A REPRESSÃO AO CRIME DE INVASÃO DE DISPOSITIVOS INFORMÁTICOS

Lucas Uchôa Silva[1]

Bruno Pereira Malta[2]

RESUMO

O presente artigo teve como temática o crime de invasão de dispositivos informáticos que está se tornando mais comum na sociedade e a sua repressão. A pesquisa deste estudo partiu do seguinte problema: como reprimir a invasão de dispositivos informáticos de um modo eficiente? Partindo desse problema, o objetivo do referido trabalho, foi o de procurar por possíveis soluções que tornem a repressão da invasão a dispositivos informáticos mais eficiente. A pesquisa se utilizou do método hipotético dedutivo e também a pesquisa bibliográfica, foram usados como base textos de autores que trataram desse assunto, entrevistas com especialistas em crimes digitais, a legislação e projetos de lei. Por fim, percebeu-se que se deve dar educação digital a população; a necessidade da polícia se atualizar para enfrentar esse crime, através do treinamento de policiais e utilizando-se de equipamentos adequados; a realização de alterações legislativas, podem ser meios eficientes de reprimir esse crime.

Palavras-chave: Crime digital. Invasão de dispositivo informático. Direito Penal

[1]Acadêmico(a) do 9º período de Direito, pela Universidade de Rio Verde, Campus Caiapônia, GO.
[2]Bacharel em Direito. Docente do Curso de Direito da Universidade de Rio Verde, Campus Caiapônia, GO

1 INTRODUÇÃO

A tecnologia tem avançado muito nos últimos anos e um dos avanços mais significativos foi a internet que vem alterando a sociedade de vários modos proporcionando mudanças em como as pessoas se relacionam, facilitando o acesso à informação, diminuindo distâncias, etc., além disso, ela vem se tornando mais acessível no Brasil, trazendo um aumento no número de brasileiros que a acessam e se tornando indispensável.

Mas, a internet também gerou novos problemas, como o surgimento dos crimes digitais, um deles é a invasão de dispositivos eletrônicos. Ela pode ser cometida de vários modos, os quais vêm se diversificando com o avanço da tecnologia. Sendo necessária a criação de mais normas eficazes e outras medidas que tratem desse assunto. Diante da perspectiva apresentada, acerca dos cibercrimes, delimitou-se o seguinte tema: A repressão do crime de invasão de dispositivos informáticos.Em análise ao que foi exposto sobre essa nova modalidade de crime que vem se tornando mais comum, este estudo questiona: como reprimir a invasão de dispositivos informáticos de um modo eficiente?

Com base na problemática apresentada, propõem-se as seguintes hipóteses: **A)**O aumento da pena do crime de invasão de dispositivos eletrônicos pode intimidar aqueles que pensam em cometê-lo; **B)**Com base no grande número de técnicas utilizadas para cometer esse crime, é necessário tipificar tais técnicas para evitar que brechas sejam deixadas pela lei, assim trazendo resultados positivos; **C)** A criação de programas para conscientizar a população dos perigos que correm na internet, além de ensiná-la a se proteger destes perigos, o que pode contribuir para a diminuição da ocorrência desses crimes; **D)**A criação de mais delegacias especializadas em investigar crimes cibernéticos, assim como a especialização de mais profissionais nesse tipo de investigação, poderia contribuir para a repressão do crime de invasão de dispositivos informáticos.

O presente trabalho busca tratar do crime de invasão de dispositivos informáticos, o qual, é um crime relativamente recente no ordenamento jurídico, além de estar presente no dia a dia do brasileiro, na forma de uma ameaça que pode trazer graves consequências e que é muitas vezes imperceptível à maioria das pessoas que acessam a internet, tornando-as presas fáceis para criminosos e trazendo insegurança a elas, sendo necessário analisar tal ameaça e combatê-la, para assim trazer segurança à sociedade.

Pode-se perceber que o tema é de grande relevância para a sociedade de um aspecto geral, visto que essa conduta pode violar o direito à privacidade de qualquer pessoa que não esteja familiarizada com os métodos utilizados pelos criminosos para realizar a invasão. Além disso, é importante no âmbito jurídico por ser tipificada recentemente, o que abre a possibilidade de se discutir sobre como tornar sua repressão mais eficaz, definir se ela precisa ser complementada por outras normas para que isso ocorra, esclarecer pontos que ainda são controversos. Sendo assim, relevante para os operadores do direito que atuam na área penal.

