o patrimônio, além de inconsistente, é equivocado. Uma coisa não tem nada que ver com a outra: os crimes contra o patrimônio protegem a inviolabilidade patrimonial da sociedade em geral e da vítima em particular, o que não se confunde com a vantagem ilícita conseguida pelo agente. Por isso, não é a vantagem obtida que deve ter natureza econômica; o prejuízo sofrido pela vítima é que deve ter essa qualidade.

A vantagem obtida por meio de *phishing* certamente é ilícita, mas nem sempre tem conteúdo patrimonial. Como dito por Bitencourt, o crime de estelionato protege a inviolabilidade patrimonial, ou seja, o bem jurídico protegido é o direito de propriedade.

O *phishing*, embora seja o que geralmente acontece, não necessariamente tem o objetivo de obter vantagem patrimonial e ainda quando tem, essa vantagem é obtida por conduta posterior, que pode ser propriamente tipificada no estelionato, como a compra fraudulenta por meio de cartão de crédito ou a realização de empréstimo financeiro no nome da vítima.

Desta forma, percebe-se que o *phishing* não lesiona diretamente o patrimônio da vítima, se trata de uma lesão direta aos direitos fundamentais a inviolabilidade da intimidade e vida privada (art. 5º, X da CRFB) e ao sigilo de dados (art. 5º, XII da CRFB), os mesmos bens jurídicos protegidos pelo art. 154-A do Código Penal.

Sendo assim, a prática de *phishing* não se amolda ao art. 171 do CP, visto que a vantagem ilícita obtida com a prática não tem conteúdo patrimonial, tampouco se amolda ao art. 154-A do CP, visto que não se trata de uma invasão de dispositivo informático. Deste modo, não havendo nenhum outro tipo penal que tipifique a conduta de obter informações privadas por meios fraudulentos, o *phishing* é atípico no Brasil.

Com isso, nota-se que há uma lacuna na legislação penal brasileira, uma vez que a conduta de se obter informações por meio de invasão a força de dispositivo informático é crime tipificado no art. 154-A do CP, mas o *phishing* é um fato atípico, mesmo que o bem jurídico lesado seja o mesmo e o resultado da conduta seja parecido. Há, portanto, uma desproporcionalidade por deficiência na proteção do bem jurídico mencionado. Ademais, a prática do *phishing* supera a barreira do princípio da intervenção mínima do Direito Penal e merece atenção deste ramo do direito, uma vez que o *phishing* é notavelmente contrário ao direito e lesa na mesma intensidade os

mesmos bens jurídicos protegidos no art. 154-A do CP (a liberdade individual e o direito à intimidade, além da proteção da inviolabilidade dos dados).

3.4 VIOLAÇÃO E USO INDEVIDO DE DADOS PESSOAIS

A proteção de dados pessoais é o tema mais quente do momento para os interessados em Direito e tecnologia, sobretudo após o advento da nova Lei Geral de Proteção de Dados Pessoais (LGPD), ou Lei nº 13.709/2018, e a criação da Autoridade Nacional de Proteção de Dados (ANPD), além do Regulamento Geral de Proteção de Dados Europeu, de 2016.

Felizmente, a própria LGPD traz a definição do que são os dados pessoais, no seu art. 5º "para os fins desta Lei, considera-se: I – dado pessoal: informação relacionada a pessoa natural identificada ou identificável". Ademais, a LGPD, logo no seu primeiro artigo, diz que tem o objetivo de "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural".

Assim, a proteção de dados pessoais é uma implicação da proteção dada pelo ordenamento jurídico aos direitos da personalidade, bem como o direito fundamental à privacidade (art. 5º, X da CRFB). A proteção de dados pessoais, inclusive, já era mencionada como princípio do uso da internet no Brasil na Lei do Marco Civil da Internet (Lei nº 12.964/2014), o que mostra que a proteção de dados pessoais já não é um assunto tão recente.

Motivos para se preocupar com dados pessoais não faltam. Já há algum tempo que a mineração e tratamento de dados por empresas se tornou um negócio altamente lucrativo na indústria de marketing. Funciona da seguinte forma: os sites e aplicativos que usamos coletam nossas informações, que nós voluntariamente fornecemos e então vendem para empresas que desejam fazer anúncios direcionados para pessoas exatamente como nós, pelas nossas preferências, personalidade, histórico de compras, etc. A parte mais engraçada é que nós geralmente concordamos com esse procedimento quando clicamos no "aceito os termos de serviço". É como dito no documentário O Dilema das Redes de Jeff Orlowski (2020), quando nós usamos as

redes sociais, nós não somos os clientes, nós somos o produto, os clientes são as empresas que compram os dados dos usuários.

Esse processo vem ocorrendo já a um certo tempo, mas foi nessa segunda década do século XXI que os escândalos envolvendo dados pessoais começaram a estourar. Em 2018 estourou o escândalo do Facebook com a Cambridge Analytica, na qual, conforme matéria do jornalista Nicholas Confessore (2018) no jornal New York Times, a segunda empresa mencionada vendeu o perfil psicológico de milhões eleitores, adquiridos na rede social Facebook, para campanhas ao redor do mundo, tendo como a de maior repercussão a eleição presidencial americana de 2018, onde a atuação da Cambridge Analytica teria influência na vitória de Donald Trump. O fato rendeu uma CPI no parlamento americano, na qual Mark Zuckerberg teve que se explicar no capitólio, além de inspirar o documentário Privacidade Hackeada de Karim Amer e Jehane Noujaim (2019).

Mas há outros, como o caso da corretora de dados Experian, que em 2013, vendeu por engano os dados pessoais de cerca de 200 milhões de cidadãos americanos a um grupo criminoso do Vietnã (GOODMAN, 2014, p. 97). Os dados obtidos pelos criminosos vietnamitas foram disponibilizados à venda em vários sites do submundo da internet por valores como 15 centavos dólar e eram utilizados pelos compradores para solicitar cartões de crédito e fazer empréstimos fraudulentos com o nome das vítimas.

Mais recentemente, caso semelhante ao do Experian aconteceu aqui no Brasil, pois em janeiro deste ano de 2021, foi noticiado em vários jornais que ocorreu um super vazamento de dados de mais 220 milhões de cidadãos brasileiros, vivos e mortos, o que significa que quase a totalidade da população teve seus dados vazados. Além do CPF, foram vazados dados como nome, endereço, renda, imposto de renda, fotos, entre outros dados sigilosos (ROMANI, 2021). Segundo a notícia do jornal G1 (2021), não se sabe exatamente de qual base de dados esses dados foram obtidos, mas suspeita-se de que foram de vários fontes, inclusive da Serasa Experian, que negou ser a fonte desses dados, mas se sabe que o cibercriminoso responsável compilou esses dados e os disponibilizou gratuitamente num fórum online de comercialização de bases de dados.

Com isso, dá para entender o quão a situação é dramática, praticamente todos os brasileiros tiveram seus dados expostos para o proveito de criminosos, que não hesitarão em realizar uma série de fraudes em nome de vítimas, e todos somos potenciais alvos, fomos expostos. Esse é o problema do *Big Data*, é como disse José Igor Alves Fontes (2018), os dados pessoais são o novo petróleo, supervalorizados no mercado, e as grandes corretoras de dados, como a Experian, o Google, o Facebook, etc. são verdadeiros cofres de ouro e com uma segurança muito aquém do necessário. Sendo assim, esses megavazamentos são verdadeiros assaltos a bancos modernos, mas nesse caso, as vítimas não são os bancos, são o resto da sociedade, que tem seus dados neles armazenados por diversos motivos.

Como não é o objetivo deste trabalho discutir a responsabilidade dessas corretoras de dados pelos vazamentos, passemos ao que interessa: a análise da conduta à luz do Direito Penal. Mas para isso é preciso entender como essa conduta é realizada e nesse sentido devemos explorar como esses vazamentos acontecem.

De acordo com o especialista em segurança cibernética e professor da USP, Marcos Simplicio (2021 *apud* PASSARINHO, 2021), esse megavazmentos de dados ocorrem da seguinte forma: o hacker invade diretamente o banco de dados da empresa; o hacker invade site da empresa para acesso de dados pelos consumidos; ou funcionário da empresa com acesso libera as informações (vazamento interno). Ainda conforme o professor da USP, a invasão ocorre quando o hacker encontra uma falha de segurança nos sistemas da empresa e explora essa vulnerabilidade.

Quanto ao vazamento mediante invasão do sistema ou do site da empresa, não há maiores dificuldades em identificar que a conduta do hacker se amolda ao art. 154-A do CP, visto que há a invasão do dispositivo informático, há a violação de mecanismo de segurança do sistema e há a finalidade de obter para si os dados.

Entretanto, qual será a tipificação se o vazamento é interno? Ademais, qual é o crime cometido por aquele que não invade qualquer sistema, mas de alguma forma obtém esses dados e os disponibiliza a venda ou gratuitamente? É cabível no Direito Penal Brasileiro a figura do furto e a receptação de dados pessoais?

O crime de furto, previsto no art. 155 do Código Penal tipifica como crime “subtrair, para si ou para outrem, coisa alheia móvel”. A primeira coisa a se saber é se

os dados pessoais têm natureza de coisa alheia móvel e a segunda é saber se a conduta de vazar dados pessoais se amoldaria ao núcleo do tipo penal que é o verbo subtrair.

O art. 83, III do Código Civil fala que se considera bens móveis, para efeitos legais, os “direitos pessoais de caráter patrimonial e respectivas ações”. Sendo assim, o que resta saber é se dados pessoais se encaixam na definição do art. 83, III do CC, visto que visivelmente não se identifica com as outras figuras consideradas para efeitos legais do art. 83 e muito menos nos bens móveis de fato do art. 82 do mesmo código.

Muito embora os dados pessoais, como dito, seja uma mercadoria valorizada no mercado, sendo o centro da publicidade, não há como, pelas lições da doutrina, encaixá-los como direitos pessoais de caráter patrimonial, pois esses se restringem a direito de crédito e os direitos autorais, como explicam Flávio Tartuce (2015, p. 151) e Maria Helena Diniz (2016, p. 384). Ademais, sem querer esgotar a discussão sobre a natureza jurídica dos dados pessoais, há como dizer que estes estão mais próximos dos direitos da personalidade do que dos direitos pessoais de caráter patrimonial.

Quem dá uma boa definição do que sejam os direitos da personalidade são os autores Cristiano Chaves e Nelson Rosenvald (2015, p. 138):

> O conjunto dessas situações jurídicas individuais, susceptíveis de apreciação econômica, é dito patrimônio. E, ao lado dessas situações patrimoniais (com vocação econômica), existem os chamados direitos da personalidade, enraizados na esfera mais íntima da pessoa e não mensuráveis economicamente, voltados à afirmação dos seus valores existenciais. Em sendo assim, considerando que a personalidade é um conjunto de características pessoais, os direitos da personalidade constituem verdadeiros direitos subjetivos, atinentes à própria condição de pessoa.

Deste modo, os direitos da personalidade são o conjunto de características próprias do ser humano, como nome, aparência, voz, imagem, etc. Como dito pelos autores, esses direitos são extrapatrimoniais, é dizer, não são mensuráveis economicamente, mas nada impede que suas manifestações sejam licenciadas para uso de terceiros, por meio de contrapartida econômica. Tal não é difícil de visualizar, pois é prática comum a cessão de direito de imagem, voz, etc. de pessoas famosas para fins publicitários e coisa semelhante ocorre com os dados pessoais, pois são manifestações da personalidade, informações referentes às pessoas humanas e que podem ser, como são, objeto de cessão para uso.

Além de muito provavelmente não se encaixarem no conceito de bens móveis, problema existe no verbo subtrair, elementar do crime de furto. Como explica a doutrina, subtrair é “apoderar-se o agente, para si ou para outrem, de coisa alheia móvel, tirando-a de quem a detém (diminui-se o patrimônio da vítima)” (CUNHA, 2016, p. 251). Assim, além de ser coisa alheia móvel, seria necessário que o agente subtraísse os dados pessoais, retirasse de quem a detinha, que eles deixassem de ser acessíveis ao anterior detentor dos mesmos.

Entretanto, não é o que normalmente ocorre. Quando ocorre um vazamento de dados, o que o agente responsável pela conduta geralmente faz é copiar as informações, com o fim de obtê-las, sem que os demais detentores percam essas informações, passarão a existir cópias, sem limites, dos mesmos dados. Sendo assim, não há como se configurar o crime de furto, conclusão, inclusive, que encontra respaldo jurisprudencial na 7ª Câmara Criminal do Tribunal de Justiça do Rio Grande do Sul, no julgamento da Apelação Criminal nº 70049844483.

Como a conduta de vazar dados não se amolda ao crime de furto, também não há na legislação outro tipo penal que tipifique a conduta de vazar dados pessoais, sendo, portanto, penalmente atípica. Se não há crime na obtenção desses dados pessoais, também não será a conduta de disponibilizar esses mesmos dados a venda, pois o crime de receptação, do art. 180 do Código Penal, visto que o tipo penal fala “adquirir, receber, transportar, conduzir ou ocultar, em proveito próprio ou alheio, coisa que sabe ser produto de crime, ou influir para que terceiro, de boa-fé, a adquira, receba ou oculte”.

Pode-se concluir, portanto, que a conduta de vazar dolosamente ou usar indevidamente dados pessoais de terceiros é penalmente atípica no Brasil e apenas as circunstâncias podem implicar na tipicidade da conduta, quando por exemplo, o agente invade o banco de dados para obter os dados a força (art. 154-A do CP), ou quando os dados são utilizados para praticar fraudes, o que implicará, em tese, no crime de estelionato. Contudo, se o agente apenas se utilizar de acesso que tem ao sistema para vazar as informações, usar identidade, mas não praticar fraude patrimonial ou se recebê-las de terceiros e dispor a venda, não comete crime.

