CRIMES CIBERNÉTICOS E A RECEPÇÃO DA LEI Nº 12.737/2012 NO BRASIL

Marcelo Matos Brito [1]

Prof. Cristiano Lázaro[2¹]

RESUMO: O presente trabalho versa sobre os cibercrimes, bem como a atuação do Poder Judiciário brasileiro perante essa tipo de crime. O objetivo geral consiste em analisar a alteração legislativa no combate aos crimes cibernéticos vigente no Brasil, fazendo uma observação no comportamento na esfera jurídica do Brasil após validação da legislação que aborda essa espécie de ílicito penal, para compreender como o país trata atualmente esses casos e verificar a eficiência da Lei. Especificamente, busca-se realizar uma análise histórica de crimes desta natureza no Brasil, para examinar a norma nacional vigente e obter uma visão demasiada sobre a competência desta legislação e sua amplitude. O presente trabalho objetiva, ainda, identificar os elementos que contribuem ou incentivam a existência e prática desses crimes, demonstrando a imensidão que podem alcançar os indivíduos envolvidos. Busca-se, ao final, apresentar o posicionamento a respeito da prática desses crimes e as medidas que laboram que podem ampliar o combate a esse fenômeno. Consiste o presente artigo na utilização de análise de bibliografias, como, artigos, livros e periódicos em PDF, retiradas da base de dados da internet, bem como, obras físicas. Portanto, o presente trabalho, visa analisar e promover uma concepção mais extensa acerca desses atos cada vez mais repetitivos na atualidade.

Palavras-Chave: Cibercrimes. Cibernéticos. Lei Carolina Dieckmann. Crime. Virtuais.

[1] Bacharel em Direito pela Universidade Católica do Salvador. Pós-Graduando do curso de Ciências Criminais da Universidade Católica do Salvador.

[2¹] Advogado. Professor de Direito Penal e Processo Penal da Universidade Católica do Salvador e Unifass.

ABSTRACT: This work deals with cybercrimes, as well as the action of the Brazilian Judiciary in the face of this type of crime. The general objective is to analyze the law to combat cybercrime in Force in Brazil, making an observation in the behavior of the Brazilian Judiciary after validation of the legislation that addresses this type of criminal law, to understand how the country currently treats these cases and verify the efficiency of the Law. Specifically, it seeks to carry out a historical analysis of crimes of this nature in Brazil, to examine the current national law and obtain too much view on the competence of this legislation and its breadth. The present work also aims to identify the elements that contribute or encourage the existence and practice of these crimes, demonstrating the immensity that can reach the individuals involved. In the end, it seeks to present the position regarding the practice of these crimes and the measures they work to expand the fight against this phenomenon. This article consists in the use of analysis of bibliographies, such as articles, books and journals in PDF, taken from the internet database, as well as physical works. Therefore, the present work aims to analyze and promote a more extensive conception about these increasingly repetitive acts nowadays.

Keywords: Cybercrimes. Cyber. Carolina Dieckmann Law. Crime. Virtual.

INTRODUÇÃO

Os crimes cibernéticos apresentam-se mais comuns no cenário mundial atual, causando extrema preocupação às pessoas de todas as localidades. Essas ações são motivadas, na maioria dos casos, com a finalidade de alcançar os objetivos financeiros[2], pois, no geral, acreditam que são capazes de afetar significativamente

[2] 2020. NICOLAI, Thiago et. al. O aumento silencioso dos cibercrimes. Migalhas de Peso. Disponível

empresas, principalmente de pequeno e médio porte, através de seus conhecimentos informáticos, conseguindo invadir sistemas operacionais e servidores para obterem dados que possibilitem ganhos monetários. Porém, suas motivações não são apenas de cunho financeiro. Muitas vezes o indivíduo ou a organização age com intuito de provocar alarde e pânico, mostrar sua capacidade e a dimensão que podem atingir com suas técnicas ou apenas obter dados importantes de pessoas ou, até mesmo, de um governo.

Assim, a escolha do tema foi, entre outros motivos, por causa da dúvida a respeito da atuação dos juízes brasileiros e o quanto a Lei nº 12.737/2012 está equivalente ao tipo penal em questão, visto a amplitude que pode atingir tal crime, ou seja, se as medidas certas e justas serão aplicadas sempre que a Lei for exigida.

Após uma onda de crimes dessa natureza, é natural alguns países adotarem medidas imediatas, sobretudo, com o intuito de acalmar os ânimos dos cidadãos e buscar conter os medos. Existem cibercrimes que marcaram a história e são lembrados até os tempos de hoje, que resultaram em alterações governamentais. Podemos destacar Robert Tapan Morris[3], cujo marcou a década de 90, quando criou um vírus, inicialmente inofensivo e apenas para efeitos científicos, porém que tomou uma proporção imensa, afetando na época o equivalente a 10% (dez por cento) da internet mundial. O mesmo teve como pena uma multa de dez mil dólares e 400 horas de serviço comunitário.