2 REVISÃO DE LITERATURA

2.1 SURGIMENTO DA INTERNET E DOS CRIMES DIGITAIS

Castells (2003) afirma que o início da internet se deu com a *Advanced Research Projects Agency Network* (ARPANET), a qual era uma rede de computadores construída pela *Advanced Research Projects Agency* (ARPA) em setembro de 1969. Essa agência foi criada pelo Departamento de Defesa dos Estados Unidos com a finalidade de superar a tecnologia militar soviética, a ARPANET tinha o objetivo de compartilhar informações entre os computadores da agência.

Mandel, Simon e Lyra (1997) afirmam que o primeiro experimento realizado com a ARPANET ocorreu em janeiro de 1970 e conectou a Universidade da Califórnia em Los Angeles, a Universidade da Califórnia em Santa Bárbara, o *Stanford Research Institute*, Universidade de Utah. Nesse momento ela era utilizada tanto pelos acadêmicos quanto pelos militares. A sua primeira demonstração pública da rede ocorreu em 1972, nesse ponto ela era capaz de prover login remoto e correio eletrônico. Segundo Castells (2003) a internet se espalhou pelo mundo por conta do desenvolvimento da *World Wide Web* (WWW), criada em 1990 pelo programador inglês Tim Berners-Lee.

No que diz respeito ao surgimento dos cibercrimes Jesus e Milagre (2016) dizem que, há divergências na doutrina sobre qual teria sido o primeiro delito informático, certos autores dizem que o primeiro crime digital ocorreu no *Massachusetts Institute of Technology* (MIT) em 1964, onde um aluno teria cometido um ato que pode ser caracterizado como um cibercrime. Outros autores afirmam que foi a invasão realizada por um aluno da Universidade Oxford a uma rede de computadores em 1978, com o objetivo de obter a cópia de uma prova.

Wendt e Jorge, (2013) pontuam que em 1971 Bob Thomas, um funcionário de uma empresa relacionada a construção da ARPANET criou o *Creeper Virus*. Em 1982 Richard Skrenta desenvolveu o *Elk Cloner*, o qual, na visão de alguns estudiosos, seria o primeiro vírus feito para infectar computadores, mas o termo "vírus de computador" foi concebido apenas dois anos depois por Fred Cohen.

Segundo Jokura (2019) em 1986 dois irmãos paquistaneses criaram o vírus *Brain* para intimidar as pessoas que estavam criando a cópias piratas de um *software* feito por eles, quando alguém utilizava uma cópia era exibida na tela uma mensagem com os dados dos irmãos, para que a pessoa em posse da versão pirata comprasse o produto original e em pouco tempo o *Brain* se espalhou pelo mundo. Wendt e Jorge (2013) apontam que ainda em 1986 também surgiu o vírus cavalo de troia.

2.2 HACKERS E CRACKERS

Cassanti (2014) afirma que, mesmo que os *hackers* geralmente sejam associados a invasão de dispositivos eletrônicos e roubo de informações, eles, na verdade, são programadores com um grande conhecimento acerca de sistemas que não procuram causar danos, já os *crackers* é que são os criminosos. O referido autor também diz que, os *crackers* costumam praticar "[...], a quebra de sistemas de segurança, códigos de criptografia e senhas de acesso a redes, de forma ilegal e com a intenção de invadir e sabotar para fins criminosos."(CASSANTI, 2014, p.20).

Ainda segundo Cassanti (2014), os *crackers* são subdivididos de acordo com as suas habilidades, sendo os principais os *carders, spammers, defacers, phishers e phreakers*. Os *carders* que roubam dados bancários; os *spammers* espalham e-mails com correntes e vírus com a capacidade de roubar dados ou danificar o dispositivo do usuário; os *defacers* costumam vandalizar sites, deixando mensagens contra o site; os *phishers* são especialistas em aplicar golpes e encontrar falhas em um sistema e os *phreakers* se utilizam de técnicas para trespassar o sistema de segurança de empresas telefônicas.

2.3 CRIME DE INVASÃO DE DISPOSITIVO ELETRÔNICO

2.3.1 Origem e conceito

Santos e Martins (2017) afirmam que a criação do crime de invasão de dispositivos informáticos deu-se com a Lei de crimes informáticos. Lei nº 12.737, de 30 de novembro de 2012, também conhecida como Lei Carolina Dieckmann foi criada após o vazamento de fotos íntimas da atriz repercutir nacionalmente, ela entrou em vigor em 2 de abril 2013. De acordo com Jesus e Milagre (2016) essa lei não trouxe a obrigação dos provedores de conexões ou serviços guardarem os registros das conexões de seus clientes, ou de que aplicações eles acessaram, o que seria necessário para uma investigação, essa obrigação foi trazida posteriormente pelo Marco Civil da Internet, Lei nº 12.695/2014.