Pelo exposto, há uma lacuna na legislação penal, pois não há dúvidas da relevância penal da conduta, que como explicado, tem o potencial de gerar danos a

uma grande número de pessoas. Atinge, portanto, relevantemente, a ponto de romper a barreira da intervenção mínima, bens jurídicos protegidos pelo ordenamento jurídico brasileiro, quais sejam os direitos fundamentais de privacidade e o livre desenvolvimento da personalidade da pessoa natural, pela descrição dada pela Lei Geral de Proteção de Dados. A LGPD, inclusive, representa um grande avanço na proteção dos dados pessoais, mas pecou em não trazer nenhum conteúdo penal. A lacuna existente cria uma desproporcionalidade no sistema, por deficiência na proteção dos bens jurídicos citados.

3.5 O ATAQUE DE NEGAÇÃO DE SERVIÇO (DDOS ATTACK)

O ataque de negação de serviço é uma conduta nociva praticada por meio da internet há bastante tempo, mas demorou para haver alguma reação de governos em relação a esse tipo de ataque. Esse ataque tem o objetivo de causar a falha de um serviço na internet por meio de uma quantidade de solicitações de acesso além da capacidade de resposta do servidor.

De acordo com a empresa de cibersegurança Kaspersky (c2021) o cibercriminoso se utiliza de uma rede computadores “zumbis” para esse ataque, previamente infectados, que obedecem os comandos do hacker sem que os usuários dos computadores infectados percebam. Com o controle de uma legião de “zumbis”, o hacker controla as máquinas para que enviem várias solicitações para o servidor vítima até que sua capacidade de atender as solicitações seja ultrapassada e o servidor seja derrubado, ficando inacessível.

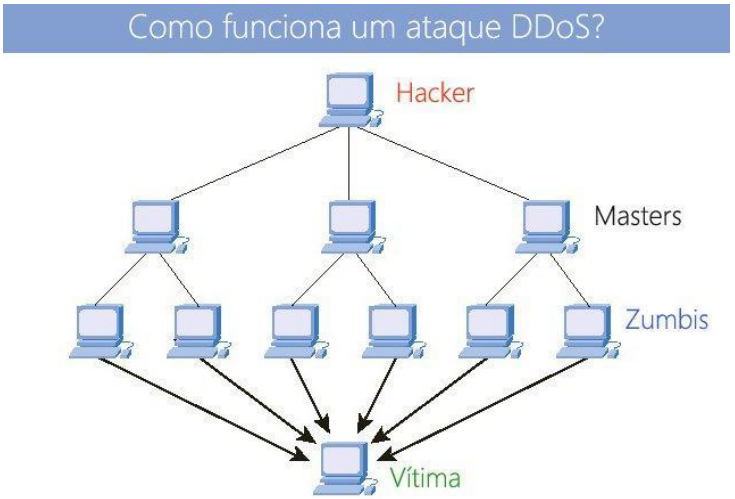

Imagem 1: Ataque de negação de serviço

Fonte: Canaltech

O objetivo deste ataque não necessariamente é obter alguma vantagem indevida ou informações, mas simplesmente tirar um site do ar, por puro vandalismo, com o objetivo de prejudicar a vítima ou por atividade hacktivista. Desde o seu surgimento, o grupo hacktivista Anonymous realizou uma série desses ataques, tendo como vítima, inclusive, os sites das financeiras Visa e Mastercard.

Não há maiores dificuldades em entender porque esse tipo de ataque atinge bens jurídicos protegidos pelo ordenamento jurídico brasileiro, pois ter seu site desabilitado pode ser fonte de vultosos prejuízos para uma grande variedade de empresas, mas sobretudo aquelas que concentram seus negócios por esse canal, como o segmento de comércio eletrônico. Conforme matéria de Nathan Vieira (2019) no site Canaltech, ataques de negação de serviço causaram cerca de 45 bilhões de dólares em prejuízo só em 2018.

A hipótese é de que ao praticar o ataque de negação de serviço, o hacker estaria incurso no art. 154-A do Código Penal, o crime de invasão de dispositivo informático. No entanto, há uma série de problemas em relação a isso.

Em primeiro lugar, o ataque de negação de serviço não é uma invasão de dispositivo informático, é dizer, a máquina de vítima, geralmente o servidor que hospeda um site, não é invadido, apenas recebe mais solicitações de acesso do que

pode aguentar. A única hipótese em que há invasão de dispositivos informáticos é quando o hacker invade outras máquinas e cria uma rede de computadores “zumbi” para realizar o ataque. Acontece que isso não é necessário, pois o ataque pode ser realizado por uma máquina só, que pode enviar várias solicitações e derrubar servidores na proporcionalidade da sua própria capacidade de processamento. É como explica o professor Otto Carlos Muniz Bandeira Duarte (2006):

> Uma forma de provocar os ataques é aproveitando-se de falhas e/ou vulnerabilidades presentes na máquina vítima, ou enviar um grande número de mensagens que esgote algum dos recursos da vítima, como CPU, memória, banda, etc. Para isto, é necessário ou uma única máquina poderosa, com bom processamento e bastante banda disponível, capaz de gerar o número de mensagens suficiente para causar a interrupção do serviço, ou ter o controle de um grupo de máquinas, que podem ter recursos mais humildes, que se concentrem em enviar mensagens para a vítima. Este último, por distribuir os ataques em várias máquinas, é denominado ataque de Negação de Serviço Distribuído, ou DDoS (Distributed Denial of Service).

Sendo assim, vê-se que a conduta não se amolda ao art. 154-A do CP quando é praticado pela própria máquina do responsável pelo ataque, sem invadir qualquer dispositivo que seja.

Apesar disso, não se pode esquecer que há uma hipótese em que o ataque de negação de serviço, mesmo não se amoldando ao art. 154-A do CP, encontra tipificação no art. 266, §1º do mesmo código, que também foi introduzido pela Lei 12.737/2012. Essa hipótese ocorre quando o servidor atacado interrompe serviço telemático ou de informação de utilidade pública, além da hipótese de interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico.

Logo, vê que apenas as circunstâncias do ataque de negação de serviço podem ocasionar a tipificação da conduta no Direito Penal Brasileiro, mas a conduta em si é atípica, em outras palavras, o ataque de negação de serviço apenas pode funcionar como um meio para o cometimento de crimes. Isso significa dizer que se o hacker, utilizando poderosa máquina própria, sem invadir qualquer dispositivo, ataca e tira do ar site de grande empresa do setor do comércio eletrônico, causando vultosos prejuízos a esta, não comete crime no Brasil.

Em que pese a atipicidade do fato em comento, sabe-se que a conduta descrita lesa relevantemente bens juridicamente protegidos pelo ordenamento, como os valores sociais do trabalho e da livre iniciativa (art. 1º, IV da CRFB), fundamentos da república que regem a ordem econômica. Quando a Constituição em livre iniciativa, como explica

o professor Adalberto Pasqualotto (2019) “o que se quer (ou se deveria querer) significar é que ela deve ser, desejavelmente, desimpedida de maiores embaraços”. Ao dizer uma atividade livre de embaraços, se quer positivar um direito de *status* negativo contra o Estado e o restante da sociedade de perturbar o exercício de atividade econômica, desde que seja lícita e respeite os fins constitucionais.

Assim, é um bem jurídico protegido ordenamento jurídico o exercício desembaraçado de atividade econômica, bem jurídico esse que já recebe atenção do Direito Penal, uma vez que o Código Penal, em seu art. 202 prevê o crime de sabotagem, que diz que é crime “Invadir ou ocupar estabelecimento industrial, (...) com o intuito de impedir ou embaraçar o curso normal do trabalho, ou com o mesmo fim danificar o estabelecimento ou as coisas nele existentes ou delas dispor”.

Com isso, o art. 202 do CP protege o exercício de atividade econômica contra perturbação de terceiros, perturbação essa que difere do ataque de negação de serviço somente pelo meio empregado para sabotar a atividade. Para melhor explicar, enquanto o ataque de negação de serviço usa um meio virtual e prejudica um espaço eletrônico, o art. 202, com as expressões invadir ou ocupar, fala numa sabotagem presencial, com a invasão do espaço físico onde se exerce a atividade. Por esse motivo, o ataque de negação de serviço não se amolda ao art. 202, nem se pode aplicar analogicamente este tipo ao ataque em comento, uma vez que o Direito Penal veda a analogia *in malam partem*.

Pelo exposto, conclui-se esse trecho da pesquisa constando que o ataque de negação de serviço, embora mereça atenção do Direito Penal, é penalmente atípico no Direito Brasileiro, sendo uma verdadeira lacuna deixada pelo legislador. Por fim, não restam dúvidas que o fato ultrapassa as barreiras do princípio intervenção mínima, uma vez que lesa relevantemente bens juridicamente protegidos e condutas semelhantes, mas praticados por meios físicos são tipificados no Código Penal, como o crime de sabotagem (art. 202 do CP).

3.6 O ATAQUE DE BLOQUEIO OU DE CRIPTOGRAFIA (RANSOMWARE ATTACK)

O *ransomware* é um tipo de *malware* (programa malicioso), que merece um subitem a parte dos *malwares* em geral, que foram tratados no subcapítulo 3.2, devido a suas particularidades que são bem relevantes.

A empresa de cibersegurança Kaspersky (c2021) define o *ransomware* como um tipo de *malware* que bloqueia o acesso ao sistema da vítima ou criptografa as informações armazenadas na máquina, após isso, geralmente, é exigindo um resgate (*ransom*) da vítima para que esta recupere o acesso ao seu sistema e aos seus dados, sendo, portanto, um *malware* muito utilizado para praticar o crime de extorsão (art. 158 do CP).

Ainda conforme a Kaspersky (c2021), existem dois tipos principais de *ransomwares*: os de bloqueio de sistema e os de criptografia. A título de exemplo, em 2017 houve um grande ataque de *ransomware* com um *malware* que ficou conhecido como *WannaCry*[10]. Naquele ano, o *WannaCry* vitimou cerca de 230 mil computadores em todo o mundo, atingiu um terço das fundações hospitalares do Reino Unido e gerou um prejuízo global estimado em 4 bilhões de Dólares (KASPERSKY, c2021). Nesse ataque, o *malware* criptografou os dados existentes nas máquinas e exigia um resgate em Bitcoins para liberar o acesso a esses dados (KASPERSKY, c2021).

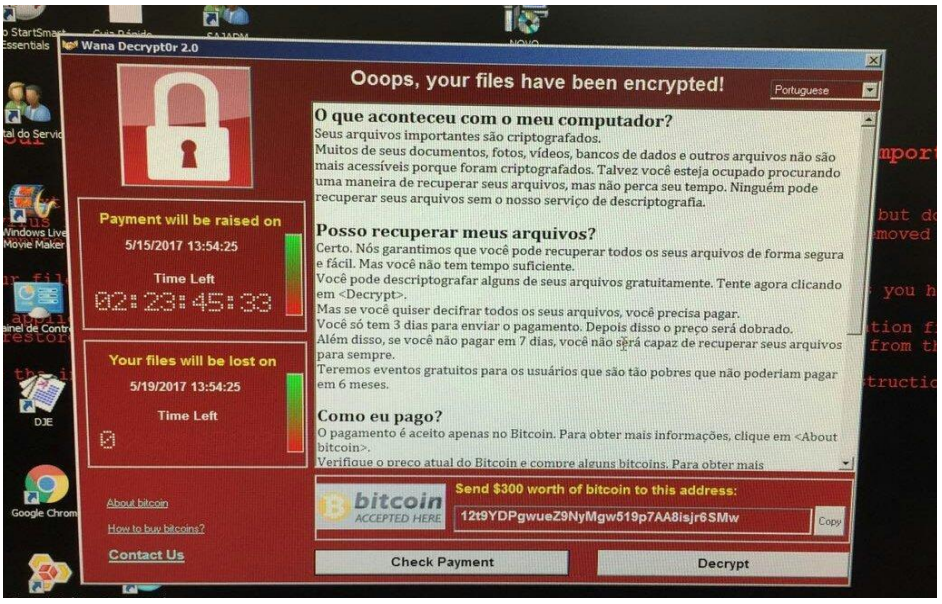

Imagem 2: Computador infectado pelo WannaCry

[10] Palavra do inglês que pode ser simplesmente traduzida como quero chorar. Foi um *ransomware* de criptografia que mudava todos os arquivos do computador para uma extensão que os hackers nomearam de .WCRY (eram criptografados) e eram inutilizados. Para que seus arquivos voltassem ao normal, o *malware* exigia um resgate em bitcoins (TECMUNDO, 2017).

Fonte: Gizmodo

Outro exemplo de *ransomware* é o Ryuk, dito com um dos mais notáveis dos últimos (CRYTOID, 2020), ataque realizado em 2018, que além de criptografar os arquivos das vítimas, exigindo um pagamento em Bitcoins para que os arquivos fossem recuperados, ele desativava a opção de Restauração do Sistema do Windows, o que tornava impossível restaurar arquivos criptografados sem um backup. Na época o efeito dos ataques foi bem sentido nos Estados Unidos, onde muitas empresas foram obrigadas a pagar o resgate para não perder informações importantes.

Existiram vários outros grandes ataques, como o dos *malwares* Jigsaw, CryptoLocker, Petya, Golden Eye, Troldesh, etc. Mas o fato é que esses ataques já causaram prejuízos bilionários a nível global e vem se intensificando nos últimos 5 anos, sendo uma lucrativa fonte de recursos para o crime cibernético e uma gigantesca fonte de preocupações para usuários de dispositivos informáticos e empresas no mundo todo.

Quanto a tipificação dessa conduta para o Direito Penal, parece não haver problema em encaixar o fato no crime de extorsão (art. 158 do CP), uma vez que como dito, o ataque de *ransomware* geralmente tem o objetivo de cobrar um resgate da vítima para que esta recupere o acesso ao seu sistema ou as suas informações. O art. 158 do CP tem a seguinte redação: “constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa”. Assim, pode-se dizer que a ameaça de perder em definitivo as informações ou o acesso ao sistema é a grave ameaça, meio empregado para realizar extorsão, e o resgate cobrado é a vantagem econômica que se busca obter, não parecendo haver qualquer problema na tipificação do delito.