Outro destaque é o nome de Kevin Mitnick, famoso hacker dos anos 80 e 90, em que sua fama foi oriunda da invasão telefônica e sistemas empresariais, bem como, ludibriou o FBI, órgão de inteligência da polícia dos Estados Unidos, resultando no que ficou conhecida como “a maior caçada cibernética da história”, a qual durou quinze anos. Ele chegou a ser descoberto, porém não hesitou em continuar suas ações, o que elevou ainda mais sua fama.

Muitos outros hackers marcaram épocas, porém não há espaço para citação de todos. Observando as histórias, percebe-se o quão longe pode chegar suas ações e, com passar dos anos, o escalão almejado é cada vez mais exigente. A busca pelo “fruto proibido” está mais prazeroso para eles, o que causa medo e insegurança. A configuração desse tipo de crime na atualidade é proveniente de elementos

---

em <https://www.migalhas.com.br/depeso/326593/o-aumento-silencioso-dos-cibercrimes>

[3] 2019. Dez hackers famosos e seus feitos. Terra. Disponível em <https://www.terra.com.br/noticias/tecnologia/infograficos/hackers/hackers-08.htm>

históricos, que tomaram força após a chegada da globalização, em que passaram as grandes potências mundiais se mostrarem cada vez mais poderosas, levando à desejos em explorar essas áreas, por serem alvos de maiores poderios financeiros. Neste sentido, o presente trabalho, que se encontra estruturado em dois capítulos, além das considerações finais, aborda, no primeiro capítulo, uma contextualização histórica do cibercrime no mundo até a atualidade, buscando definir o tipo penal.

No segundo capítulo, visa tratar acerca da criação da legislação pátria em relação ao crime cibernético e a atuação do Poder Judiciário brasileiro posterior a vigência da mesma, fazendo uma análise profunda para mostrar o alcance que esse crime é capaz de obter em uma sociedade ou além.

Segundo LAKATOS (1992), a pesquisa bibliográfica é o levantamento de toda a bibliografia já publicada, em forma de livros, revistas, publicações avulsas e imprensa escrita, auxiliando na análise das pesquisas ou na manipulação de suas informações. Portanto, a metodologia utilizada para elaboração da presente obra foi esta, utilizando para tal dados da biblioteca da Universidade, bem como, livros e artigos da base de dados da internet.

A importância do presente trabalho se dá em razão da possibilidade de destacar uma realidade que assombra o planeta, com o propósito de analisar esse cenário no mundo contemporâneo, visto que, embora seja assunto de debate interpessoal e em meios de comunicação, sua natureza e seus objetivos ainda encontram-se distante ao conhecimento de muitas pessoas. Por isso, é importante elucidar as pretensões de indivíduos praticantes desse crime, assim como, demonstrar o quanto a lei brasileira garantirá a punição adequada, a justiça e as medidas corretas contra os sujeitos responsáveis pela ação criminosa em face de segurança e defesa dos direitos de seus cidadãos. Ainda, mostrar as atitudes do país frente a esses atos com o fito de abolir.

1 CONCEITO DE CIBERCRIMES

Uno modo, é importante realizar um esboço acerca da definição e do que consiste o crime virtual, bem como, os elementos que o compõem, por isso, nesse capítulo inicial, irão ser abordados os aspectos mais relevantes que existem repetitivamente em cada ato dos criminosos praticantes de uma atrocidade dessa espécie.

1.1. Definição e Noção de Crimes Cibernéticos

Com base em INTERPOL (2015)[4], a melhor conceituação para o cibercrime seria a atividade criminosa ligada diretamente a qualquer ação ou prática ilícita na internet. Ainda, pode se dizer que são crimes com utilização de computadores e internet, com fins de fraudar sistemas de comunição, segurança de computadores e redes corporativas. As empresas, atualmente, são as mais visadas, por conter informações sigilosas que podem gerar retorno financeiro em grande escala.

Melhor dizendo, é toda atividade criminal de caráter virtual que se realiza com a finalidade de conseguir seus objetivos financeiros. É o uso do meio digital, através de ataques localizados, a um indivíduo, uma pessoa jurídica ou órgão governamental, de modo a causar terror, com o intuito de obter quantia significativa ou informações, bem como, gerar danos. Vale ressaltar, a conduta de hackers desenvolve-se fora do contexto comum. Por isso, combater esse tipo de crime e levar os criminosos ao tribunal é uma tarefa, extremamente, complexa.

Dessa forma, pode-se classificar o cibercrime das seguintes formas: *Cyberbullying*, cujo usa a internet e outras tecnologias para propagar frases, textos ou imagens, com o intuito de constranger ou intimidar um sujeito ou grupo; *Ciberguerra*, em que a guerra não ocorre de modo físico, mas no meio informático, onde os ataques são deferidos entre nações ou organizações por métodos cibernéticos; *Ciberterrorismo*, que seria a utilização da internet para atacar nações, a fim de implantar ideais defendidos pela organização e gerar aflição. Esse tipo de crime cibernético se fortaleceu após a expansão da internet no mundo e a inserção do terrorismo em meios digitais; *Ciberespionagem*, o qual utiliza algum método virtual para obter informações sigilosas de indivíduos, com a intenção de vigiar ou controlar o fluuxo de dados.