Santos e Martins (2017) afirmam que a Lei nº 12.737/12 foi trazida como outra opção em relação à Lei Azeredo, Lei nº 12.735, de 30 de novembro de 2012, a qual, sofria críticas por conta de inspirar o medo de que a liberdade virtual fosse suprimida e por conta disso ao ser promulgada previu apenas a que os órgãos da polícia judiciária são obrigados a se estruturar para combater crimes virtuais.

Segundo Jesus e Milagre (2016) a invasão é o ato de acessar de maneira indevida, a força e ocupar um dispositivo informático, o qual é todo dispositivo que tem a capacidade de processar ou guardar dados, de acordo com Prado (2019) a ação de invadir no entendimento do texto legal, quer dizer devassar, vasculhar, obter conhecimento em parte ou na totalidade do conteúdo do dispositivo informático. Crespo (2012) afirma que esse delito se caracteriza como um crime digital próprio por conta de a conduta afetar um bem jurídico informático.

2.3.2 Bem jurídico

O bem jurídico tutelado segundo Jesus e Milagre (2016) é, a liberdade individual de manter privados os dados que se encontram em um meio digital, assim como manter ilesos os dispositivos informáticos, que possuam um mecanismo de segurança, de acessos que não tenham sido autorizados pelo proprietário do dispositivo. Nucci (2017) entende que a liberdade individual é o bem tutelado mediato, enquanto o bem imediato tutelado seria a intimidade, à honra, à impossibilidade de se violar a comunicação e correspondência e à vida privada.

2.3.3 Sujeitos

Na visão de Greco (2015) o sujeito ativo desse delito pode ser qualquer pessoa, por este tipo penal em questão não exigir uma condição especial. De acordo com Prado (2019) a terminologia utilizada na informática para quem invade dispositivos buscando uma vantagem indevida ou causar prejuízo a outra pessoa, é chamada de *cracker.* Ainda segundo Greco (2015, p. 609) o "Sujeito passivo é o proprietário (pessoa física ou jurídica) do dispositivo informático invadido, ou mesmo qualquer outra pessoa que nele tenha arquivados dados ou informações".

2.3.4 Tipicidade objetiva e subjetiva

A antiga redação do art.154-A estabelecia, in verbis:

> Art. 154-A: Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 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.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º 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: Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I – Presidente da República, governadores e prefeitos;
> II – Presidente do Supremo Tribunal Federal;
> III – Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV – dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (BRASIL, 1940).

Segundo Jesus e Milagre (2016) o núcleo do tipo é a ação de invadir um dispositivo informático de outrem, o qual, na antiga redação do crime deveria estar protegido por um mecanismo de segurança e essa invasão deve ter como objetivo a obtenção, destruição, alteração de dados ou a intenção de instalar uma vulnerabilidade que venha a gerar vantagem ilícita.

Ainda de acordo com Jesus e Milagre (2016) é necessário apenas que a invasão seja realizada com uma dessas finalidades para se encaixar no tipo penal. O mecanismo de segurança violado para Prado (2019), pode ser tanto físico como portas, chaves ou lógico como senhas e a criptografia de dados.

Nucci (2017) pontua que para fins de criminalização o legislador decidiu dar o mesmo grau de importância a preparação e a execução, ou seja, no caso do autor instalar a vulnerabilidade no dispositivo informático, para que futuramente ele ou outra pessoa a utilize, se ele instalar esse ponto fraco e depois invadir, cometerá apenas um crime e se outra pessoa invadir se valendo dessa fragilidade, os dois irão cometer delitos distintos.

De acordo com Jesus e Milagre (2016) não existe modalidade culposa prevista na lei, apenas a modalidade dolosa é punida. Ainda nesse sentido Jesus e Milagre (2016 p. 165) também diz que, "o dolo é a vontade livre e consciente de invadir o dispositivo. Já a expressão 'para obter, adulterar, destruir informações, ou instalar vulnerabilidade para conseguir vantagem ilícita' configura um elemento subjetivo do tipo."

2.3.5 Consumação e tentativa

Na visão de Jesus e Milagre (2016 p. 170) "a consumação ocorre com a constatação da invasão, esta comprovada por prova pericial, que avaliará os artefatos e evidências como data e hora de conexão (*login*), data e hora do fim da conexão (*logout*)". Segundo Greco (2015) caso o invasor obtenha, modifique ou venha a destruir dados ou informações, sem que tenha autorização do proprietário do dispositivo informático, seja ela expressa ou tácita, essas ações serão consideradas como o exaurimento do crime, o que vale também para a instalação de vulnerabilidade com o objetivo de obter um benefício ilícito.