No entanto, o problema surge se nenhuma extorsão for praticada, é dizer, se o hacker bloquear o sistema das vítimas ou seus arquivos por qualquer outro motivo que não seja de obter vantagem de fundo econômico. O crime de extorsão, mesmo na modalidade em que o criminoso obriga a vítima a fazer, tolerar que se faça ou deixar de fazer alguma coisa, deve, obrigatoriamente a finalidade de obter uma vantagem

econômica, para si ou para outrem, uma vez que o crime em comento se localiza no capítulo de crimes contra o patrimônio, como explica Rogério Sanches Cunha (2016, p. 283):

> O art. 158 do CP pune o delito de extorsão, protegendo, em primeiro lugar, o patrimônio e, secundariamente, a inviolabilidade pessoal da vítima. A despeito da gravidade, e a exemplo do crime de roubo, a finalidade do agente é obter vantagem econômica, tolhendo o patrimônio do ofendido (sendo a busca do indevido locupletamento a razão pela qual se inseriu a extorsão entre os crimes patrimoniais). (...) Aqui reside a principal diferença com o delito de constrangimento ilegal: a finalidade que orienta os dois delitos é diversa, pois no constrangimento busca-se a restrição da liberdade (eis o fim almejado); na extorsão, o enriquecimento do agente (o constrangimento, aqui, é meio).

Deste modo, se o agente não tiver o objetivo de obter vantagem econômica, mas apenas de prejudicar a vítima, por qualquer outro motivo, não haverá extorsão, mas subsistirá um prejuízo que pode ser vultoso, a depender das circunstâncias do alvo.

Há ainda outro tipo penal que parece aplicável ao caso: a invasão de dispositivos informáticos (art. 154-A do CP), artigo recorrentemente visitado neste trabalho.

No entanto, o problema aqui é que o ataque de *ransomware* não é necessariamente uma invasão de dispositivo informático, nem precisa o hacker violar qualquer mecanismo de segurança na máquina de vítima, além de não ter exatamente o objetivo de obter, adulterar ou destruir os dados da vítima, apesar de fazê-lo como meio empregado para constrangê-la. Como esclarece a Kaspersky (c2021) “ele pode contaminar os computadores por meio de anexos ou links em e-mails de *phishing*, por um download feito em um site infectado ou pelo uso de unidades USB infectadas”.

Dessa forma, a própria vítima geralmente introduz o software malicioso na sua máquina no mínimo descuido e, após isso, o *ransomware* age bloqueando o acesso ao sistema, ou criptografando os arquivos salvos na máquina e assim não pratica núcleos do art. 154-A, *caput* do CP, sendo este inaplicável ao ataque de *ransomware*.

Há ainda a forma equiparada do art. 154-A, § 1º do CP, também já discutido no tópico de *malwares* e que traz a seguinte redação: “na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput”.

Como dito, o *ransomware* é um *malware*, mas diferente dos vírus, *trojans, spywares,* etc. os classificados como *ransomwares* não são produzidos para invadir dispositivos, tampouco são produzidos com a finalidade de obter, destruir ou alterar informações, pelo menos não diretamente, pois sua finalidade geralmente é a de obter um resgate e a inutilização dos dados funcionam como um mecanismo de convencimento da vítima a pagar o resgate.

Deste modo, há uma dificuldade, pelo menos em tese, de tipificar a fabricação, ou distribuição de *ransomwares* neste dispositivo, mas para aquele que apenas usa o software adquirido de algum lugar obscuro da internet para realizar seu ataque, a aplicação do art. 154-A do CP está totalmente descartada, pois não pratica nenhum dos verbos do tipo penal.

Talvez um pouco mais útil seja o art. 266 do CP, que tipifica o crime de interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública. Esse tipo penal também já foi visto e, como nos outros casos, apresenta os mesmos problemas.

O ataque de *ransomware*, como é um ataque que geralmente deixa o sistema, ou arquivos do sistema, inacessíveis a vítima, certamente tem a capacidade de interromper ou perturbar a prestação de um desses serviços descritos no arts. 266, *caput* e 266, § 1º, ambos do CP, basta que criptografe arquivos essenciais dos sistemas envolvidos na prestação do serviço, ou que bloqueie o próprio acesso a esses sistemas. Todavia, esse tipo penal, como já foi discutido, é bem restrito e não resolve o problema da tipificação do ataque de *ransomware*.

Por tudo que foi dito, podemos concluir que o Direito Penal brasileiro tem uma séria brecha quanto a tipificação do ataque de *ransomware*, pois embora esse ataque possa ser recorrentemente tipificado como extorsão (art. 158 do CP), basta que o cibercriminoso não exija a vantagem de ordem econômica, ou que seu objetivo seja de simplesmente prejudicar as vítimas, para o art. 158 do CP seja afastado e o fato seja, com raras exceções vistas, penalmente atípico.

Sendo assim, a lacuna é evidente, pois o ataque de *ransomware* é uma conduta nociva para a sociedade que pode ter consequências gravíssimas, como o caso do WannaCry que atingiu sistemas de hospitais no Reino Unido e gerou um prejuízo

global estimado em 4 bilhões de Dólares. Além disso, a conduta fere gravemente bens jurídicos protegidos pelo ordenamento jurídico, quais sejam, os mesmos protegidos no art. 154-A do CP (a liberdade individual e o direito à intimidade, além da proteção da inviolabilidade dos dados e informações existentes em dispositivo informático), com intensidade suficiente para ultrapassar a barreira do princípio da intervenção mínima e merecer tipificação penal completa.

3.7 SPOOFING

O *spoofing*, palavra que vem do inglês *spoof* e significa enganar, como explica Ivan Belci (2020), no site da empresa de cibersegurança AVAST, é um ardil cibernético em que o cibercriminoso se passa por um contato ou endereço virtual conhecido pela vítima para ludibriá-la a passar-lhe informações confidenciais. Esse ataque pode acontecer de uma variedade de formas e com diferentes níveis técnicos e é comumente utilizado com a finalidade de praticar *phishing*. Dito de forma resumida, no *spoofing*, o hacker se passa por outra pessoa, ou máquina, para enganar outras pessoas, ou máquinas.

Dentre as variedades de ataques de *spoofing*, uma muito comum é o *spoofing* de e-mail (BELSIC, 2020), em que o cibercriminoso forja um e-mail, para parecer que o e-mail está sendo enviado por uma pessoa ou empresa de confiança da vítima, como o banco o qual é cliente, por exemplo. Quando se diz que o e-mail é forjado para parecer, é porque realmente ele é criado para que consiga enganar uma boa porcentagem das pessoas menos atentas, mas geralmente há caracteres no endereço do e-mail que podem denunciar a tentativa de *spoofing*.

O *spoofing* de e-mail, no entanto, é apenas a variante mais básica em aspectos técnicos, há ainda o *spoofing* de IP[11] (*Internet Protocol*), de DNS[12], de telefone e o

[11] O IP é um sigla para *Internet Protocol*, ou em português, protocolo da internet. O endereço IP é o endereço da máquina quando conectada à internet, ou seja, é a identidade virtual da sua máquina, como uma espécie de CPF. Se trata de um conjunto numérico que vai de 0.0.0.0 até 255.255.255.255 (IPv4) e segue o padrão definido pelo protocolo IP. Cada máquina conectada à internet possui um IP na rede local, e um IP na rede global (GOGONI, 2019).

[12] DNS é uma sigla em inglês para *Domain Name System*, ou em português, sistema de nomes de domínios. Trata-se de um serviço que existe na internet para traduzir endereços *web* nominais (www.exemplo.com) em endereços IP (CIPOLI, c2021).

spoofing de ARP[13]. Este último vai melhor detalhado, uma vez que é muito usado para realizar ataques de homem do meio (Man-In-The-Middle - MITM) (BELSIC, 2020).

O ARP (*Address Resolution Protocol*) é um dos protocolos utilizados em rede de computadores para mapeamento de endereços de rede (IP) e endereços de máquina (MAC). O *spoofing* de APR, em apertada síntese fornecida por Ivan Belcic (2020) é um ataque que:

> Permite que o cibercriminoso se infiltre em uma LAN disfarçando seu computador como um membro da rede. Cibercriminosos usam spoofing ARP para roubar informações com ataques Man-In-the-Middle. O cibercriminoso intercepta secretamente uma conversa e faz se passar por ambos os participantes, coletando todas as informações que são discutidas.

Assim, temos a definição do ataque de ARP e ainda, de bônus, a definição do ataque *Man-In-The-Middle*. O primeiro é um ataque que engana as máquinas em uma rede local (*Local Area Network* - LAN), se fazendo passar por outra máquina e o segundo, emprega a primeira fraude para interceptar informações que iriam para aquela.

Para detalhar um pouco melhor em termos técnicos o protocolo ARP consiste numa tabela que relaciona endereços IP (de rede), que são dinâmicos, podendo mudar, a endereços de cada máquina (endereço MAC[14]), que são estáticos. De posse deste detalhes técnico, o site de notícias sobre segurança digital We Live Security (2017) explica que, resumidamente, o hacker utiliza códigos para modificar a tabela ARP das máquinas e com essa tabela "envenenada", as máquinas enviarão informações para a máquina do hacker por engano, o que possibilita que o cibercriminoso receba indevidamente mensagens, arquivos, etc. que eram endereçados para outro computador.

O *spoofing* ganhou até certo destaque em âmbito nacional recentemente devido a operação *spoofing* da Polícia Federal. A mencionada operação da PF foi instaurada para apurar o ataque cibernético que originou o maior escândalo judicial da história do Brasil, que ficou conhecido como Vaza Jato. No ataque, conforme informações do

[13] Sigla em inglês para *Address Resolution Protocol*, ou em protguês, protocolo de resolução de endereços. Trata-se de uma tabela que registra endereços IP na rede local e os vincula aos endereços MAC (endereço físico) das máquinas (PPLWARE, 2011).
[14] Sigla em inglês para *Media Access Control*, ou em protuguês, controle de acesso de mídia. O endereço MAC nada mais é do que o endereço físico de uma placa de rede que é único no mundo e corresponde ao respectivo equipamento. Trata-se de um endereço estático de 48 bits ou 12 algarismos hexadecimais (PPLWARE, 2010).

portal G1 da Globo (2019), o hacker Walter Delgatti Neto teria conseguido o código do Telegram para celulares para abrir autorizar o terminal de mensagens de várias autoridades, dentre elas o então Ministro da Justiça Sérgio Moro e o então procurador da Operação Lava Jato Deltan Dallagnol. Com isso, o hacker conseguiu interceptar várias mensagens trocadas entre as autoridades, revelando uma série de abusos praticados por autoridades na famosa Operação Lava Jato.

É de amplo conhecimento que as mensagens interceptadas pelo hacker foram repassadas ao jornalista americano Glenn Greenwald, que as publicou no site The Intercept a série de mensagens vazadas que denominou de Vaza Jato. Neste caso, o ataque não foi de todo nocivo para a sociedade, pois desmascarou autoridades que usavam o cargo público com propósitos pessoais, mas o potencial foi demonstrado, é dizer, pode ser usado unicamente com propósitos maliciosos. Não é difícil de imaginar ataques de *spoofing* sendo realizados para prejudicar assunto de Estado, vazar segredos industriais e os mais diversos próprios nocivos que esse ataque pode ter.

O problema para tipificar a conduta de *spoofing* é mais complicado do que parece. À primeira vista, pode parecer se tratar de uma invasão de dispositivo informático, para obtenção de informações, o que atrairia a aplicação do art. 154-A do Código Penal, já bem visto nesta pesquisa. No entanto, o ataque de *spoofing* não é uma invasão de dispositivo informático. Nesse tipo de ataque cibernético, o hacker frauda a sua própria identidade ou as credenciais da sua máquina, para enganar terceiros e poder interceptar informações. Não havendo invasão de dispositivo informático, resta afastada a aplicação do art. 154-A do CP.

No caso da operação *spoofing*, o Ministério Público Federal (2020), na denúncia contra o hacker Walter Delgatti Neto e outros, imputou ao citado o crime de invasão de dispositivos informáticos (art. 154-A do CP), uma vez que as investigações concluíram que além da interceptação de mensagens (ataque do homem do meio - MITM), os investigados haviam invadido dispositivos informáticos para a extração das mensagens, documentos e agendas de contatos armazenados no Telegram. Entretanto, é preciso que se diga que nem todo tipo de ataque de *spoofing* realiza invasão de qualquer dispositivo.

Se pudesse se comparar a algum outro crime já existente no Código Penal, este seria a falsificação de documento particular, do art. 298 do CP, pois se trata de um

crime onde se realiza uma fraude prévia (falsificação do documento), geralmente para se utilizar em uma fraude posterior (geralmente um estelionato). É exatamente o que ocorre no *spoofing*, o hacker frauda sua identidade, se apresentando como outra pessoa ou empresa de confiança da vítima (*spoofing* de e-mail), ou ainda, falsifica os parâmetros de endereços das máquinas (*spoofing* de ARP) para enganar as vítimas e suas máquinas e conseguir captar (*phishing*) ou interceptar informações. Todavia, não há como se aplicar o crime em comento, visto que o que se falsifica no *spoofing* não pode ser classificado como documento, nem particular, nem público.

Fato é que, não há, no capítulo de crimes contra a fé pública, que abarca os crimes de falsidades, nem em qualquer outra lei penal a previsão de falsificação de identificação, endereço ou credenciais digitais como crime, a não ser que esteja se falando de um documento público ou particular. Ocorre que, tomando o exemplo do ataque de *spoofing* local (ARP), a tabela ARP e endereços IP (*Internet Protocol*) e MAC das máquinas não documentos, pois não provam nenhuma situação jurídica e nem poderiam ser, uma vez que se tratam de endereços dinâmicos (IP) ou podem ser alterados em alguns casos (endereço MAC). Se trata de uma fraude muito específica, para realizar um ataque bem específico.