A ideia inicial de combate aos cibercrimes nas legislações nacionais era a de proteção exclusiva da ordem interna dos Estados. Assim, para tal luta, serve-se a norma interna de figuras penais do direito comum. Nessa linha de raciocínio, entende-se que a maior parte das legislações internas que tratam do tema consideram as condutas por meios virtuais como infrações de direito penal comum.

---

[4] 2019. NASCIMENTO, Samir. Cibercrimes: Conceito, modalidades e aspectos jurídicos-penais. Âmbito Jurídico. Disponível em <https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitos-modalidades-e-aspectos-juridicos-penais/>

Todavia, essa definição precisou ser modificada, em virtude da amplitude que alcançou esses atos e, consequentemente, da necessidade de criação de normas que tutelem especificamente o terrorismo.

1.2. Os Crimes Virtuais no Século XXI

O aparecimento dos primeiros casos de crimes cibernéticos ocorreu por volta da década de 1960, onde o infrator manipulava, sabotava ou exercia uso abusivo de computadores e sistemas. A partir de 1980, houve um aumento das ações criminosas, que passaram a ser mais diversificados, como, por exemplo, manipulações de caixas bancários, pirataria de programa, abusos de telecomunicação e pornografia infantil. Historicamente, os cibercrimes vêm sofrendo modificações em seus métodos de conduta a partir da evolução dos meios de comunicações e digitais. Tomou força após a globalização, onde as nações aprimoraram suas relações e a maneira de compartilhar informações. Com isso, os praticantes do cibercrime, começaram a se modernizar e mudar suas técnicas, para então conseguirem seus objetivos.

Com o início do século XXI, os crimes cibernéticos passaram a acontecer com mais frequência, criando uma nova identidade, carregados de conceitos modernos, porém sem perder a essência do passado. Pode se dizer, portanto, que foi modernizado em razão das mudanças globais ao longo dos anos.

O crime virtual é uma prática constante no Brasil e tomou força no século XXI. O país liderou o ranking mundial de cibercrime, em 2002, segundo informações de uma empresa britânica[5]. No ano de 2004, através uma pesquisa feita pela mesma empresa do Reino Unido, foi constatado que o Brasil abriga um dos maiores números de hackers ativos do mundo. Na área de pirataria de software, a indústria de programas para computador fez uma estimativa de mais de um bilhão de dólares de prejuízo no Brasil em 2007. Já em 2008, o Brasil liderou o ranking de ataques às contas bancárias. Ainda, uma pesquisa feita por uma empresa fornecedora de antivírus, Symantec, revelou que o país registra uma média de 3 mil violações de segurança por dia, bem superior à média mundial. Somente em 2017, foi contabilizado que 62 milhões de brasileiros sofreram um cibercrime, representando cerca de 60% da população adulta que utiliza os meios digitais no país.

[5] Crime Informático. Disponível em <https://pt.wikipedia.org/wiki/Crime_inform%C3%A1tico>

Os crimes cibernéticos podem ser classificados em: virtuais puros, mistos e comuns. O *Crime virtual puro* seria a conduta ilícita, cuja atenta o hardware e/ou software de um computador, ou seja, tanto a parte física quanto a parte virtual. Já o *Crime virtual misto* utiliza a Internet para realizar a conduta ilícita, e visa, muitas vezes, as transações ilegais de valores de contas correntes. Por fim, temos o *Crime virtual comum,* o qual é utilização da Internet apenas como um instrumento para realização de crimes, estes normalmente especificados no Código Penal, como, por exemplo, distribuição de conteúdo pornográfico infantil por diversos meios, espionagem, violação de autorização, falsificação de dados, vazamento indevido de informação, sabotagem do computador e muitos outros meios.

Podemos ainda caracterizar tais crimes em dois tipos básicos. Os crimes cometidos por meio da utilização de computador como ferramenta para cometer a infração, bem como, aqueles cujo crime é cometido contra o computador em si, o objeto é danificado ou prejudicado de alguma forma.

No século atual, se tornou cada vez mais comum a mídia mundial utilizar o termo "guerra cibernética" para definir uma série de ataques cibernéticos direcionados a um país. Richard Clarke, especialista em segurança do governo estadunidense, conceituou a guerra cibernética como um conjunto de ações efetuadas por um Estado que acarretam a penetração dos ordenadores ou em redes de outro país, com o objetivo de causar prejuízo ou alteração. Em contra partida, Arquilla e Ronfeldt acreditam que essa guerra diz respeito ao ato de preparar e conduzir operações militares de acordo com princípios relacionados à informação, ou seja, significaria causar graves danos no que se refere aos dados e sistemas de comunicação.