De acordo com Greco (2015) por conta de sua natureza plurissubsistente e a possibilidade de dividir o *iter criminis*, pode- se vislumbrar a tentativa onde, por exemplo, o agente é detectado enquanto tentava trespassar o mecanismo de segurança do dispositivo informático com um ou mais dos objetivos que estão previstos no caput do art.154-A do Código Penal, o que acabaria caracterizando o crime tentado.

A figura equiparada prevista no § 1º do artigo mencionado diz, "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." Para Nucci (2017) pelo fato de ela ter como objetivo

punir os atos preparatórios da invasão do dispositivo informático, não se admite a sua tentativa. Já para Greco (2015) se admite a modalidade tentada por ser possível fracionar o iter criminis.

2.4 ALTERAÇÕES TRAZIDAS PELA LEI Nº 14.155 DE 2021

A Lei nº 14.155 de 27 de maio de 2021 trouxe alterações nos crimes de estelionato, furto e uma nova redação para o art. 154-A do Código penal, essas mudanças trazem um aumento de pena na conduta descrita no caput e também nas hipóteses do § 2º e 3º. Além disso também retirou a necessidade de o dispositivo informático estar protegido por um mecanismo de segurança, in verbis:

> Art. 154-A: Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
> § 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.
> § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.
> § 3º 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: Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I – Presidente da República, governadores e prefeitos;
> II – Presidente do Supremo Tribunal Federal;
> III – Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV – dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (BRASIL, 1940).

2.5 MÉTODOS UTILIZADOS

2.5.1 Vírus

Segundo Jesus e Milagre (2016) é uma espécie de *malware*, um programa que pode causar alterações em sistemas ou dados, podendo também destruir e alterar programas ou arquivos, além de realizar funções imprevistas em um dispositivo informático ou sistema operacional. Como o vírus de *boot* que segundo Wendt e Jorge (2013) se fixa no setor de inicialização do sistema.

2.5.2 *Backdoor*

De acordo com Jesus e Milagre (2016) o *backdoor* é um código malicioso que permite alterar os privilégios dos usuários, invadir ou tomar um sistema e até mesmo desativar mecanismos de segurança, ele pode ser inserido previamente por programadores dos sistemas e também durante ataques, para facilitar que o atacante acesse novamente o sistema que já foi invadido.

2.5.3 *Trojan*

Wendt e Jorge (2013) afirmam que o *trojan* ou cavalo de troia é um arquivo malicioso que o computador do agente acesse remotamente outro computador e consiga obter dados privados da vítima, no momento em que esse arquivo é executado ele irá permitir que o *cracker* domine o dispositivo afetado como se fosse o próprio usuário e o utilize para danificar outros.

2.5.4 *Spyware*

Jesus e Milagre (2016) dizem que o *spyware* é um código ou programa que pode ser instalado ou injetado em *apps* que tenham sido baixados em fontes não confiáveis, ele pode ajudar o criminoso a controlar o computador, mas geralmente tem o objetivo de coletar dados de um usuário e enviá-los ao criminoso, essas informações geralmente são os sites que o usuário visita, o que ele consome, entre outras.

2.5.5 *Botnets*

De acordo com Wendt e Jorge (2013) os *botnets* são uma rede de computadores que foram infectados por arquivos maliciosos e permitem que o criminoso controle a distância o computador da vítima, utilizando-se de falhas ou vulnerabilidades no sistema operacional, ou em *softwares,* as vítimas não percebem que o seu computador está sendo utilizado para atacar outros.

2.5.6 Quebra de senhas

Segundo Jesus e Milagre (2016) existem três técnicas de quebra de senha, a primeira é a força bruta em que o criminoso tenta todas as senhas possíveis, esse método pode ser realizado por ferramentas que automatizam essa técnica; a segunda é o ataque dicionário em que se testam palavras do dicionário até que se descubra a senha, ela pode ser feita em conjunto com a técnica de quebra se senha; a terceira é a *rainbow table*, que é utilizada para quebrar senhas criptografadas, nela submete-se os *hashs* a uma comparação com uma tabela de *hashs* que já foram calculados.

2.5.7 *Keylogger*

De acordo com Wendt e Jorge (2013) se trata de um *software* que monitora o que a vítima digita, sendo usado com o objetivo de obter informações que poderão ser usadas posteriormente, os programas *keyloggers* atuais são capazes de realizar capturas de tela também e não apenas o que a vítima está digitando em seu teclado, esses programas podem ser instalados no computador ou então se utiliza de um dispositivo que fica instalado entre a CPU do computador.