No caso do específico do ataque do homem do meio (MITM), há uma possibilidade de tipificação da conduta. Se o hacker interceptar simultaneamente mensagens trocadas entre interlocutores, estará, em tese, incorrendo no crime de interceptação indevida de comunicações telefônicas e telegráficas, previsto no art. 10 da Lei nº 9.296/96, com a seguinte redação: “Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei”.

Sem embargo, o entendimento da doutrina (GOMES, 2011, p. 24) é que o crime de interceptação de comunicação telefônica ou informática só ocorre se o agente captar as mensagens no exato momento em que elas estão sendo trocadas, entendimento referendado pela 6ª turma do STJ (REsp nº 1.428.961 - SP). Assim, o crime do art. 10 da Lei nº 9.296/96 somente se aplica nessas hipóteses específicas, em que há uma captação simultânea de comunicações trocadas pelos interlocutores.

Deste modo, se a captação não é simultânea ou se o conteúdo interceptado não é uma comunicação telefônica/informática, não se aplica o art. 10 da Lei de Interceptações e se também não há invasão de dispositivos informáticos, o fato é atípico. Não é difícil de imaginar um caso em que a conduta do agente seja penalmente atípica no Brasil, basta lembrar há uma grande variedade de ataques de *spoofing* e o primeiro que foi mencionado neste tópico, o *spoofing* de e-mail, não é realizado com invasão de dispositivos, nem intercepta comunicações.

Além deste, há outro exemplo importante que é o ataque de *spoofing* de DNS. O DNS (*Domain Name System*) é um serviço fornecido por um servidor que traduz um endereço em palavras - como por exemplo o site do Facebook: www.facebook.com, cujo endereço IP (*Internet Protocol*) é o [157.240.7.35] - o que quer dizer que quando pesquisamos um site pelo seu endereço nominal, um servidor DNS é consultado para dizer o endereço IP e nos levar ao espaço digital buscado. O objetivo deste ataque, dito de forma bem resumida, é fraudar a resposta do servidor DNS, fazendo com que este informe um caminho incorreto para a vítima que solicita o serviço, para que este seja direcionado para um site fraudulento, com o objetivo de aplicar outras fraudes, obter dados (*phishing*), etc. (WE LIVE SECURITY, 2018).

Uma das variantes do ataque de DNS *spoofing*, talvez o mais comum, é o DNS *cache poisoning*[15]. Essa variante se processa da seguinte forma: o hacker faz uma requisição para o servidor DNS, para saber o endereço de um site específico, mas o servidor não terá esse endereço em seu cache, então vai começar o processo de mapeamento, solicitando a outros servidores DNS que possam saber o endereço. É neste ponto que o hacker resolve a solicitação do servidor atacado, por meio de um servidor DNS autoritativo falso por ele criado, informando o endereço IP solicitado, mas não só isso, ele também envia endereços falsos para sites que já existiam no cache do servidor atacado, fazendo que eles sejam reescritos (SAYTSON; PETERSON; BORZINO, 2019). É deste modo que a vítima pode, por exemplo, buscar o site da loja virtual da Amazon e ser remetido a um site fraudulento, criado por hackers, para comprar produtos que nunca chegarão, enquanto os cibercriminosos embolsam o dinheiro.

[15] temos em inglês que significa envenenamento de cache em português.

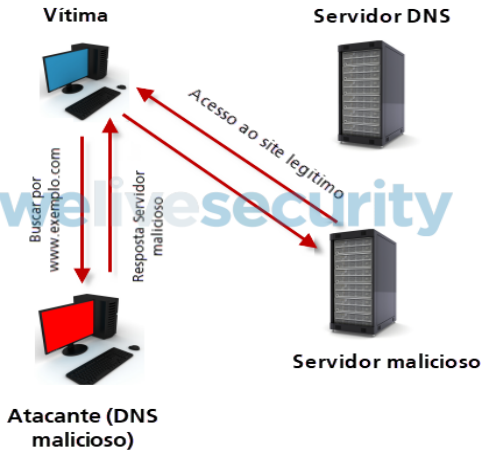

Imagem 3: Ataque de *spoofing* de DNS

Fonte: We Live Security

Dito isso, logo se vê que não é difícil de encontrar exemplos que em o ataque de *spoofing* não será tipificado como crime no Brasil, isso porque o ataque em si não é previsto como crime, apenas as circunstâncias do caso podem fazer com que algum crime seja praticado, como por exemplo, o caso do agente faz ataque de *spoofing* para interceptar mensagens trocadas instantaneamente, ou o agente que realiza uma modalidade *spoofing* que implique a invasão de algum dispositivo informático. É o que também ocorre com as outras condutas investigadas neste trabalho e igualmente aqui, a atipicidade do fato, puramente considerado, é a única conclusão possível.

Para finalizar este tópico, resta discutir se a conduta de praticar *spoofing*, que como visto é atípica, deveria ser prevista como crime. Aqui, como ocorre nos demais casos pesquisados, estamos tratando de uma conduta nociva à sociedade, que de tão gravosa, ultrapassa a barreira da intervenção mínima penal, merecendo atenção deste ramo do Direito. O referido ciberataque lesa a integridade dos sistemas informáticos e causam prejuízos vultosos aos consumidores do país. Basta lembrar do estudo realizado pela Globo (2021), que revelou que mais de 60 milhões de brasileiros já sofreram fraudes financeiras na internet e o *spoofing* é um ataque muito empregado para essa finalidade. Além disso, também é uma conduta que lesa outros bens jurídicos protegidos pelo ordenamento jurídico, como os protegidos pelo crime de invasão de dispositivos informáticos (a liberdade individual e o direito à intimidade,

além da proteção da inviolabilidade dos dados e informações existentes em dispositivo informático), visto que podem ter a mesma finalidade, apesar de nem sempre realizar a conduta invadir.

A impressão deixada pelo estudo atento de condutas nocivas praticadas por cibercriminosos é a de que o legislador teve a intenção de resolver todas as lacunas penais legislativas com a Lei Carolina Dieckmann e seu crime de invasão de dispositivos informáticos (art. 154-A do CP), mas basta pesquisar em termos técnicos sobre os ataques cibernéticos mais comuns que se percebe que o art. 154-A do CP não tem como abarcar todos eles, pois, como visto, nem todos se processam invadindo algum dispositivo informático.

4 OS DESAFIOS PARA INVESTIGAÇÃO E REPRESSÃO DOS CRIMES CIBERNÉTICOS

Os crimes praticados pelos meios informáticos oferecem novos desafios às autoridades no que diz respeito à investigação e persecução penal, sobretudo quanto a elucidação da autoria delitiva, uma vez que os meios de prova tradicionais, como testemunhas, identificação por impressões digitais, imagens, etc. serão de pouca serventia nesses casos. Os crimes praticados por meios digitais são praticados sem que o criminoso precise sair de casa, nem apontar uma arma contra quem quer que seja, ele o pratica sem deixar qualquer rastro biológico.

É nesse contexto que a assessora técnica do Grupo de Combate aos Crimes Cibernéticos da Procuradoria da República, Adriana Shimabukuro (2017), fala que “saem as digitais e entram os números IPs”. Ao dizer isso, ela se refere ao fato que as investigações em ambiente cibernético se baseiam em localizar um número IP, que é o endereço que as máquinas recebem na internet e que segue um padrão que é mundial. Com a informação do endereço IP de onde partiu a ação criminosa, os órgãos investigativos podem solicitar mais informações aos provedores com o fim de tentar descobrir de onde partiu o ataque e a quem pertence o terminal.

Em assunto de investigação de delitos informáticos, o Marco Civil da Internet (Lei nº 12.965/2014) foi de grande avanço. O art. 13 desta lei obriga a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento a manter os registros de conexão, dados pessoais, conteúdo de comunicações privadas ou outras informações que possam contribuir para a identificação do usuário ou do terminal, pelo prazo de um ano e a mesma obrigação para provedores de aplicação na internet, pelo prazo de 6 meses (art. 15). Além disso, ainda obriga essas entidades a fornecer essas informações às autoridades mediante ordem judicial, ou independente de ordem judicial se as informações forem referentes apenas aos dados cadastrais que informem qualificação pessoal, filiação e endereço (art. 10, §3º).

À primeira vista, o Marco Civil parece ter dado munição suficiente para os órgãos investigativos solucionarem os mais diversos crimes cibernéticos, mas ainda há uma série de desafios que dificultam as investigações deste tipo de crime e serão tratados ponto a ponto.

4.1 O serviço de *proxy*

Como foi dito, quando tratamos de investigação de crimes cibernéticos, evidências tradicionais têm pouca utilidade, enquanto um único elemento tem grande relevância para criar uma linha investigativa com potencial de revelar a autoria da ação defeituosa: o endereço IP de onde partiu o ataque.

Acontece que nem mesmo esse endereço é uma evidência totalmente confiável, pois como é esclarecido pela especialista em redes de computadores Adriana Shimabukuro (2017), é muito fácil mascarar o IP utilizando serviços de *proxy*. Ainda conforme a autora, o serviço de *proxy*[16] é prestado por um computador intermediário entre o usuário e o destino com alguns objetivos, sendo que nem todos são usados com propósitos necessariamente criminosos.

Existem aplicações na rede que filtram conteúdo na rede de acordo com o IP da máquina, como Netflix, que disponibiliza certos conteúdos para alguns países e outros não, assim se usuário utilizar o serviço de *proxy*, é possível acessar um conteúdo que não estaria disponível para endereços IP do seu país de origem. Sendo assim, os serviços de *proxy* são utilizados com diversos propósitos, mas o que importa a pesquisa é a função que tem o serviço de anonimizar as comunicações do usuário na rede. Para entender melhor, segue abaixo imagem do aplicado Real Hide IP:

Imagem 4: Aplicativo Real Hide IP

fonte: Tela do aplicativo Real Hide IP

[16] Termo em inglês que significa representante ou procurador em português.

Com uso dessa ferramenta, como explica Adriana Shimabukuro (2017), um cibercriminoso pode facilmente ludibriar os investigadores a acreditarem que ele está localizado num país estrangeiro, enquanto ele pode muito bem morar a algumas quadras de distância.

E as dificuldades não param por aí. O software livre The Onion Router[17] (TOR), ferramenta muito utilizada por cibercriminosos para cobrir seus rastros, permite uma conexão intermediada por vários servidores *proxies*, o que torna praticamente impossível se descobrir o IP real de onde partiu uma ação criminosa digital (SHIMABUKURO, 2017).

4.2 As Criptomoedas

Em alguns crimes, sobretudo nos crimes que envolvem ganhos financeiros, como os do colarinho branco, a estratégia de investigação mais utilizada é a *follow the money*, ou siga o dinheiro em português. A expressão *follow the money* ficou popular com o escândalo de *Watergate*, que culminou na renúncia do presidente americano Richard Nixon.

No episódio, repórteres, do Jornal The Washington Post, desvendaram um esquema espionagem para chantagear adversários políticos, comandado pelo então presidente, através de um cheque de 25 mil dólares depositados pelo comitê de campanha de Nixon na conta de um dos homens que invadiram os escritórios do Partido Democrata para implantar escutas. É por motivos como esse que movimentações bancárias são provas importantes para identificar uma lavagem de capitais, uma organização criminosa, desmascarar políticos corruptos ou grandes traficantes de drogas, por exemplo.

Acontece que a lavagem de dinheiro tradicional ficou obsoleta na era da criminalidade digital e a estratégia *follow the money* pode não ter mais a mesma

[17] O The Onion Router, conhecido simplesmente como TOR, é um software livre usado para manter o anonimato dos seus usuários na internet. Isso é possível através de um complexo mecanismo de transmissão de dados que faz com as comunicações em rede passem por diversas máquinas, o que torna muito complicado rastrear de onde a mensagem partiu inicialmente (PEREIRA, c2021).

eficácia, tendo em vista que existem à disposição criptomoedas simplesmente não são rastreáveis, como a famosa Bitcoin. Como explica Adriana Shimabukuro (2017):

> A principal característica do Bitcoin é a possibilidade de proteger a identidade do seu dono. Diferente da lavagem de dinheiro tradicional, que deixa rastros por onde as autoridades perseguem os criminosos, quando falamos em moedas digitais, temos interessados na aquisição de moeda procurando sites de câmbio que transformam o dinheiro ilícito em moeda legal, visto que o Bitcoin não tem meios de fiscalização ou supervisão por qualquer órgão regulamentador. Após a aquisição dos Bitcoins, o dinheiro pode ser reinjetado em novas transações legais, sem qualquer suspeita de sua origem.

Tendo isso em vista, não é atoa que o *Silk Road*[18] - site de comércio de produtos ilícitos - apenas admitia Bitcoins como forma de pagamento, ou ainda, não é atoa que cibercriminosos cobram resgate em Bitcoins para liberar máquinas atacadas por um *ransomware*. Assim, a grande dificuldade que envolve a investigação de cibercrimes, é que os cibercriminosos têm à disposição uma série de ferramentas que o permitem cobrir os rastros deixados pela sua ação criminosa. Embora haja muitos defensores, o surgimento das criptomoedas são diretamente responsáveis pela atual era de ouro dos cibercrimes.

4.3 Jurisdição e a transnacionalidade da rede

Não é nenhum segredo que a internet é um sistema informático transnacional que conecta computadores do mundo todo, por isso mesmo chamada também de rede mundial de computadores. O próprio Marco Civil da Internet reconhece a escala mundial da rede como um dos fundamentos do uso da rede no Brasil (art. 2º, I da Lei nº 12.965/14). Isso quer dizer, em termos geopolíticos, que a Internet não conhece fronteiras nacionais, pelo contrário, é uma rede homogênea em que uma pessoa que mora no Brasil pode acessar um site hospedado no outro lado do mundo com apenas um clique, sem precisar passar por nenhuma barreira alfandegária.