Secundum Bruce Schneier, especialista em segurança cibernética, questiona todas as ideologias existentes de guerra cibernética. Segundo ele, na maioria das vezes, a definição desse tipo de guerra não está bem aplicada, pois, ainda não se sabe como é uma guerra no espaço cibernético, quando ela se inicia e tampouco se sabe como fica o espaço cibernético após o término da guerra. Para Schneier, tanto os políticos quanto os especialistas em segurança cibernética não estão de acordo quanto à definição adequada para a guerra cibernética. As guerras virtuais mencionadas, em sua grande maioria, são consideradas guerras retóricas porque se observa que o conceito de guerra está aplicado em situações que na realidade não ocorrem no âmbito físico. Ademais, todas as ações que já foram classificadas como guerras cibernéticas poderiam se encaixar em tipos penais já existentes na maioria

dos ordenamentos jurídicos dos países democráticos. O especialista opina ainda que há uma dificuldade em definir a guerra virtual devido a confusão feita pela maioria das pessoas com tática de guerra, isto é, muitos acreditam que esse tipo de conflito nada mais é do que uma tática governamental para atacar outras nações. Ressalta ainda que a impossibilidade de identificar as atribuições dos ataques cibernéticos e de saber seus reais motivos enfraquece a classificação de tais acontecimentos como guerra.

Atualmente, existe um certo exagero por parte de alguns governos e da própria mídia em enfatizar a existência de guerras cibernéticas quando de fato são em sua maioria atos de espionagem. Em países democráticos, este exagero se torna algo ruim, principalmente, pelo fato de os governos usarem esse pretexto para tentar controlar cada vez mais o espaço virtual em nome da segurança nacional. Todavia, alguns países terminam desrespeitando importantes valores democráticos, como, a privacidade.

Houve alguns cibercrimes no século atual que marcaram a história de maneira simbólica e até os dias atuais, principalmente nos países que aconteceram os fatos, existem lembranças e cicatrizes severas. Dentre eles estão, o ocorrido em 2003, com o famoso “hacker do chapéu cinza”, Adrian Lamo, o qual obteve sua fama após invadir o sistema do jornal The New York Times, um dos mais renomados jornais dos Estados Unidos, e incluir seu nome na lista de colaboradores. O jornal denunciou Lamo ao FBI e o próprio se declarou culpado em 2004 pelo crime e por ter invadido os sistemas do Yahoo, Microsoft e WorldCom, grandes empresas do mundo digital, pegando seis meses de prisão domiciliar e mais dois anos de liberdade vigiada. Anos depois, veio a público sua denúncia no FBI contra um soldado do exército americano, o qual, segundo Lamo, foi responsável por vazar informações sigilosos sobre a Guerra do Iraque, inclusive de um vídeo em que uma aeronave dispara contra civis. Alegou ter feito a acusação na tentativa de salvar milhares de soldados americanos em combate. Antes criticado por suas ações como hacker, hoje é cumprimentado por muitas pessoas pelo seu patriotismo.

Outro caso dessa espécie a ser citado é de Albert Gonzalez, onde obteve uma vida de milionário devido às suas habilidades, com mansão, carros de luxo e festas invejáveis. Porém, não de modo positivo. Conseguiu tudo isso graças a um programa criado por um amigo que, através desse instrumento, ele invadiu os sistemas de lojas famosas, extraiu informações importantes e sigilosas, assim como, aproximadamente 130 milhões de números de cartões de crédito. Ele vendia os dados dos clientes na

internet e, com os cartões, realizava compras fraudulentas e, em seguida, vendia os produtos virtualmente. Foi considerado o maior esquema de fraude da história até o momento. Tudo isso aconteceu durante os anos de 2005 e 2007. Contudo, somente foi descoberto e levado para a prisão muitos anos depois, condenado a 20 anos de prisão, todavia, reduzida a pena em cinco anos devido suas alegações de ter uma série de problemas que possibilitaram tal redução.

Existem muitos outros crimes cibernéticos que causaram grande movimentação e alerta, como, por exemplo, no ano de 2009, em que o francês François Cousteix, conhecido como “Hacker Croll”, invadiu a conta do Twitter, famosa rede social, do homem considerado o mais poderoso do plantea na época, presidente norte-americano Barack Obama. Assim como, conseguiu também adentrar nas contas de celebridades, como, Britney Spears, e nos servidores de empresas renomadas, como, por exemplo, Fox News e Facebook. Em sua defesa, alegou ter feito isso para alertar os internautas sobre a escolha da senha e que nenhum dado foi destruído. Mesmo assim, foi condenado por suas ações à cinco meses de liberdade vigiada, pena mais rigorosa do que a pedida pelo Ministério Fiscal, que era de dois meses.

E para finalizar, podemos destacar também o caso na Rússia, cujo nome do autor nunca foi revelado, onde o indivíduo utilizou de suas capacidades e conhecimentos tecnológicos para invadir o sistema do telão de anúncio publicitário no centro da capital russa, exibindo vídeo de conteúdo pornográfico durante uns vinte minutos, causando confusão e engarrafamento, pois as pessoas paravam para assistir. Foi preso semanas após o ocorrido, confessando a autoria do delito, e está aguardando julgando, podendo receber até dois anos de prisão, com fulcro em Lei vigente no país. Após o incidente, o país estuda a possibilidade de banir publicidade através de telões.