2.5.8 *Connection back*

Jesus e Milagre (2016) afirmam que pode se tratar de técnica ou de um programa, que faz com que a vítima se conecte ao criminoso e por conta disso o criminoso consegue acessar o computador da vítima. Ainda segundo os autores citados, o que geralmente ocorre é o atacante tentar se conectar ao dispositivo alvo, mas ele pode ser impedido por *firewalls*; seu alvo pode não ser acessível pela internet ou não conhecer o endereço de IP; sendo assim ao se utilizar

dessa técnica ou programa, o criminoso consegue que o seu alvo se conecte ao seu computador, o que evita esses problemas.

2.5.9 *Hijacker*

Wendt e Jorge (2013) afirmam que se trata de um código malicioso (*malware*) que sequestra o navegador de internet e direciona constantemente o seu usuário para outros sites e muda a página inicial do navegador, ele também pode gerar anúncios *pop-ups* ligados a sites não confiáveis.

2.5.10 *Rootkits*

Trata-se de um *software* que corrompe as atividades de programas, de arquivos do sistema, do sistema operacional, etc. Ao comprometer um programa por exemplo, além de executar sua atividade padrão, esse programa pode deixar o computador vulnerável. O *rootkit* tem o objetivo de preservar o acesso do *cracker* dispositivo enquanto oculta os processos que ele criou, esse *software* geralmente é composto por um *backdoor* e trojan. (JESUS; MILAGRE, 2016)

2.5.11 *SQL injection*

É uma técnica em que o atacante altera as medidas ou instruções que são executadas em tabelas de um banco de dados, o *cracker* se utiliza da linguagem SQL (*structured query language*), o que torna possível que o atacante execute comandos inesperados que o permitam acessar dados privados. Além de permitir que ele destrua, altere ou acrescente novos dados. (JESUS; MILAGRE, 2016)

2.5.12 *Phishing scam*

De acordo com Wendt e Jorge (2013) trata-se de uma técnica que consiste em enviar um e-mail a um indivíduo, com o intuito de instigá-lo a acessar um site falso, o qual, permitiria que as informações de quem se conecta a ele fossem obtidas, essa conduta também pode

consistir em mensagens que levem a vítima a instalar códigos maliciosos ou expor dados privados através do ato de preencher um formulário. De acordo com Jesus e Milagre (2016) essa primeira modalidade é o *phishing scam* com engenharia social.

2.6 INVESTIGAÇÃO DO CRIME

Segundo Wendt e Jorge (2013) a investigação de crimes virtuais é dividida em uma fase inicial, uma técnica e a consequencial que seria a fase de campo, na fase técnica as informações trazidas pela vítima são analisadas para que se possa compreender o fato; os policiais orientam a vítima a preservar os indícios do delito, começa-se a coleta de provas; o boletim de ocorrência é instaurado, ocorre também a investigação inicial na internet com o intuito de encontrar os possíveis autores, origem de emails, registro do endereço do site e onde ele está hospedado.

Ainda segundo o mesmo autor na fase técnica, também se realiza a formalização de relatório ou de uma certidão referente as provas coletadas; a representação diante do Poder Judiciário, para obter autorização para a quebra de dados, acesso ou conexão e a análise dos dados entregues pelos provedores de conexão e/ou conteúdo, o que poderá levar a identificação do endereço de IP do computador utilizado pelo criminoso. Após localizar-se o computador, a investigação irá avançar para a fase de campo, em que os agentes policiais, irão realizar o reconhecimento operacional do local.

De acordo com Borin (2020) a representação diante do Poder Judiciário para que se autorize a quebra de sigilo de dados pode ser requerida pelos seguintes legitimados: a parte ofendida; a autoridade policial, apenas quando for necessário para uma investigação criminal; e por membro do Ministério Público.

2.6.1 Dificuldades enfrentadas na investigação

Segundo Soares e Dorigon (2018), os policiais encontram dificuldades várias dificuldades e entre elas, as principais são a falta de legislação em relação a crimes virtuais; a guarda dos registros de conexão e de acesso gera dificuldades, pelo fato de os provedores de acesso serem obrigados a guarda-los por apenas um ano; outro problema são as formas de a localização do criminoso através de seu IP, como as redes de *WI-FI* abertas que são utilizadas

por muitas pessoas, a utilização de *lan houses* que não registram seus clientes e servidores *proxies* que escondem o verdadeiro IP do usuário.