Se a Internet não conhece limites territoriais, os cibercrimes também não. Em outras palavras, um cibercriminoso pode, por exemplo, praticar um crime contra uma

[18] O Silk Road foi o maior comércio eletrônico de produtos ilícitos do mundo, criado por Ross William Ulbricht, o Dread Pirate Roberts, que foi preso pelo FBI em 2013 e condenado à prisão perpétua sob várias acusações. O Silk Road era um site acessível após várias camadas de *proxies* do sistema TOR, o que garantia o anonimato dos seus usuários. Neste site se vendiam de drogas ilícitas a contratos de assassinato de aluguel e a única forma de pagamento aceita eram criptomoedas. O site existiu por dois anos, de 2011 a 2013, quando foi fechado pelo FBI (G1, 2015).

vítima no Brasil, mesmo estando no seu apartamento em Moscou, na Rússia, e guardar o produto criminoso digital em um servidor localizado na Nova Zelândia, tudo isso em pouco tempo e sem levantar da cadeira. Nesse exemplo, percebe-se que a ação criminosa envolveu três países – mas poderia envolver muitos mais – e tudo isso causa problema para as jurisdições estatais.

Isto posto, a questão da territorialidade traz dois problemas: a lei brasileira pode ser aplicada ao caso? e o que fazer se as provas ou os investigados/processados se encontram fora do país?

O primeiro problema é facilmente resolvido pelo Direito Penal pátrio, haja vista que o art. 6º do Código Penal adota a seguinte redação: “Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado”.

Como ensina Rogério Greco (2016, p 210), existem três teorias para se definir o local onde o crime é praticado: a teoria da atividade, do resultado e a mista, ou da ubiquidade. A primeira considera o local do crime onde a conduta foi praticada, a segunda considera o local onde ocorreu o resultado e a terceira adota as duas teorias anteriores.

Com a redação do art. 6º, o Código Penal adotou a teoria da ubiquidade, o que resolve problemas relacionados aos crimes em que a ação ou omissão é praticada em um local, mas o resultado se dá em outro. É o caso dos crimes informáticos, que são crimes tipicamente praticados à distância. Se o Código Penal tivesse adotado qualquer das outras teorias, o Direito Penal brasileiro teria problemas em se aplicar a delitos informáticos, que muitas vezes têm vítimas e ofensores em países diferentes. Deste modo, se um cibercriminoso brasileiro, por exemplo, praticar um crime contra uma vítima em Portugal, ou vice-versa, o Direito Penal brasileiro se aplicará ao caso.

O segundo problema é que não é tão simples de se resolver. Embora a internet seja uma rede mundial, os servidores que hospedam *sites* são estruturas físicas computacionais que estão localizadas em algum país do mundo. Trazida essa premissa, logo se vê que o problema é uma questão de soberania.

A soberania, como explica o ilustre jurista Miguel Reale (2000, p. 157):

> Significa o Direito do Estado como pessoa jurídica de Direito público, e resolve-se, em última análise, no poder originário e exclusivo que tem o Estado de declarar e assegurar por meios próprios a positividade de seu Direito e de resolver, em última instância, sobre a validade de todos os ordenamentos jurídicos internos.

O citado autor (REALE, 2000, p. 157) ainda fala que soberania tem como sentido político externo, a condição de que o Estado é independente, é dizer, o soberano - seja um monarca ou um representante republicano – não está subordinado a nenhuma autoridade superior. Não havendo soberania, não há jurisdição, que é uma das funções da soberania, sendo um dos aspectos do poder estatal.

Com essa lição, tiramos o nosso problema: o Estado brasileiro tem soberania e jurisdição sobre o seu território e nele pode fazer valer, coercitivamente, suas decisões, o que já não ocorre com pessoas e empresas que estão localizadas em território estrangeiro, pois neste vigora a soberania e a jurisdição do respectivo Estado estrangeiro. Assim sendo, quando o processo depende de prova que está na posse de provedor ou servidor localizado geograficamente em outro país, dentre outras situações que podem ocorrer, a solução que resta é o pedido de cooperação internacional.

Esses pedidos, como explicam as Procuradoras da República Fernanda Teixeira Souza Domingos e Priscila Costa Schreiner Röder (DOMINGOS; RÖDER, 2017):

> Conhecidos como *Mutual Legal Agreement Treaties* (MLATs) – Acordos de Assistência Mútua em Matéria Penal, tradicionalmente têm um processamento muito lento, pois dependem de que os pedidos sejam feitos de forma correta, de que sejam traduzidos e enviados pelas autoridades competentes, para que uma autoridade no país requerido dê início à execução do pedido.

Além disso, as procuradoras completam dizendo que em muitas oportunidades, as empresas prestadoras de serviço pela internet que detém provas sobre delitos digitais não têm nenhum vínculo com o local onde se investiga, o que gera um imbróglio ainda maior para obtenção dessas provas.

Ademais, embora grande parte dos países respondam a pedidos de cooperação internacional, conforme informações do Ministério da Justiça (BRASIL, 2014), nada impede que esse pedido seja negado, ainda mais se os países não tiverem acordos nem boa relação diplomática.

O Brasil compõe uma série de tratados bilaterais que preveem assistência mútua em matéria Penal, como por exemplo, o tratado de cooperação jurídica penal

entre Brasil e Suíça (Decreto nº 6.974/2009), Brasil e México (Decreto nº 7595/2011), além de integrar as Convenções das Nações Unidas Contra a Corrupção (Decreto nº 5687/2006) e Contra o Crime Organizado Transnacional (Decreto nº 5.015/2004), que também preveem colaboração internacional. Entretanto há, desde de 2001, um importante tratado multilateral de combate ao crime cibernético internacional, o qual o Brasil não é parte, pelo menos até a redação deste texto: a Convenção de Budapeste.

4.4 A Convenção de Budapeste

A Convenção de Budapeste sobre cibercrimes foi firmado em 2001 no âmbito da União Europeia com artigos voltados para obrigar os Estados parte a implementar legislações para garantir que uma série de condutas relacionadas aos cibercrimes fossem tipificadas, a investigação fosse possível a cooperação internacional fosse garantida e célere entre os acordantes. Embora o tratado tenha sido firmado no âmbito da União Europeia, entre os países daquele bloco, ele é aberto para adesão de outros países, inclusive para o Brasil, que foi convidado a aderir ao tratado em 2020.

No segundo capítulo da convenção, há uma obrigatoriedade, por exemplo, de criminalizar condutas como a invasão de dispositivos informáticos para obter, eliminar ou alterar dados (arts. 2 e 4), a obstrução de sistemas informáticos (art. 5), a produção, posse e distribuição de malwares e dispositivos empregados no cibercrime (art. 6) e a falsificação informática (art. 7).

É perceptível que mesmo sem ter ainda aderido à convenção, o Brasil já se adequa a algumas dessas exigências, visto que já criminaliza condutas como invasão de dispositivos informáticos para obtenção, alteração ou obstrução de dados com art. 154-A do Código Penal, além da fabricação e disseminação de *malwares* com o §1º do art. 154-A do mesmo código.

Ainda assim, a adesão a Convenção de Budapeste tem um potencial de ajudar o país a fechar lacunas mencionadas neste trabalho, sobretudo pela redação dos artigos 5º e 7º deste tratado, que tem o seguinte conteúdo:

> Artigo 5º - Interferência em sistemas
>
> Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, a

> obstrução grave, intencional e ilegítima, ao funcionamento de um sistema informático, através da introdução, transmissão, danificação, eliminação, deterioração, modificação ou supressão de dados informáticos.
>
> Artigo 7º - Falsidade informática
>
> Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, a introdução, a alteração, a eliminação ou a supressão intencional e ilegítima de dados informáticos, produzindo dados não autênticos, com a intenção de que estes sejam considerados ou utilizados para fins legais como se fossem autênticos, quer sejam ou não directamente legíveis e inteligíveis. Uma Parte pode exigir no direito interno uma intenção fraudulenta ou uma intenção ilegítima similar para que seja determinada a responsabilidade criminal.

O artigo 5º recebe o nome de interferência em sistemas e cobra a tipificação da conduta de obstruir dolosamente o funcionamento de sistema informático, através da alteração ou eliminação de dados. Cumprindo esta obrigação, o Brasil tipificaria como crime o ataque de *ransomware*, que como explicado no capítulo específico, não se trata de uma invasão de dispositivo informático e atípico no Brasil, a não ser que o agente cobre um resgate para cessar a obstrução do sistema e dos arquivos da vítima, o que nem sempre ocorrerá.

Ademais, o art. 7º, de falsidade informática, a depender da forma como fosse implementado, seria uma oportunidade de tipificar essencialmente todos os ataques de *spoofing*, que consistem na alteração de dados para utilização fraudulenta, mesmo que não sejam de uso para fins legais, uma vez que o trecho final do artigo acrescenta que o direito interno pode exigir uma intenção fraudulenta ou similar, que poderia ser a de enganar sistemas informáticos.

Nas disposições em relação ao processamento dos crimes, a Convenção de Cibercrimes tem uma preocupação enfática na adoção de medidas legislativas para preservação de dados informáticos relativos ao tráfego de dados (art. 16), além de garantir um acesso rápido a esses dados pelas autoridades competentes (art. 17). Nesses quesitos, o Brasil não deixa a desejar, uma vez que o Marco Civil da Internet (Lei n 12.965/2014) já criou a obrigação dos provedores de internet e de administradores de sistemas autônomos de manter os registros de conexão, por determinado prazo, para estarem à disposição das autoridades, que podem requisitá-las, além de poderem requisitar acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço sem necessidade autorização judicial (art. 10, §3º da Lei nº 12.965/2014), o que torna o acesso mais célere a esses dados.

Por fim, chega-se ao ponto principal da Convenção de Budapeste: a cooperação internacional. Como foi bem explicado no subcapítulo 4.1.3, a Internet é uma rede que simplesmente não sofre limitação por fronteiras nacionais, o que transforma os cibercrimes em modalidade de crime essencialmente transnacional. Quer se dizer com isso que haverá facilmente casos de cibercrimes onde o criminoso se localiza num país A, a vítima num país B, e as provas estejam armazenadas em máquina localizada em país C.

É nesse contexto que a cooperação internacional se torna essencial e a Convenção de Budapeste é o único tratado internacional multilateral que obriga a cooperação entre as partes em matéria penal em relação a delitos informáticos (art. 23), além de asseverar que essa cooperação deva ser a mais ampla possível e realizada de forma célere (art. 25).

Para ser mais específico, uma parte pode pedir a outra, por exemplo, “para investigar ou aceder de forma semelhante, apreender, ou obter de forma semelhante, e divulgar dados armazenados por meio de sistema informático que se encontre no território dessa outra Parte” (art. 31). Por esses motivos apresentados, a adesão do Brasil à Convenção de Budapeste traz claras vantagens no âmbito do combate aos cibercrimes.

5 PROJETOS DE LEI EM TRAMITAÇÃO NO CONGRESSO NACIONAL E POSSÍVEIS ESTRATÉGIAS DE PREVENÇÃO

Para finalizar o trabalho, com as consequentes conclusões, resta fazer uma pesquisa de panorama, é dizer, após apontar lacunas na legislação penal brasileira em relação aos crimes cibernéticos resta verificar a possibilidade de essas lacunas se preencheram em um futuro breve, ao analisar projetos de lei em tramitação no Congresso Nacional.

5.1 PROJETO DE NOVO CÓDIGO PENAL (PL 236/2012 DO SENADO)

O primeiro Projeto de Lei (PL) a ser apresentado, certamente é o que o pode alterar mais significativamente o Direito Penal Brasileiro, incluindo em relação aos crimes cibernéticos, o PL nº 236/2012 do Senado. O referido é nada mais, nada menos, que o projeto de Novo Código Penal, que se aprovado, vem para substituir o Decreto-Lei nº 2848 de 1940, da era Vargas.

As alterações trazidas pelo projeto de Novo Código Penal são significativas. Além de unificar o Direito Penal Material, reunindo uma série de crimes previstos em Leis Penais Extravagantes, o projeto traz novos tipos penais relativos aos cibercrimes.

A primeira inovação que o Código pode trazer, se aprovado, é uma seção só para delitos informáticos (Título VI), com dois tipos penais (arts. 209 e 210) e um artigo de conceitos (art. 208). Além disso, o novo código cria duas figuras típicas diferentes para o que hoje é definido pelo crime de invasão de dispositivos informáticos (art. 154-A do Decreto-Lei nº 2848/40):

> Dano aos dados informáticos
> Art. 164. Destruir, danificar, deteriorar, inutilizar, apagar, modificar, suprimir, ou de qualquer outra forma, interferir indevidamente ou sem autorização em dados informáticos, ainda que parcialmente:
> Pena prisão, de seis meses a três anos.
> Parágrafo único. Na mesma pena incide quem produz, mantém, vende, obtém, importa ou por qualquer outra forma distribui, indevidamente, ou sem autorização, dispositivos, programas e outros dados informáticos, destinados a destruir, inutilizar ou deteriorar coisa alheia.
> (...)
> Acesso indevido
> Art. 209. Acessar, indevidamente ou sem autorização, por qualquer meio, sistema informático protegido, expondo os dados informáticos a risco de divulgação ou utilização indevida:
> Pena: prisão, de seis meses a um ano, ou multa.

> §1º Na mesma incorre quem, sem autorização ou indevidamente, produz, mantém, vende, obtém, importa, ou por qualquer outra forma distribui códigos de acesso, dados informáticos ou programas, destinados a produzir a ação descrita no caput deste artigo.

Com isso, o que hoje é um crime só com a mesma pena (art. 154-A do CP), passariam a ser duas figuras separadas, com probabilidades diferenciadas: danificar dados informáticos (art. 164 do PL) e acessar indevidamente sistemas informáticos (art. 209 do PL). Mas essa não é única inovação que esses artigos trazem, o art. 164 do PL tipifica o ataque de *ransomware* que criptografa dados das vítimas, por inutilizar sem autorização dados informáticos. O ataque de ransomware na modalidade bloqueio de sistema também não passaria impune no Novo Código Penal, pois receberia tipificação no art. 210:

> Sabotagem informática
> Art. 210. Interferir de qualquer forma, indevidamente ou sem autorização, na funcionalidade de sistema informático ou de comunicação de dados informáticos, causando-lhe entrave, impedimento, interrupção ou perturbação grave, ainda que parcial:
> Pena - prisão, de um a dois anos.