Pode se entender que, com a modernização, os amplos meios de comunicação e armazenamento de dados e o avanço tecnológico, elementos marcantes da era contemporânea, os cibercriminosos conseguiram desenvolver, inclusive no que tange a amplitude de suas ações e as habilidades técnicas dos seus autores, métodos ainda mais eficazes de invasão e que possibilitam um grande alerta na sociedade. O cibercrime sempre esteve um passo a frente do desenvolvimento tecnológico, visto seu contexto histórico, pois existe e é algo forte antes mesmo do surgimento e expansão do espaço informático, e continua cada vez mais se modernizando e expandindo seus objetivos. Os objetos utilizados por eles, os computadores, se

tornaram de fácil aquisição e mais poderosos com o passar dos anos, os quais, atualmente, a grande maioria da população mundial possui em sua residência ou trabalho. Com isso, gera um número maior de alvos, bem como, possibilidades maiores de ataques e a criação de métodos diversificados para efetuar.

Ademais, o mundo está adentrando cada vez mais na era digital, principalmente, empresas, como, por exemplo, bancos, então serão alvos com mais frequência, visto o principal objetivo dos autores desses delitos, que seria a parte financeira. Portanto, é preciso tomar os devidos cuidados, inclusive, por conter dados de clientes e armazenar dinheiro destes. Assim como, as pessoas de modo geral e que andam muito "conectadas" devem se precaver e tomar cuidado, pois qualquer um pode ser vítima de um crime cibernético.

2 OS CRIMES CIBERNÉTICOS E A LEGISLAÇÃO BRASILEIRA

Neste segundo capítulo da obra, será destacada a maneira como a legislação do Brasil classifica e trata os crimes virtuais, trazendo as alterações da Lei Carolina Dieckmann, algumas jurisprudências para melhor compreender o método de julgamento dos magistrados, com base nas mudanças da legislação pátria, e de que forma tais condutas ilícitas podem atingir alguns princípios constitucionais vigentes.

2.1 A Origem da Lei Carolina Dieckmann e suas Alterações Legislativas para o Combate dos Cibercrimes

A Lei Carolina Dieckmann, Lei nº 12.737/2012, assim como a Lei Maria da Penha, foi criada a partir de um acontecimento que marcou o cenário brasileiro. No ano de 2012, a atriz Carolina Dieckmann teve seu computador invadido e suas informações pessoais subtraídas, inclusive, fotos íntimas que, posteriormente, se espalharam na internet, causando enorme constragimento à vítima. O caso chamou atenção e teve grande repercussão, dando origem ao projeto de Lei, o qual não demorou a ser sancionado e a nova Lei ser incorporada na legislação pátria.

Na parte da legislação[6] que trata a respeito da invasão de dispositivo informático, temos o art. 154-A que foi incorpordo no Decreto Lei nº 2.848/1940 (Código Penal Brasileiro), o qual diz: "***Invadir dispositivo informático alheio,***

[6] **Lei nº 12.737 de 30 de Novembro de 2012.** Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>

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". Podemos observar alguns termos que trazem a ideia de uma objetividade jurídica da Lei apegada à tutela da liberdade individual, isto é, visa assegurar o sigilo de dados e informações de cada indivíduo armazenados em dispositivos informáticos.

Essa modalidade de ilícito admite que pode figurar no polo ativo qualquer pessoa, pois não é exigida nenhuma qualidade especial do autor. Assim como, qualquer indivíduo que venha a sofrer danos com o crime pode figurar como sujeito passivo. Um terceiro também pode aparecer no polo passivo, visto a possibilidade de danos ao mesmo pela conduta típica. Ademais, trata-se de crime de ação vinculada, pois exige para a capitulação do fato ao tipo penal, que a conduta seja praticada "mediante violação indevida de mecanismo de segurança".

Est digna, não basta a vontade livre e consciente do autor de invadir dispositivo informático alheio, devendo a conduta conter elementos subjetivos para tal incriminação, isto é, em sua ação deve existir uma das finalidades descritas na norma.

Em regra, para os crimes apontados no art. 154-A, a ação penal é de natureza pública condicionada à representação da vítima ou de seus sucessores, salvo "*se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos*", conforme o *caput* do art. 154-B da mesma legislação, também acrescido no Código Penal.

Para o crime tipificado no *caput* do art. 154-A, a pena inicial é detenção de três meses a um ano e multa. Muitas pessoas acham uma punição branda, visto o dano que as ações desses sujeitos podem alcançar. Todavia, existem mecanismos na Lei que proporcionam o aumento da punibilidade, conforme a dimensão da conduta. Como exemplo, podemos citar o §3º desse artigo, que diz: "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, a pena será reclusão de seis meses a dois anos, e multa, se a conduta não constitui crime mais grave". Observa-se uma punição pelo crime mais rigorosa, podendo haver ainda causas de aumento proporcionais à

conduta do autor do delito. Mas, será que a pena ainda é adequada se analisado os resultados que esses tipos de ações podem chegar, bem como, os danos de diferentes naturezas que a vítima sofre?

Há mais questões tratadas na Lei para ampliar o rol de condutas por ela enquadradas. Seria o caso dos artigos 266 e 298, ambos incorporados no Código Penal brasileiro, que abordam acerca da interrupção ou perturbação de serviços de utilidade pública e falsificação de documentos, respectivamente. O indivíduo pode pegar detenção de um a três anos e multa, no caso em que for julgado por crime definido no art. 266 da legislação, e reclusão de um a cinco anos e multa para delito enquadrado no art. 298 da mesma Lei. A única possibilidade de aumento de pena dentro dessas situações seria o exposto no §2º do art. 266, o qual informa que "Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública". Ou seja, para crime de falsificação de documentos, abordado pelo art. 298, não há possibilidade de aumento de pena.