Ainda de acordo com o mesmo autor, outros problemas enfrentados durante a investigação são o *cloud computing* ou computação nas nuvens, que permite aos criminosos acessar e executar arquivos e programas utilizando a internet sem que os mesmos estejam em seus computadores; o fato de os crimes digitais poderem ser cometidos por um criminoso localizado em outro país; por último, a falta de capacitação técnica dos agentes e a falta de equipamento.

2.7 PROJETOS DE LEI

O legislador viu a necessidade de aumentar a pena do crime de invasão de dispositivos informáticos e criou o PL 3.683/2020 que prevê um aumento na pena de quem cometer esse crime. A pena deixaria de ser de 3 meses a 1 ano de detenção e multa, para ser de 1 a 3 anos de detenção e multa, o projeto também prevê que caso ocorra o que está descrito § 3º do art. 154-A do Código Penal, a pena deixará de ser de seis meses de detenção para 2 anos, para ser de 3 a 8 anos de detenção e multa.

O Projeto de Lei 3.357/2015 tem como objetivo adicionar o parágrafo sexto ao art.154-A do Código Penal, que tratará da invasão de dispositivo informático com o objetivo de alterar um site na internet, o que é chamado de *defacement* ou *deface*, que segundo Cassanti (2014) é cometido por um tipo de cracker chamado *defacer*, o qual, já foi citado anteriormente.

3 OBJETIVOS

3.1 OBJETIVO GERAL

Analisar meios de tornar a repressão do crime de invasão de dispositivos informáticos mais eficiente, uma vez que com o avanço tecnológico, crimes virtuais possuem a tendência de se tornarem cada vez mais comuns.

3.2 OBJETIVOS ESPECÍFICOS

- Estabelecer se é necessário tipificar o grande número de técnicas utilizadas para invadir dispositivos eletrônicos;
- Analisar se o aumento da pena do crime de invasão de dispositivos informáticos pode intimidar aqueles que a praticam;
- Examinar se a criação de mais delegacias especializadas em investigar crimes digitais e a especialização de mais profissionais nessa modalidade de investigação, pode contribuir para uma repressão mais eficiente do crime de invasão de dispositivos informáticos;
- Averiguar se a criação de programas para a conscientizar a população dos perigos que correm na internet, além de ensiná-las a se proteger destes perigos, irá contribuir para a diminuição de invasões a dispositivos informáticos.

4 METODOLOGIA

O presente estudo utilizou da pesquisa bibliográfica, em códigos, doutrinas, súmulas, leis, livros, sites e outros materiais que tenham informações relevantes para o assunto. Segundo Prodanov e Freitas (2013) a pesquisa bibliográfica tem como finalidade permitir que o pesquisador entre em contato com o material relacionado ao assunto pesquisado, como, por exemplo, artigos científicos, periódicos, jornais, monografias, entre outros.

O método de abordagem que foi utilizado pelo presente artigo é o dedutivo, Gil (2008) afirma que o método dedutivo, ao partir de uma premissa geral para uma particular, possibilita alcançar a verdade através de conclusões lógicas, o que ocorre por utilizar como ponto de partida princípios considerados verídicos e irrecusáveis.

A natureza da pesquisa realizada neste estudo é a básica, que segundo Prodanov e Freitas (2013, p. 51), “objetiva gerar conhecimentos novos úteis para o avanço da ciência sem aplicação prática prevista. Envolve verdades e interesses universais”. A pesquisa utilizada pelo para atingir os objetivos deste trabalho foi a exploratória, Gil (2008) afirma que essa modalidade de pesquisa busca desenvolver, alterar e esclarecer conceitos, assim possibilitando a elaboração de problemas mais exatos e hipóteses passíveis de serem pesquisadas, essa modalidade pode envolver pesquisa bibliográfica, documental, pesquisas não padronizadas e estudos de caso.

O ponto de vista que foi adotado por esse estudo é o da pesquisa qualitativa, que segundo Prodanov e Freitas (2013) esta abordagem não requisita que sejam utilizados métodos e técnicas estatísticas, sendo parte de seu processo a atribuição de significados e a explicação de fenômenos.

5 RESULTADO E DISCUSSÕES

Uma das hipóteses apresentadas neste trabalho foi de que o aumento da pena poderia desencorajar os criminosos a cometerem o crime de invasão de dispositivos informáticos. Soares e Dorigon (2018) apontam que a investigação de crimes como esse enfrenta diversas dificuldades, como, por exemplo, a falta de equipamento adequado e profissionais qualificados e a dificuldade em localizar os criminosos. O que dificulta prende-los e como consequência pode reduzir a efetividade da hipótese apresentada.