Deste modo, o ataque de *ransomware* estaria abarcado pelo Novo Código Penal, caso seja aprovado do jeito que está. Um grande ponto sobre esse PL é entender que a invasão de dispositivos informáticos não é um fim em si mesmo, é um meio empregado para realizar uma série de condutas de diferentes gravidades e reprovabilidade, como visto anteriormente.

Além disso, a invasão de dispositivos informáticos não é a única forma de realizar essas condutas nocivas, é dizer, nem todo ciberataque invade um dispositivo informático, outros meios podem ser empregados. Assim, o Novo Código Penal tem o potencial de preencher algumas das brechas apontadas pela pesquisa se aprovado, sobretudo em relação ao ataque de *ransomware*, que passaria a ser uma figura típica mesmo que o agente não pratique a extorsão.

Outra inovação seria a figura da fraude informática, inserida entre outras modalidades de fraudes patrimoniais, prevista no art. 170 do PL:

> Art. 170. Obter, para si ou para outrem, em prejuízo alheio, vantagem ilícita, mediante a introdução ou supressão de dados informáticos, ou interferência, por qualquer outra forma, indevidamente ou sem autorização, no funcionamento de sistema informático:
> Pena - de prisão, de uma a cinco anos.

Com essa redação, a fraude informática poderia tipificar os ataques de *spoofing*, que consistem em fraudes perpetradas pela interferência no funcionamento de sistemas informáticos, como adulteração de dados, contudo, cai em problemas já discutidos aqui, a fraude perpetrada pelo ataque de *spoofing* nem sempre terá caráter patrimonial. Assim, embora o artigo feche mais as brechas em relação ao ataque de *spoofing*, deixa uma aberta. De toda forma, o artigo reforça a ideia de que o PL entende que nem todos ataques cibernéticos são realizados com invasão de dispositivos, sendo um meio para atingir diferentes resultados.

5.2 PROJETO DE LEI 5278/20 DA CÂMARA DOS DEPUTADOS

Tramita ainda no Congresso Nacional o PL 5278/20, que propõe aumentar a pena do atual crime de invasão de dispositivos (art. 154-A do CP) para 4 a 10 anos de reclusão, pois segundo o autor do PL, o Deputado Luizão Goulart, a pena do referido crime é muito branda diante do avanço dos cibercrimes.

A opinião de que a pena do crime é muito branda não está necessariamente errada, mas o projeto é problemático levando em conta que a invasão de sistemas não é um fim em si mesmo e sim um meio empregado para realizar uma série de condutas de diferentes níveis de nocividade e reprovabilidade. Sendo assim, atribuir uma pena mais alta puramente ao ato de invadir sistemas informáticos não presta um bom serviço ao princípio da individualização da pena.

Neste aspecto, o projeto de Novo Código Penal parece acertar mais ao individualizar as condutas pelo objetivo e pelo resultado e não pelo meio empregado, afinal, o invasor do dispositivo pode ter as mais diferentes intenções, desde extorquir a vítima, aplicar uma fraude financeira ou apenas se divertir causando transtorno as vítimas, por exemplo. Além disso, o PL não fecha nenhuma das brechas propostas pelo trabalho, sendo mero recrudescimento penal.

5.3 POSSÍVEIS ESTRATÉGIAS DE PREVENÇÃO DE CRIMES CIBERNÉTICOS

O trabalho até aqui tem se focado na tipificação penal e outros problemas relacionados à repressão penal de crimes cibernéticos, mas não pode ser ignorado que

repressão penal de forma isolada pode não ser suficiente para reduzir a incidência das práticas criminosas cibernéticas, como não parece ser nos crimes tradicionais. O professor Eduardo Viana (2020, p. 418), falando sobre prevenção de delitos no contexto da criminologia, explica que a criminologia moderna observa um panorama mais complexo que a política penal, ao invés de prestar atenção somente no criminoso, também se leva em consideração a figura da vítima e da comunidade para identificar fatores criminógenos de risco e elaborar estratégias de prevenção.

Em outras palavras, uma política de prevenção de crimes deve observar e combater fatores que aumentam o risco de ocorrência de crimes. Sem querer se estender muito no tema da criminologia, há uma multiplicidade de fenômenos que originam o crime (VIANA, 2020, p. 428). Esses fenômenos vão desde desigualdade social até a escassez de vigilância policial e outros fatos que aumentam as oportunidades de se delinquir com chances de impunidade.

O problema dos crimes cibernéticos é que esses fogem a lógica dos crimes tradicionais e fatores como vigilância policial ou iluminação de vias não têm como influir no aumento ou diminuição desses crimes.

A maioria dos ataques pode ser dificultado com investimentos em ferramentas de cibersegurança, como os *malwares* que são combatidos por *softwares* antivírus, mas acontece que nenhum antivírus é capaz de prevenir 100% contra qualquer ameaça. Para isso, basta lembrar que relatório da Kaspersky Lab (2013) concluiu que mais de 315 mil novos softwares maliciosos surgem todos os dias e os antivírus não conseguem atualizar sua base de dados nessa mesma velocidade para identificar todos os novos *malwares* que são criados todos os dias. É o que diz matéria de Fernando Daquino (2010), no site Tecmundo, que fala que nenhum antivírus pode ser considerado totalmente eficiente, devido a desatualização de sua base de dados, entre outros fatores.

A notícia boa é que a informação pode ser a melhor arma para evitar que um indivíduo se torne vítima de grande parte dos cibercrimes, sobretudo os mais praticados, que envolvem fraudes financeiras, *spoofing* e *phishing*. Basta lembrar da matéria do Fantástico (2021) que noticiou que cerca de 60 milhões de brasileiros já sofreram fraude financeira na internet, mas não é só isso, a matéria revela também a

maioria das vítimas têm a percepção de que são as grandes culpadas por terem caído na fraude, seja por falta de atenção ou de informação.

Pegando como exemplo o *phishing*, o cibercriminoso tenta, como já foi dito, coletar informações sigilosas da vítima se utilizando de alguma fraude. Um método bem utilizado é mandar um e-mail se passando por alguma empresa a qual a vítima é cliente pedindo informações, mas se a vítima for cuidadosa e informada e observar o endereço de e-mail do remetente, pode perceber a fraude.

A citada matéria do Fantástico (2021) dá dicas de alguns cuidados ao realizar compras pela internet pode prevenir boa parte das fraudes praticadas contra consumidores na internet, como verificar o código dos boletos bancários ante de efetuar o pagamento, verificar o CNPJ da loja, verificar se há reclamações e outras qualificações da loja, etc. Uma das fraudes mais citadas na matéria citada (FANTÁSTICO, 2021) é o golpe do Whatsapp, que pode ser classificado como *spoofing*, em que os farsantes clonam o Whatsapp de uma pessoa e começam a interagir com pessoas conhecidas da vítima para praticar fraudes financeiras. O fato é que a utilização da nova ferramenta de segurança de verificação por duas etapas pode reduzir drasticamente o número de fraudes praticadas com essa estratégia, basta que a informação chegue ao número mais amplo de pessoas.

É sabendo da importância da informação no combate aos cibercrimes que há, no âmbito da União Europeia, algumas iniciativas para informar a população sobre cibersegurança. Uma delas são os avisos públicos e os guias de prevenção da Europol. No site da Europol (c2021) é possível encontrar uma ampla gama de guias sobre como funcionam os principais golpes que estão sendo praticados pela internet e como preveni-los. Uma iniciativa como essa seria muito positiva se aplicada no Brasil e seria muito importante para reduzir a quantidade de pessoas que caem nesses golpes todos os anos no país.

Essa não é a única iniciativa no âmbito da União Europeia para prevenção de cibercrimes, tem outros e um em especial merece menção neste trabalho: o *No More Ransom* (www.nomoreransom.org). Esse site é um esforço conjunto da Europol e empresas de cibersegurança como a Kaspersky e McAfee para combater os ataques de *ransomwares*. No site do projeto *No More Ransom*, é possível encontrar informações importantes, dicas de prevenção valiosas, espaço para reportar crimes e o

mais interessante, há uma série de *ransomwares* que o projeto já consegue anular os efeitos na máquina da vítima.

Há ainda outras iniciativas interessantes, como o *Anti-Phishing Working Group* (c2021), que traz muitas informações sobre como prevenir ataques de *phishing*. O fato é que, as principais técnicas para se combater ameaças cibernéticas envolvem informação e uso de tecnologia, ou seja, se combate tecnologia da informação, com tecnologia da informação.

CONCLUSÃO

Os crimes cibernéticos, ou cibercrimes, seguem uma tendência forte de crescimento nos últimos anos e seu potencial é assustador. Exemplos como o assalto virtual de 80 milhões de dólares ao Banco de Bangladesh são apenas uma porção do que pode ser feito em termos de crimes por meios digitais.

Com o avanço da tecnologia, mais e mais máquinas se integram ao processo chamado de internet das coisas e se conectam às redes. O problema desse processo, é que mais máquinas conectadas a internet são mais máquinas ao alcance de cibercriminosos. Isso quer dizer que em breve, não apenas os computadores tradicionais poderão ser alvos de ciberataques, mas a geladeira, o carro etc.

Em que pese o perigo gritante e atual potencial dos cibercrimes, que aliás já era anunciado há um certo tempo, só há como concluir que a legislação penal brasileira é deficitária em relação aos cibercrimes havendo lacunas e condutas graves que podem passar impunes por falta de uma tipificação mais específica, além de haver desproporcionalidade por deficiência na proteção de bens jurídicos tutelados pelo ordenamento jurídico pátrio.

O crime de invasão de dispositivos móveis (art. 154-A do CP) já foi um grande avanço, visto que antes disso o fato era simplesmente atípico no Brasil, mas há uma crença equivocada de que este crime resolve todos os problemas de tipificação de cibecrimes, quando na verdade cobre apenas parte delas. Nem todos ataques cibernéticos, como mostrado, são praticados invadindo dispositivos informáticos, muitos são praticados até com uma grande ajuda da vítima, que ludibriada, contribui para o ataque funcionar, o que não faz com que as condutas sejam menos graves.

Além disso, a invasão de dispositivos informáticos não é um fim em si mesmo, mas um meio empregado para obter diferentes resultados, com diferentes gravidades, motivo pelo qual mereceriam diferentes penas. Não é só isso, o tipo penal não traz nenhuma diferenciação em termos de pena pelo sistema que foi invadido, o que pode ser considerado uma lacuna, uma vez que os sistemas críticos oferecem um risco muito superior a sociedade do que sistemas não críticos e o princípio da individualização da pena exige que a conduta seja punida levando em conta essa circunstância.

O *phishing* é o tipo de ataque cibernético mais praticado para subsidiar uma série de outras fraudes financeiras graves, pois é uma forma muito simples de se conseguir dados sigilosos da vítima sem precisar realizar qualquer invasão de dispositivos ou outro ataque mais técnico, mas, ainda assim, a conduta em si é penalmente atípica no Brasil.

Em que pese a importância dada recentemente aos dados pessoais, inclusive com a edição da LGPD e a criação da Autoridade Nacional de Dados, a legislação penal brasileira peca em não tipificar a conduta de vazar dados pessoais, o que está em descompasso com a importância dessas informações, que são pedras preciosas nas mãos de cibercriminosos e golpistas de todo tipo.

Também é atípico no Direito Penal pátrio o ataque de negação de serviço, que tem um potencial de causar danos graves, sobretudo às empresas de comércio eletrônico ou cuja atividade depende diretamente dos seus servidores. Como foi visto, embora uma a forma mais comum de realizar este ataque seja por meio de invasão de computadores para criar um “rede zumbi”, isso não é necessário, basta que o atacante tenha uma máquina potente o suficiente, ou um conjunto de máquinas para realizar o ataque sozinho, sendo uma conduta simplesmente atípica, independente do dano que possa causar.

O ataque com *ransomwares* é uma forma comum de se praticar extorsão no âmbito do crime cibernético, mas nada impede que hacker não cobre qualquer resgate da vítima, criptografando ou bloqueando o sistema das vítimas por pura diversão. Neste caso, estaremos diante de um fato penalmente atípico, pois não há extorsão e também não há invasão de dispositivo informático.

De forma semelhante, o ataque de *spoofing* é outra figura, que puramente considerada, é penalmente atípica no Brasil, dependendo de outras circunstâncias para se amoldar a alguma figura típica existente, como a prática de estelionato ou a interceptação não autorizada de comunicação informática. Com isso há uma brecha na legislação, pois o *spoofing* por si já é uma fraude que atenta contra a confiabilidade e o bom funcionamento dos sistemas informáticos.

No âmbito da investigação e repressão dos crimes cibernéticos há vários desafios, a começar pela transnacionalidade da rede e portanto, a transnacionalidade

da prática deste tipo de crimes e das provas a serem colhidas. Tal fato obriga as nações a dependerem da cooperação internacional para solucionar crimes cibernéticos, o que pode trazer incerteza e lentidão ao processo e às investigações. Uma forma de amenizar esse problema é a adesão do Brasil à Convenção de Budapeste, que pode acelerar essa cooperação internacional com uma série de países da União Europeia e de fora.

Outro desafio para as investigações é que os meios clássicos de identificação da autoria de crimes não funcionam para os crimes cibernéticos. O meio capaz de se criar uma linha investigativa para identificar a autoria do crime é por meio da identificação do endereço IP de onde partiu o ataque. O problema que há nisso é que os cibercriminosos podem esconder seus endereços IP por trás de várias camadas de *Proxies*, o que dificulta muito o trabalho investigativo e exige muita capacidade técnica dos órgãos investigativos.

Ademais, a estratégia *follow the money* não é muito eficaz quando se trata de crimes cibernéticos, visto que há uma forte tendência de se utilizar criptomoedas irrastreáveis, como a Bitcoin, para cobrar resgates e comercializar produtos ilícitos na *deep web* entre outros meios de circulação de valores produtos do crime na internet. A verdade é que as criptomoedas facilitam muito a obtenção de lucro criminoso na internet e têm relação direta com a era de ouro dos cibercrimes.