No decorrer de uma investigação criminal de um crime cibernético, é comum que a autoridade policial, ao solicitar informações cadastrais a provedores de conteúdo digital que possibilitem mais agilidade e eficácia no trabalho, tenha que esperar muito. Em muitas situações, inclusive, a prestação de tais informações é falha, incompleta, sem mencionar a burocracia estatal vigente. O combate a esses tipos de crimes no país ainda é muito desafiador por conta da dificuldade no rastreio das informações.

A Lei 12.737/12, apesar de ser considerada como um avanço na investigação de crimes virtuais, não dispõe, dentre outros defeitos, de meios processuais que garantam a sua eficácia. Sua vigência, por mais tardia, demonstrou obter determinados equívocos em sua redação. Se considerarmos que a referida lei foi criada especialmente para a punição de condutas ilícitas cometidas por meios informáticos, esta demonstra uma tímida repressão estatal, pouco inibidora para os criminosos. Isso se dar, principalmente, pela pena imposta aos crimes dessa natureza.

O tipo penal em questão apenas se configura como crime quando sua finalidade for especificamente obter, adulterar ou destruir dados e informações, com fulcro no exposto em Lei, caso contrário, não há o que se falar em crime. Outra falha que podemos apontar seria a ausência de definição a respeito do termo "mecanismo de segurança" apresentado no art. 154-A da legislação. Vejamos, se o dispositivo

invadido não possuir qualquer tipo de proteção, a conduta será atípica, uma vez inexistente a modalidade culposa. Ou seja, uma questão importante na hora de julgar tal conduta. Ademais, estabelece que dispositivo tem que ser indevidamente violado ou invadido.

BERETTA[7] (2014), traz um ótimo exemplo dessa situação. Um sujeito X e outro Y são amigos e cada um está com o seu computador. X pede a Y seu notebook emprestado e Y empresta, autorizando o seu acesso. Acontece que X sabia que seu amigo estava lhe traindo tendo relações com sua namorada. Assim, ao utilizar o computador de Y, X encontra diversas fotos de Y com sua namorada em momentos íntimos. X, então, entra no sistema de fotos do computador de Y e adquire, altera e apaga todas as fotos para posterior divulgação na Internet. Nesse caso em tela, com base na redação do art. 154-A da Lei Carolina Dieckmann, não houve prática de crime por parte do sujeito X, visto que o mesmo não utilizou de nenhum método para violar o sistema e obter acesso ao dispositivo de Y. Ocorreu a autorização tácita, portanto, não pode ser enquadrado em tal legislação.

Essa Lei vem sendo palco de muitas críticas, pois, para muitos, seus dispositivos são amplos, confusos e podem gerar dupla interpretação, ou mesmo interpretação subjetiva. Resultando, portanto, na utilização dela para enquadramento criminal de condutas triviais, ou para a defesa e amparo de praticantes desse ilícito, o que poderia tornar a lei ineficaz. Ainda, acreditam que as penas são pouco inibidoras, o que poderia contribuir para ineficiência no combate ao crime cibernético no Brasil. Isso pode ocorrer em detrimento à falhas técnicas a respeito da presença de termos vagos dificultando para que o mesmo seja enquadrado na Lei, ou seja, nota-se uma falta de cuidado ao formalizar o projeto de lei e melhor aproveitamento de ideias.

Um dispositivo jurídico que merece breve citação é a Lei nº 12.965/2014, mais conhecida como Marco Civil da Internet ou Constituição da Internet. Foi criada a partir de um movimento antagônico aos projetos para implementação da Lei Carolina Dieckmann, com intuito de suprir algumas lacunas deixadas por esta em sua redação. Nessa Lei estão contidos dez princípios que garantem a liberdade de

[7] 2014. BERETTA, Pedro. **Sem Meios Eficazes, Lei Carolina Dieckmann até Atrapalha**. Disponível em <https://www.conjur.com.br/2014-mai-10/pedro-beretta-meios-eficazes-lei-carolina-dieckmann-atrapalha>

expressão, a privacidade e os direitos humanos no ambiente digital, porém não impossibilita o controle necessário à segurança de dados e informações, de pessoas ou empresas, pelas entidades competentes. O objetivo desse dispositivo é definir o que pode ou não fazer durante a utilização de meios virtuais no âmbito civil, antes de criminalizar uma conduta.

2.2 Atuação do Poder Judiciário Brasileiro após Vigência da Lei nº 12.737/2012

No tocante ao cenário do Poder Judiciário brasileiro, posterior ao início da vigiência da Lei Carolina Dieckamnn, há uma grande quantidade de julgamentos que fazem citação à legislação. Contudo, a maior parte dos julgados diz respeito ao aproveitamento da alteração no Código Penal promovida por essa Lei em benefício do infrator. Isto é, muitos juristas ao elaborarem a defesa de seu cliente, querem utilizar de tal mecanismo jurídico, principalmente o *caput* do art. 154-A, para obter a pena mais benéfica ao réu.