Além disso, de acordo com Jesus e Milagre (2016) a prisão não seria o método mais eficiente para lidar com esses criminosos e que por conta da nova Lei das prisões eles dificilmente seriam presos preventivamente, sendo assim, a aplicação de penas como as que tratem da prestação de serviços de proteção de informação e blindagem de sistemas seria mais eficiente.

Emerson Wendt em uma entrevista realizada em 2011 ao G1, quando perguntado o que ele pensava que devia ser melhorado no combate a crimes virtuais, afirmou que:

> Acho que a Polícia precisa de mais treinamento e agentes policiais em investigação, além de equipamentos e ferramentas adequadas. Sentimos, também, falta de mais peritos formados na área, justamente para que possam comparecer e realizar o que chamamos de perícia online. Acredito que para 2011 - se o planejamento dependesse só de mim - o ideal seria termos ao menos uma Delegacia de Polícia em cada Estado, interagindo e trabalhando em conjunto no combate aos crimes praticados no ambiente virtual.(ROHR, 2011)

Mais recentemente em uma palestra realizada em 2019 Emerson Wendt disse que as pessoas não sabem se proteger na internet, além de dizer que deveria ser criada uma rede nacional de Laboratórios de inteligência cibernética, que ajudem os policiais a solucionar crimes digitais e delitos que utilizem tecnologia, ele também acredita que a Lei Geral de

Proteção de Dados, Lei n. 13.709, de 14 de agosto de 2018 vai facilitar a investigação policial. (POVO, 2019)

Assim como o legislador pensou que seria necessário acrescentar a modalidade de defacement ao art.154-A do Código Penal. Jesus e Milagre (2016) acreditavam que a redação antiga desse artigo não abarcava o *phishing scam* na modalidade de engenharia social, por intenderem que a vítima é enganada, para que desative os mecanismos de segurança, ou seja, nesses casos não ocorrerá violação de uma medida de segurança, pois a vítima não pode ser considerada um mecanismo de segurança. Agora essa conduta pode se encaixar na fraude eletrônica trazida pela Lei nº 14.155.

Os referidos autores também afirmam:

> a Lei n. 12.737/2012 longe está de solucionar todos os problemas relativos ao crime cibernético no Brasil. A solução não é fácil de ser encontrada, mas com certeza não resolve tão somente com a edição de leis criminais. Envolve educação digital, políticas criminais e estrutura investigativa. (JESUS; MILAGRE, 2016, p.226)

6 CONSIDERAÇÕES FINAIS

Foi possível perceber que para tornar a repressão do crime de invasão de dispositivos informáticos mais eficiente, primeiramente seria necessário dar uma educação digital a população, para que ela saiba se proteger dos indivíduos que busquem cometer esse crime e também fornecer equipamentos e instrução à polícia, para facilitar a captura desses criminosos.

Após essas medidas serem realizadas, o aumento de pena seria mais eficaz para intimidar os criminosos que planejem cometer esse crime, podendo também serem adicionadas outros tipos de pena. Além disso foi possível perceber que a Lei Carolina Dieckmann não engloba algumas das técnicas utilizadas para invadir os dispositivos eletrônicos como no caso do *defacement* que seu objetivo não se enquadra com o que é punido pelo art.154-A do Código Penal. Portanto, é necessário tipificar tais técnicas.

THE REPRESSION TO THE CRIME OF INVASION OF COMPUTER DEVICES

ABSTRACT

The present article had as its theme the crime of invasion of computer devices that is becoming more common in society and its repression. The research for this study started from the following problem: how to effectively suppress the invasion of computer devices? Starting from this problem, the objective of the referred work was to look for possible solutions that make the repression of the invasion of computer devices more efficient. The research carried out was the bibliographic research, texts from authors who dealt with this subject, interviews with specialists in digital crimes, legislation and bills were used as basis. Finally, it was realized that the population should be digitally educated; the need for the police to update themselves to face this crime, through the training of police officers and the use of appropriate equipment; making legislative changes can be an effective means of suppressing this crime.

Keywords: Digital crime. Computer device invasion. Criminal Law

REFERÊNCIAS

BORIN, L. C. O Marco Civil da Internet e a quebra do sigilo de registros. In: ROCHA, L. R. L. (Coord.). et al. *Caderno de Pós-Graduação em direito*: crimes digitais. Brasilia: UniCEUB, 2020. Disponível em: <https://repositorio.uniceub.br/jspui/handle/prefix/14602>. Acesso em: 14 abr. 2020

BRASIL. Câmara dos Deputados. Projeto de Lei nº 3.357/2015 de 21 de outubro de 2015. Dispõe sobre o crime de invadir dispositivo informático, sem a devida autorização, modificando conteúdo de sítio da internet. Brasília, DF: Câmara dos Deputados, 2015. Não paginado. Disponível em: <https://www.camara.leg.br/propostas-legislativas/2024070>. Acesso em: 23 mar. 2021

BRASIL. *Código Penal-Decreto Lei nº 2.848 de 7 de dezembro de 1940*. Não paginado. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 15 out. 2020.