Ao analisar as mudanças que podem ocorrer em curto período de tempo, é positivo ver que o PL 236 do Senado (Projeto de Novo Código Penal) fecha algumas das brechas apontadas, ao tipificar o ataque de *ransomware* e reduzir as hipóteses em que o ataque de *spoofing* será atípico, mas a principal inovação que o PL pode trazer é uma mudança no entendimento da invasão de dispositivos informáticos. O Novo Código Penal, se aprovado do jeito que está no projeto original, deixa de lado o crime de invasão de dispositivos informáticos, e tipifica o objetivo final das condutas dos cibercriminosos, é dizer, segue a visão defendida no trabalho de que a invasão de dispositivos móveis é um meio empregado, uma ferramenta, para se atingir os mais diversos objetivos. Tal mudança é muito positiva, reduz a brechas e aumenta a individualização das condutas de acordo com seus graus de reprovabilidade.

Por fim, o trabalho trouxe possíveis estratégias de prevenção de crimes cibernéticos, para além da abordagem penal. Em razão das peculiaridades

tecnológicas, estratégias tradicionais de prevenção, como reforço de policiamento ostensivo não surtem efeito nos crimes cibernéticos. No entanto, foi demonstrado no trabalho como a informação é a principal estratégia para prevenir uma série de fraudes praticadas pela internet, ataques de *phishing* e *spoofing*, uma vez que os cibercrimes que praticam esses ataques cibernéticos contam sobremaneira com a falta de atenção e informação da própria vítima para o golpe funcione.

Uma série de iniciativas já são praticadas por órgãos e organizações do âmbito da União Europeia para prevenir crimes cibernéticos como cartilhas de informações bem acessíveis e dicas de prevenção da Europol, sites informativos como o do *Anti-Phishing Working Group* e o site do *No More Ransom*, iniciativas que podem ser copiadas no âmbito nacional.

Ao final, resta apenas concluir que todas as hipótese lançadas na introdução foram confirmadas, quer-se com isso dizer: a) a maioria da principais condutas antijurídicas praticadas na internet não gozam de tipificação própria e apenas recebem atenção penal quando o ataque cibernético é um meio empregado para realização de outros crimes, como o estelionato; b) o crime de invasão de dispositivos informáticos, embora tipificado, não prevê uma pena diferenciada para a invasão de sistemas críticos, o que está em desacordo com princípio constitucionais como a individualização da pena; c) os crimes cibernéticos impõe novos desafios à investigação criminal, sendo que alguns desses desafios são difíceis de superar; e d) existem estratégias de prevenção aos crimes cibernéticos já bastante difundidas no âmbito da União Européia e que podem ser replicadas sem maiores problemas no Brasil.

REFERÊNCIAS

13 ATAQUES FULMINANTES DO GRUPO HACKER ANONYMOUS**. EXAME**, 2011. Disponível em: <https://exame.com/tecnologia/13-ataques-fulminantes-do-grupo-hacker-anonymous/> Acesso em: 25 jan. 2021.

ARAÚJO, Laysa Bernardes Marques de. Dinamite. **Brasil Escola**, c2021. Disponível em: <https://brasilescola.uol.com.br/quimica/dinamite.html>. Acesso em 13 abr. de 2021.

ARP SPOOFING: ATAQUE ÀS REDE LOCAIS. **We Live Security**, 2017. Disponível em: <https://www.welivesecurity.com/br/2017/11/07/arp-spoofing-ataque-as-redes-locais/> Acesso em: 25 fev. 2021.

BECCARIA, Cesare. **Dos Delitos e das Penas**. Ridendo Castigat Mores, 2001. Disponível em: <http://www.dominiopublico.gov.br/download/texto/eb000015.pdf> Acesso em 14 de abr. 2021.

BELSIC, Ivan. O guia essencial sobre phishing: Como funciona e como se proteger. **AVAST**, 2020. Disponível em: <https://www.avast.com/pt-br/c-phishing> Acesso em 1 fev. 2021.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal**. 17 ed. São Paulo: Saraiva, 2012.

BORTOT, Jéssica Fagundes. Crimes Cibernéticos: aspectos legislativos e implicações na persecução penal com base nas legislações brasileira e internacional. **VirtuaJus**. v. 2, n. 2, Belo Horizonte, 2017.

BRASIL É CONVIDADO A ADERIR À CONVENÇÃO DO CONSELHO DA EUROPA CONTRA CRIMINALIDADE CIBERNÉTICA. **Governo do Brasil**, 2020. Disponível em: <https://www.gov.br/secretariageral/pt-br/noticias/2020/julho/brasil-e-convidado-a-aderir-a-convencao-do-conselho-da-europa-contra-a-criminalidade-cibernetica#:~:text=Conven%C3%A7%C3%A3o%20contra%20a%20Criminalidade%20Cibern%C3%A9tica,o%20combate%20ao%20crime%20cibern%C3%A9tico.> Acesso em 8 mar. 2021.

BRASIL. Câmara dos Deputados. Projeto de Lei PL 5278/2020. Altera o art. 154-A do Código Penal. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node0a6r11qm4v5td72ss345vzjdw2930374.node0?codteor=1944233&filename=PL+5278/2020> Acesso em: 9 mar. 2021.

BRASIL. **Código Penal**. Decreto-Lei nº 2.848 de 7 de dezembro de 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm> Acesso em: 25 jan. 2021.

BRASIL. Constituição de 1988. **Constituição da República Federativa do Brasil**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso em: 25 jan. 2021.

BRASIL. **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. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em: 25 jan. 2021.

BRASIL. Ministério da Justiça. **Cooperação Jurídica Internacional em Matéria Penal.** Disponível em: <https://www.justica.gov.br/sua-protecao/lavagem-de-dinheiro/institucional-2/publicacoes/arquivos/cartilha-penal-09-10-14-1.pdf> Acesso em: 5 mar. 2021.

BRASIL. Ministério da Justiça. Polícia Federal. Inquérito Policial Operação Spoofing. Disponível em: <https://static.poder360.com.br/2019/12/relatorioPF-operacaospoofing-18dez2019-pt2.pdf> Acesso em: 26 fev. 20121.

BRASIL. Ministério Público Federal. Denúncia Operação Spoofing, 2020. Disponível em: <http://www.mpf.mp.br/df/sala-de-imprensa/docs/denuncia-spoofing> Acesso em: 26 fev. 2021.

BRASIL. Senado Federal. Projeto de Lei PL 236/2012. Anteprojeto de Código Penal. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=3515262&ts=1613697834640&disposition=inline> Acesso em: 9 mar. 2021.

BRASIL. Tribunal de Justiça do Rio Grande do Sul (TJRS - 7ª Câmara Criminal). **Apelação 70049844483**. Crimes contra o patrimônio. Furto qualificado pelo abuso de confiança. Cópia de arquivos e documentos informáticos. Atipicidade da conduta. Relatora: Des. Naele Ochoa Piazzeta, Julgamento: 29/04/2014. Disponível em: <https://tj-rs.jusbrasil.com.br/jurisprudencia/120128469/apelacao-crime-acr-70049844483-rs> Acesso em 12 fev. 2021.

CABRAL, Danilo César. O que foi o escândalo Watergate? **Superinteressante**, 2011. Disponível em: <https://super.abril.com.br/mundo-estranho/o-que-foi-o-escandalo-watergate/> Acesso em: 4 mar. 2021.

CARVALHO, Rodrigo César Picon de. O crime de subtração de dados pessoais. **Canal Ciências Criminais**, 2020. Disponível em: <https://canalcienciascriminais.com.br/o-crime-de-subtracao-de-dados-pessoais/> Acesso em: 12 fev. 2021.

CHAVES, Cristiano; ROSENVALD, Nelson. **Curso de Direito Civil.** 13 ed. São Paulo: Atlas, 2015.

CIPOLI, Pedro. O que é DNS? **Canaltech**, c2021. Disponível em: <https://canaltech.com.br/internet/o-que-e-dns/> Acesso em 29 abr. 2021.

CONFESSORE, Nicholas. Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. **New York Times,** 2018. Disponível em: <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.ht

ml> Acesso em: 12 fev. 2021.

CONHEÇA A HISTÓRIA DA INTERNET, SUA FINALIDADE E QUAL O CENÁRIO ATUAL. **Rockcontent**, 2020. Disponível em: <https://rockcontent.com/br/blog/historia-da-internet/> Acesso em: 25 jan. 2021.

CONVENÇÃO sobre Cibercrime = CONVENTION on Cybercrime. 23 novembro 2001. Disponível em:<http://www.mpf.mp.br/atuacao-tematica/sci-en/rules-and-legislation/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf> Acesso em: 8 mar. 2021.

CORRONS, Louis. Quando 'hackear' deixou de ser diversão e virou cibercrime? **Tecmundo**, 2021. Disponível em: <https://www.tecmundo.com.br/seguranca/210253-hackear-deixou-diversao-virou-cibercrime.htm> Acesso em: 25 jan. 2021.

CRESPO, Marcelo. Ataques DoS e DDoS: anotações em face do ordenamento jurídico penal brasileiro. **Jusbrasil**, 2015. Disponível em: <https://canalcienciascriminais.jusbrasil.com.br/artigos/229897612/ataques-dos-e-ddos-anotacoes-em-face-do-ordenamento-juridico-penal-brasileiro> Acesso em: 27 jan. 2021.

CRIADOR DO SITE SILK ROAD É CONDENADO À PRISÃO PERPÉTUA. **G1**, 2015. Disponível em: <http://g1.globo.com/tecnologia/noticia/2015/05/criador-do-site-silk-road-e-condenado-prisao-perpetua.html> Acesso em: 5 mar. 2021.

CUNHA, Rogério Sanches. **Manual de Direito Penal**. 8 ed. Salvador: JusPODIVM, 2016.

DAQUINO, Fernando. Mito ou verdade: dá para confiar em antivírus? **Tecmundo**, 2010. Disponível em: <https://www.tecmundo.com.br/antivirus/4252-mito-ou-verdade-da-para-confiar-em-antivirus-.htm> Acesso em 14 abr. 2021.

DESAFIOS E BENEFÍCIOS DAS SOLUÇÕES DE PAGAMENTO DETALHADOS EM PESQUISAS A PARTIR DE UMA PERSPECTIVA GLOBAL. **BCD Travel.** UTRECHT, Holanda – 25 de abril de 2019. Disponível em: <https://www.bcdtravel.com/o-futuro-dos-pagamentos-virtuais-explorado-em-estudo-de-caso-da-bcd-travel/?lang=pt-br> Acesso em: 25 jan. 2021.

DEZ HACKERS FAMOSOS E SEUS EFEITOS. **Terra**, c2021. Disponível em: <https://www.terra.com.br/noticias/tecnologia/infograficos/hackers/hackers-09.htm> Acesso em 30 de Jan. de 2021.

DIMOULIS, Dimitri; MARTINS, Leonardo. **Teoria Geral dos Direitos Fundamentais**. 5 ed. São Paulo: Atlas, 2014.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro**. 33 ed. São Paulo: Saraiva, 2016.

DOMINGOS, Fernanda Teixeira Souza; RÖDER, Priscila Costa Schreiner. Obtenção de provas digitais e jurisdição na Internet. In: BRASIL. Tribunal Regional Federal da 3ª Região. Escola de Magistrados. **Investigação e prova nos crimes cibernéticos.** São Paulo: EMAG, 2017.

DUARTE, Otto Carlos Luiz Bandeira. Denial of Service - Negação de Serviço. **GTA - UFRJ**, [2006]. Disponível em: <https://www.gta.ufrj.br/grad/06_1/dos/index.html> Acesso em: 18 fev. 2021.

ELEIÇÕES E ATAQUE HACKER AO STJ MARCARAM O MÊS DE NOVEMBRO. **Consultor Jurídico**, 2020. Disponível em: <https://www.conjur.com.br/2020-dez-31/eleicoes-ataque-hacker-stj-marcaram-mes-novembro> Acesso em: 25 jan.2021.

ENTENDA O CIBERATAQUE QUE AFETOU MAIS 200 MIL PCS EM 150 PAÍSES. **Olha Digital**, c2019. Disponível em: <https://olhardigital.com.br/especial/wannacry/> Acesso em 15 fev. 2021.

ESCUDEIRO, Leo. Apenas 0,1% das vítimas do ransomware WannaCry pagou o resgate dos dados. **Gizmodo**, 2017. Disponível em: <https://gizmodo.uol.com.br/vitimas-wannacry-resgate/> Acesso em: 15 fev 2021.

FONTES, José Igor Alves. **Dados Pessoais Digitais e seu tratamento no ordenamento jurídico brasileiro**. 2018. Monografia. Universidade Federal do Rio Grande do Norte, 2018.

FRANCO, Alberto Silva. **Crimes Hediondos**. 4 ed. São Paulo: Revista dos Tribunais, 2000.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 4 ed. São Paulo: Atlas, 2002.

GOGONI, Ronaldo. O que é IP? **Tecnoblog**, 2019. Disponível em: <https://tecnoblog.net/290145/o-que-e-ip/> Acesso em 19 abr. 2021.

GOMES, Luiz Flávio. **Interceptação telefônica**: comentários à Lei 9.296/1996. São Paulo: Ed. RT, 2011.

GOODMAN, Marc. **Future Crimes**. São Paulo: HSM Editora, 2015.

GRECO, Rogério. **Curso de Direito Penal**. 17 ed. Rio de Janeiro: Impetus, 2015.

INVADIR. *In:* MICHAELIS, Dicionário Brasileiro de Língua Portuguesa. Editora Melhoramentos, 2021. Disponível em: <https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/invadir#:~:text=1%20Entrar%20%C3%A0%20for%C3%A7a%20em,tomar%3A%20%C3%81tila%20invadiu%20a%20G%C3%A1lia.&text=2%20fig%20Assumir%20indevidamente%3B%20assenhorear,Detestava%20que%20invadissem%20suas%20atribui%C3%A7%C3%B5es.> Acesso em: 1 fev. jan. 2021.