Dito isso, é possível concluir, portanto, que a Lei, criada com a finalidade de julgar crimes virtuais e evitar a ocorrência desses em maior escala, pois acreditavam os colaboradores de tal legislação, que estavam criando algo que causaria inibição aos praticantes do crime em questão, todavia, resultou em uma maneira de obter vantagem por parte dos autores do delito. Mostrando, assim, que podem existir falhas significativas na aludida norma jurídica e ficando cada vez mais evidente os motivos para tantas críticas.

Para exemplificar o mencionado, vejamos um caso de Santa Catarina[8], STJ – HC: 288812 SC 2014/0035193-7, onde o advogado do réu impetrou pedido de *habeas corpus* e, um dos seus argumentos, seria a aplicabilidade do art. 154-A do Código Penal, por entender a conduta do seu cliente se enquadrava na situação ora em questão, visando obter a lei penal mais favorável ao acusado em sua pena. A relatora designada na época assim não entendeu e indeferiu seu pedido.

Outra situação ocorreu por meio de Recurso Especial a favor do réu. O caso

[8] Jusbrasil, 2014. Superior Tribunal de Justiça STJ – habeas corpus. Disponível em <https://stj.jusbrasil.com.br/jurisprudencia/890989535/habeas-corpus-hc-288812-sc-2014-0035193-7?ref=serp>

aconteceu no estado de São Paulo[9], STJ – Resp: 1834023 SP 2019/0253101-2, em que o réu foi acusado por roubo majorado pelo emprego de arma de fogo. Em sede de Recurso Especial, o advogado do réu, além de outros pedidos, solicitou à autoridade judicial que fosse observado o exposto no art. 154-A, alegando que, na ocasião, houve desrespeito dessa lei por parte da autoridade policial em seu procedimento para extração de provas. Utilizou o jurista da norma, que teoricamente deveria ser temida por criminosos, para benefício de seu cliente, obtendo êxito nesse pedido, pois o relator do processo entendeu que houve violação da norma por parte da autoridade policial, decidindo como produção de prova ilícita.

Pode se concluir, portanto, com base nos exemplos trazidos acima e no exposto durante o presente trabalho, que tal modificação na legislação pátria tem defeitos explícitos e esses estão sendo usados para obtenção de vantagem processual. Por mais frequentes os pedidos em favor do réu por meio dessa Lei, os magistrados não estão reconhecendo tais solicitações em benefício do autor do delito, porém encontram dificuldades em julgar tais situações.

CONSIDERAÇÕES FINAIS

Assim, com a tradução de cibercrime, abordando seus elementos e suas características, bem como, a concepção deste no âmbito do ordenamento jurídico brasileiro, conclui-se que a lei vigente no país, elaborada equivocadamente e com falhas técnicas gritantes, não é capaz de ajuizar com total precisão os atos que poderão ser enquadrados na ideia de crime cibernético. Isso é resultado de uma tentativa de conter as manifestações populares na época, porém sem sucesso e terminou que a lei concede uma aplicação distinta do seu propósito, devido a sua redação vaga e pouco eficiente.

Caso um sujeito, suspeito pela prática de um crime virtual, fosse levado a julgamento hoje, pelas modificações na lei brasileira oriundas da Lei Carolina Dieckmann, haveria muitas dúvidas quanto ao enquadramento do ato na legislação pátria, assim como, possibilidade de atipicidade da conduta, determinada, inclusive, pelas imprecisões no texto de Lei. Ademais, tal redação mostra-se pouco eficiente no

[9] Jusbrasil, 2020. Superior Tribunal de Justiça STJ – Recurso Especial. Disponível em <https://stj.jusbrasil.com.br/jurisprudencia/861474973/recurso-especial-resp-1834023-sp-2019-0253101-2/decisao-monocratica-861474983?ref=serp>

tocante ao seu papel inibidor, visto seu rigor na penalização da ação, onde o indivíduo pode cometer tais crimes, muitas vezes com danos enormes de diversas categorias à vítima, e pegar uma pena relativamente branda, o que desperta o interesse de outros à cometerem mesmo delito.

Na legislação penal, o delito cibernético foi incorporado de maneira tardia, se observado que o avanço tecnológico ocorre desde o final do século passado e seu desenvolvimento no século atual vem atingindo grandes proporções muito rapidamente, onde todo dia aparece uma novidade na esfera digital. Essa demora poderia ser contornada com uma mudança na Lei bastante eficaz, mas o que aconteceu foi exatamente o oposto disso. O texto legislativo apresenta grandes deficiências técnicas e é evidente que sua criação foi a partir de um acontecimento significativo, do qual precisou tomar medidas urgentes para conter os ânimos da população, resultando uma norma jurídica implantada sem o devido cuidado. Tanto que, para preencher tais defeitos, foi implementado o Marco Civil da Internet, com a finalidade de ampliar a legislação sobre o tema de cibercrime.