BRASIL. Senado Federal. Projeto de Lei nº 3.683/2020 de 07 de julho de 2020. Altera a legislação criminal, eleitoral e de improbidade administrativa para elevar penas e sanções de crimes já tipificados e outras condutas ilegais, e criar novos tipos penais, especialmente quando praticados na internet. Brasília, DF: Senado Federal, 2020. Não paginado. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/143264>. Acesso em: 19 mar. 2021

BRASIL. Presidência da República. Lei n. 14.155, de 27 de maio de 2021 Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Diario Oficial [da] República Federativa do Brasil, Brasília, DF, 27 de maio de 2021. Não paginado. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm#art1>. Acesso em: 30 de mai. de 2021.

CASSANTI, M. O. *Crimes virtuais, vítimas reais*. Rio de Janeiro: Brasport, 2014.

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

CRESPO, M. *Crimes digitais*. São Paulo: Saraiva, 2012.

GRECO, R. *Curso de Direito Penal*: parte especial. 12. ed. Niterói: Editora Impetus, 2015. v. 2.

GIL, A. *Métodos e técnicas de pesquisa social*. 6. ed. São Paulo: Editora Atlas, 2008.

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

JOKURA, T. *Qual foi o primeiro vírus de computador? spoiler*: ele veio antes da internet. Uol.com, São Paulo 11 novembro 2019. Não paginado. Disponível em: <https://www.uol.com.br/tilt/colunas/pergunta-pro-jokura/2019/11/11/qual-foi-o-primeiro-virus-de-computador.htm>. Acesso em: 11 de out. 2020

JUSTI, J.; VIEIRA, T. P. *Manual para padronização de trabalhos para graduação e pós-graduação lato sensu e stricto sensu.* Rio Verde: Ed. UniRV, 2016.

MANDEL, A.; Simon, I.; Lyra, J. L. *Informação*: computação e comunicação. 1997. Disponível em:<https://www.ime.usp.br/~is/abc/abc/abc.html> Acesso em: 09 de out. 2020.

NUCCI, G. *Código Penal Comentado.* 17. ed. Rio de Janeiro: Editora Forense, 2017.

POVO, C. *Wendt defende criação de rede nacional de inteligência cibernética*. Correio do Povo, Rio Grande do Sul, 06 de ago. 2019. Não paginado. Disponível em: <https://www.correiodopovo.com.br/notícias/polícia/wendt-defende-criação-de-rede-nacional-de-inteligência-cibernética-1.356568>. Acesso em: 30/03/2021

PRADO, L. *Curso de Direito Penal:* Parte geral e Parte especial. 17. ed. Rio de Janeiro: Editora Forense, 2019.

PRODANOV, C. C.; FREITAS, E. C. *Metodologia do trabalho científico:* Métodos e técnicas da pesquisa e do trabalho. 2. ed. Novo Hamburgo: Universidade Feevale, 2013.

ROHR, Altieres. Trabalho contra crimes virtuais ainda está longe do ideal, diz delegado. G1. 06 de janeiro de 2011. Não paginado. Disponível

em:http:<//g1.globo.com/tecnologia/noticia/2011/01/trabalho-contra-crimes-virtuais-ainda-esta-longe-do-ideal-diz-delegado.html>. Acesso em: 26 de mar. 2021

SANTOS, L. R.; MARTINS, L. B. Os crimes cibernéticos e o direito a segurança jurídica: uma análise da legislação vigente no cenário brasileiro contemporâneo. In: CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE, 4., 2017, Santa Maria, RS. Anais… Santa Maria, RS: Universidade Federal de Santa Maria, 2017. p. 1-14. Disponível em: <http://coral.ufsm.br/congressodireito/anais/2017/7-7.pdf>. Acesso em: 25 de out. /2020

SOARES, R. V. O; DORIGON, A. *Crimes cibernéticos*: dificuldades para obter indícios de autoria e materialidade. Revista Jus Navigandi, Teresina, ano 23, n.5342, 15 fev. 2018. Disponível em: <https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade>. Acesso em: 16 de mar. 2021

WENDT, E.; JORGE, H. V. N. *Crimes Cibernéticos*: ameaças e procedimentos de investigação. 2. ed. Rio de Janeiro: Brasport, 2013.