JÚNIOR, Walter Nunes da Silva. **Curso de Direito Processual Penal**: Teoria (Constitucional) do Processo Penal. 2 ed. Natal: OWL, 2015.

KASPERSKY SECURITY BULLETIN 2013. **Kaspersky Lab**, 2013. Disponível em:<https://media.kaspersky.com/pdf/KSB_2013_EN.pdf> Acesso em: 25 jan. 2021.

LEYDEN, John. Polish teen derails tram after hacking train network. **The Register**. 11 de janeiro de 2008. Disponível em: <https://www.theregister.com/2008/01/11/tram_hack/> Acesso em: 25 jan. 2021.

LUDGERO, Paulo Ricardo. Despojar dados pessoais é crime? **Jusbrasil**, 2020. Disponível em: <https://ludgeroadvocacia.jusbrasil.com.br/artigos/878053566/despojar-dados-pessoais-e-crime> Acesso em: 12 fev. 2021.

MAIS DE 60 MILHÕES DE BRASILEIROS JÁ SOFRERAM COM FRAUDE FINANCEIRA NA INTERNET, DIZ PESQUISA. **G1**, 2021. Disponível em: <https://g1.globo.com/fantastico/noticia/2021/01/31/mais-de-60-milhoes-de-brasileiros-ja-sofreram-com-fraude-financeira-na-internet-diz-pesquisa.ghtml> Acesso em 8 fev. 2021.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas, 2003.

MASSON, Cleber. **Direito Penal Esquematizado**. 9 ed. Rio de Janeiro: Forense; São Paulo: MÉTODO, 2015.

MEGAVAZAMENTO DE DADOS DE 223 MILHÕES DE BRASILEIROS: O QUE SE SABE E O QUE FALTA SABER. **G1**, 2021.Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml> Acesso em: 12 fev. 2021.

MILLS, Elinor. Hacker says he broke into Texas water plant, others. **CNET**, 2011. Disponível em: <https://www.cnet.com/news/hacker-says-he-broke-into-texas-water-plant-others/#:~:text=A%20twentysomething%20hacker%20said%20today,at%20an%20Illinois%20water%20plant> Acesso em: 25 jan. 2021.

MORAES, Marina. Físico consegue achar vilão do ciberespaço. **Folha de São Paulo**, São Paulo, quarta-feira, 22 de fevereiro de 1995. Disponível em: <https://www1.folha.uol.com.br/fsp/1995/2/22/informatica/7.html> Acesso em: 25 jan. 2021.

NASCIMENTO, Talles Leandro Ramos. Crimes Cibernéticos. **Conteúdo Jurídico**, Brasília: 19 jan 2021. Disponível em: <https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos>. Acesso em: 25 jan. 2021.

NO MORE RANSOM! c2021. Disponível em: <https://www.nomoreransom.org/pt/index.html> Acesso em 15 abr. 2021.

O Dilema das Redes. Direção de Jeff Orlowski. Estados Unidos: Netflix, 2020.

O QUE É DOS E DDOS. **Canaltech**, c2021. Disponível em: <https://canaltech.com.br/produtos/o-que-e-dos-e-ddos/> Acesso em: 14 fev. 2021.

O QUE É UM RASONWARE? **KASPERSKY**, c2021. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/what-is-ransomware> Acesso em: 15 fev 2021.

O QUE SÃO ATAQUES DE DDOS? **Kaspersky,** c2021. Disponível em: <https://www.kaspersky.com.br/resource-center/threats/ddos-attacks> Acesso em: 14 fev. 2021.

O QUE SE SABE SOBRE A OPERAÇÃO SPOOFING E O HACKER QUE INTERCEPTOU AS MENSAGENS DAS AUTORIDADES. **G1**, 2019. Disponível em: <https://g1.globo.com/politica/noticia/2019/07/24/o-que-se-sabe-sobre-a-operacao-spoofing-e-os-suspeitos-de-interceptar-mensagens-de-autoridades.html> Acesso em: 26 fev. 2021.

OLIVEIRA, Sílvio Luís Martins de. A Internet das Coisas e o fim do mundo. **Escola de Magistrados do Tribunal Regional da 3ª Região**. São Paulo, 2017.

PASQUALOTTO, Adalberto. **Consultor Jurídico, 2019**. Disponível em: <https://www.conjur.com.br/2019-mai-20/pasqualotto-livre-iniciativa-efeitos-sociais-atividade-economica> Acesso em: 12 fev 2021.

PASSARINHO, Natália. Como megavazamentos de dados acontecem e por que é difícil se proteger deles. **BBC News Brasil**, 2021. Disponível em: <https://www.bbc.com/portuguese/brasil-56031998> Acesso em: 12 fev. 2021.

PELUSO, Cezar; et al. **Código Civil Comentado**. 7 ed. Barueri: Manole, 2013.

PEREIRA, Dimitri. Saiba o que é a Tor e como essa rede garante o seu anonimato na Web. **Canaltech**, c2021. Disponível em: <https://canaltech.com.br/internet/saiba-o-que-e-tor-e-como-essa-rede-garante-o-seu-anonimato-na-web/> Acesso em 29 abr. 2021.

PINHEIRO, Patrícia Peck. **Direito Digital**. 4. ed. São Paulo: Saraiva, 2010.

PREVENTING CYBERCRIME**. Council of Europe**, c2021. Disponível em: <https://www.coe.int/en/web/cybercrime/preventing-cybercrime> Acesso em 15 abr. 2021.

POSEY, Brien. Backdoor (computing). **TechTarget**, 2021. Disponível em: <https://searchsecurity.techtarget.com/definition/back-door> Acesso em 29 abr. 2021.

PUBLIC AWARENESS AND PREVENTION GUIDES. **Europol**, c2021. Disponível em:

<https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides> Acesso em 15 abr. 2021.

QUAIS SÃO OS DIFERENTES TIPOS DE RANSOMWARE? **Kaspersky**, c2021. Disponível em: <https://www.kaspersky.com.br/resource-center/threats/ransomware-examples> Acesso em: 15 fev 2021.

RANSOMWARE RYUK CONTINUA A ATACAR. **CryptoID**, 2020. Disponível em: <https://cryptoid.com.br/banco-de-noticias/ransomware-ryuk-continua-a-ataca/> Acesso em: 15 fev 2021.

REALE, Miguel. **Teoria do Estado e do Direito**. 5 ed. São Paulo: Saraiva, 2000.

REDES - SABE PARA QUE SERVE O PROTOCOLO ARP? **Pplware**, 2011. Disponível em: <https://pplware.sapo.pt/microsoft/windows/redes-sabe-para-que-serve-o-protocolo-arp/> Acesso em 29 abr. 2021.

REDES - SABE O QUE SÃO ENDEREÇOS FÍSICOS E ENDEREÇOS LÓGICOS? **Pplware**, 2010. Disponível em: <https://pplware.sapo.pt/tutoriais/networking/redes-%e2%80%93-sabe-o-que-sao-enderecos-fisicos-e-enderecos-logicos/> Acesso em 29 abr. 2021.

REGAN, Joseph. O que é malware? Como malwares funcionam e como se livrar deles. **AVG**, 2019. Disponível em: <https://www.avg.com/pt/signal/what-is-malware> Acesso em: 28 jan. 2021.

RIBEIRO, Celina Ferreira. Sistemas Críticos. **Devmedia**. 2010. Disponível em: <https://www.devmedia.com.br/sistemas-criticos/18952> Acesso em: 25 jan. 2021.

ROMANI, Bruno. Vazamento de 220 milhões de CPFs pode ser o mais lesivo do Brasil, diz especialista. **Terra**, 2020. Disponível em: <https://www.terra.com.br/noticias/tecnologia/vazamento-de-220-milhoes-de-cpfs-pode-ser-o-mais-lesivo-do-brasil-diz-especialista,b4886dc5c300eb51347be95041aa76b3rz8wr9cr.html> Acesso em 12 fev. 2021.

ROUBO DE SENHAS: SAIBA COMO FUNCIONA UM ATAQUE DE DNS SPOOFING. **We Live Security**, 2018. Disponível em: <https://www.welivesecurity.com/br/2018/01/29/como-funciona-um-ataque-dns-spoofing/> Acesso em: 25 fev. 2021.

ROXIN, Claus. **Estudos de Direito Penal**. Rio de Janeiro: Renovar, 2006.

SANGER, David E. Obama Order Sped Up Wave of Cyberattacks Against Iran. **The New York Times**, 2012. Disponível em: <https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html> Acesso em: 11 fev. 2021.

SAYTSON, Thiago; PETERSON, Alan; BORZINO, Tiago. Spoofing. **Grupo de**

Teleinformática e Automação da Universidade Federal do Rio de Janeiro, 2019. Disponível em: <https://www.gta.ufrj.br/ensino/eel878/redes1-2019-1/vf/dns/cache-poisoning.html> Acesso em: 25 fev. 2021.

SHIMABUKURO, Adriana. Cibercrime: quando a tecnologia é aliada da lei. In: BRASIL. Tribunal Regional Federal da 3ª Região. Escola de Magistrados. **Investigação e prova nos crimes cibernéticos.** São Paulo: EMAG, 2017.

SHMATIKOV, Sooel Son and Vitaly. The Hitchhiker's Guide to DNS Cache Poisoning. In: Jajodia S., Zhou J. (eds) **Security and Privacy in Communication Networks**. SecureComm 2010. Disponível em:<https://www.cs.cornell.edu/~shmat/shmat_securecomm10.pdf> Acesso em: 25 fev. 2021.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 27 ed. São Paulo: Malheiros, 2006.

STRECK, Lenio Luiz. Bem jurídico e Constituição: da proibição de excesso (übermassverbot) à proibição de proteção deficiente (untermassverbot) ou de como não há blindagem contra normas penais inconstitucionais. **Universidade de Coimbra**, 2004. Disponível em: <http://www.escoladaajuris.org.br/esm/images/arquivos/penal/bemjurdicoconstituiaolniolusstreck.pdf>. Acesso em 12 mar. 2021.

STRICKLAND, Jonathan. How Hackers Work. **How Stuff Works**, 2007. Disponível em: <https://computer.howstuffworks.com/hacker1.htm> Acesso em: 1 fev.2021.

SUSPEITO DO ATAQUE HACKER AO SISTEMA DO TSE É PRESO EM PORTUGAL. **UOL**, 2020. Disponível em: <https://noticias.uol.com.br/eleicoes/2020/11/28/pf-ataque-hacker-sistema-do-tse.htm> Acesso em: 25 jan.2021.

TARTUCE, Flávio. **Manual de Direito Civil**. 5 ed. São Paulo: Editora Método, 2015.

The Secret History of Hacking. Direção de Ralph Lee. Estados Unidos: September FIlms, 2001. (50 min). Disponível em: <https://www.youtube.com/watch?v=Y47m1cOyKjA&ab_channel=Jon> Acesso em: 25 jan. 2021.

TRÓIA, Pedro. Breve história do microprocessador e do computador pessoal parte 1: o primeiro processador comercial. **PC GUIA**, 2020. Disponível em: <https://www.pcguia.pt/2019/12/breve-historia-microprocessador-computador-pessoal-parte-1-primeiro-processador-comercial/> Acesso em: 25 jan. 2021.

VALENTE, Fernandes; VITAL, Danilo. STJ sofre ataque hacker e suspende prazos processuais até segunda (9/11). **Consultor Jurídico**, 2020. Disponível em <https://www.conjur.com.br/2020-nov-04/stj-sofre-ataque-hacker-suspende-prazos-segunda-911> Acesso em: 25 jan. 2021.

VEGA, Guillermo. Por que nos ciberataques o resgate é pedido em bitcoins? **El País,** 2017. Disponível em: <https://brasil.elpais.com/brasil/2017/05/12/economia/1494621106_047933.html> Acesso em: 4 mar. 2021.

VELLOZO, Jean Pablo Barbosa. Crimes informáticos e criminalidade contemporânea. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 20, n. 4515, 11 nov. 2015. Disponível em: <https://jus.com.br/artigos/44400>. Acesso em: 27 jan. 2021.

VIANA, Eduardo. **Criminologia**. 8 ed. Salvador: JusPODIVM, 2020.

VIEIRA, Nathan. Ataques DDoS geram preocupação no setor financeiro. **Canaltech**, 2019. Disponível em: <https://canaltech.com.br/seguranca/ataques-ddos-geram-preocupacao-no-setor-financeiro-156861/> Acesso em 14 fev. de 2021.

WARD, Mark. Saiba mais sobre a história dos hackers. **BBC News Brasil**, 2011. Disponível em: <https://www.bbc.com/portuguese/noticias/2011/06/110623_historiahacking_is> Acesso em 25 jan. 2021.

WANNACRY, O RANSOMWARE QUE FEZ O MUNDO CHORAR NA SEXTA-FEIRA (12). **Tecmundo**, 2017. Disponível em: <https://www.tecmundo.com.br/malware/116652-wannacry-ransomware-o-mundo-chorar-sexta-feira-12.htm> Acesso em 29 abr. 2021.

WELCOME TO AWPG PUBLIC EDUCATION. **APWG**, c2021. Disponível em: <https://education.apwg.org/> Acesso em 15 abr. 2021.

WHAT IS KEYSTROKE LOGGING AND KEYLOGGERS? **Kaspersky**, c2021. Disponível em: <https://www.kaspersky.com/resource-center/definitions/keylogger> Acesso em 29 abr. 2021.

ZETTER, Kim. An Unprecedented Look at Stuxnet, the World's First Digital Weapon. **WIRED**, 2014. Disponível em: <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/> Acesso em: 11 fev. 2021.

ZETTER, Kim. That Insane, $81M Bangladesh Bank Heist? Here's What We Know. **WIRED,** 2016. Disponível em: <https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/> Acesso em: 25 jan. 2021.