Essa falta de definição precisa leva aos cidadãos pensarem em insegurança e o quão ingênuos podem ser os governantes capazes de aprovar uma lei com tantas deficiências em sua redação, pois, com normas dessa espécie, é difícil acreditar que a justiça será feita em casos dessa magnitude e, com tantos atos dessa natureza ocorrendo pelo mundo a fora, causa desconforto em pensar que a lei do país não será capaz de tutelar com toda precisão exigível.

Além disso, o povo contesta, principalmente, o fato da aprovação dessa legislação ter acontecido fundada em fatores internos vivenciados no Brasil, em que os governantes buscavam um meio de interferir nas manifestações, e não estavam pensando em um combate especificamente ao crime cibernético, que ainda anda em uma crescente constante no planeta, observando casos sempre sendo divulgados na mídia, principalmente devido ao célere crescimento que a indústria tecnológica vem sofrendo todos os dias, pois essa espécie de crime se desenvolve juntamente, ou até mesmo está a frente.

O Brasil, por ser um país onde sua população sofre muitos ataques virtuais, com fulcro em dados estatísticos, deveria ser mais agil na tentativa de definição do cibercrime, procurando tipos penais que o compreendam. Era imaginado, no mínimo, uma melhor definição por parte da Lei brasileira, a fim de possibilitar uma aplicação mais efetiva.

Em apertada síntese, a evolução histórica da internet a sua propagação pelo mundo, bem como a necessidade do direito acompanhar essa evolução e mudanças tecnológicas geradas pelo avanço da informática. De acordo com a legislação então existente, contudo, insuficiente para caraterização dos crimes virtuais, a edição da Lei n. 12.737/2012 constituiu um importante avanço na tipificação do crime em comento quando expressamente diz: “invadir dispositivo informático”, criando um tipo penal que visou eminentemente proteger o sigilo de dado e informação pessoal ou profissional. Desse modo, analisamos os elementos típicos básicos do crime: conduta, resultado, nexo causal, tipicidade, consumação e tentativa.

Conclui-se, portanto a legislação supracitada demonstrou uma evolução da nossa legislação, na medida em que notamos uma preocupação da sociedade com a segurança e proteção do direito ao sigilo dos dados e informações no âmbito digital, mas não podemos esquecer que a lei ainda precisa ser aprimorada, principalmente no sentido da clareza e da aplicabilidade de suas disposições.

REFERÊNCIAS

2013. WENDT, Emerson et. al. **Crimes Cibernéticos: Ameaças e Procedimentos de Investigação.** 2ª Edição. Editora Brasport.

2017. DA SILVA, Ângelo Roberto Ilha. **Crimes Cibernéticos**. 1ª Edição. Editora Livraria do Advogado.

2016. BARRETO, Alesandro Gonçalves et. al. **Manual de Investigação Cibernética à Luz do Marco Civil da Internet**. 1ª edição. Editora Brasport.

2020. NICOLAI, Thiago et. al. **O Aumento Silencioso dos Cibercrimes**. Migalhas. Disponível em <https://www.migalhas.com.br/depeso/326593/o-aumento-silencioso-dos-cibercrimes>

2012. QUINTINO, Eudes. **A Nova Lei Carolina Dieckmann**. Jusbrasil. Disponível em <https://eudesquintino.jusbrasil.com.br/artigos/121823244/a-nova-lei-carolina-dieckmann>

Redação Tilt, 2018. **Brasil é o segundo país no mundo com maior número de crimes cibernéticos**. Uol. Disponível em <https://www.uol.com.br/tilt/noticias/redacao/2018/02/15/brasil-e-o-segundo-pais-no-mundo-com-maior-numero-de-crimes-ciberneticos.htm>

2019. NASCIMENTO, Samir. **Cibercrime: conceitos, modalidades e aspectos jurídicos-penais**. Âmbito Jurídico. Disponível em <https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitos-modalidades-e-aspectos-juridicos-penais/>

2003. NETO, Mário et. al. **Crimes na internet: elementos para uma reflexão sobre a ética informacional**. Revista CEJ. Disponível em <http://www.egov.ufsc.br/portal/sites/default/files/crimes_na_internet_elementos_para_uma_reflexao_sobre_a.pdf>

2019. BARRETO, Alesandro et. al. **Cibercrimes e Seus Reflexos no Direito Brasileiro**. 1ª Edição. Editora Juspodivm.

Crime Informático. Disponível em <https://pt.wikipedia.org/wiki/Crime_inform%C3%A1tico>

Terra, 2019. **Dez hackers famosos e seus feitos**. Disponível em <https://www.terra.com.br/noticias/tecnologia/infograficos/hackers/hackers-05.htm>

Constituição da República Federativa do Brasil de 1988. Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>

2014. BERETTA, Pedro. **Sem Meios Eficazes, Lei Carolina Dieckmann até Atrapalha**. Disponível em <https://www.conjur.com.br/2014-mai-10/pedro-beretta-meios-eficazes-lei-carolina-dieckmann-atrapalha>

Lei nº 12.737 de 30 de Novembro de 2012. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>

2013. SIENA, David. **Lei Carolina Dieckmann e a definição de "crimes virtuais"**. Jus. Disponível em <https://jus.com.br/artigos/24406/lei-carolina-dieckmann-e-a-definicao-de-crimes-virtuais>