

CRIMES CIBERNÉTICOS: RÁPIDA DINÂMICA NÃO ACOMPANHADA PELO ORDENAMENTO JURÍDICO

CYBER CRIMES: FAST DYNAMIC NOT ACCOMPANIED BY LEGAL ORDER

Bismarck Thiago de Freitas¹

Bruno Leandro de Carvalho²

RESUMO

O presente artigo tem por finalidade pesquisar acerca dos crimes cibernéticos devido a crescente massa de usuários cada vez mais conectados à internet. Justifica-se essa pesquisa pelas constantes violações de direitos constitucionais, inclusive da dignidade da pessoa humana, e pelos diversos crimes que estimulam os internautas a publicarem conteúdos ofensivos contra pessoas famosas ou não, sem contar os criminosos que praticam o *phishing*, invadem páginas, atuam como hackers, entre outros cibercrimes. Assim, destaca-se o dever que o Direito possui de acompanhar essa evolução para conter esses tipos de crimes, regendo e limitando essas violações cibernéticas. Na elaboração deste artigo, a metodologia utilizada foi hipotético-dedutiva, utilizando de pesquisas bibliográficas e artigos acerca do tema. Destarte, o presente artigo vem nos atentar aos riscos enquanto usuários da web, uma vez que visa ajudar na prevenção de fraudes, de modo que alerte as pessoas a não cair em tais crimes praticados no ambiente virtual, além de nos trazer ainda os tipos de crimes mais cometidos, o público alvo e o *modus operandi* dos criminosos. Após serem percorridos os tipos de crimes e como os criminosos atuam, o artigo vem com objetivo de expor como a lei penal trata esse

¹

²

tipo de crime, sendo defendido a tese de que, o ordenamento jurídico oferece leis em sentido genérico com relação a prática de crime no ambiente virtual, fazendo com que os usuários fiquem vulneráveis, às vítimas desamparadas e os criminosos destemidos devido suas condutas perante o Código Penal Brasileiro.

Palavras-chave: cibercrimes, dignidade da pessoa humana, técnicas para prevenção de fraudes virtuais, riscos, leis para prevenção.

ABSTRACTS

This article aims to research cyber crimes due to the growing mass of users increasingly connected to the internet. This article is justified by constant violations of constitutional rights, including the dignity of the human person, and by the various crimes that encourage internet users to publish offensive content against famous or not, not to mention the criminals who practice phishing, invade pages, act hackers, among other cybercrimes. Thus, we highlight the duty that the right has to follow this evolution to contain these types of crimes, governing and limiting these cyber violations. Thus, it comes to us to pay attention to the risks as web users, since the article in question aims to help prevent us from falling into such crimes committed in the virtual environment. target audience and the Modus Operandi of criminals.

Keywords: *cybercrime, human dignity, techniques for preventing virtual fraud, risks, laws for prevention.*

Sumário: 1. Introdução; 2. Desenvolvimento; 2.1 Aspectos Históricos e o avanço da tecnologia; 2.1.1 A sociedade e o uso da internet; 2.1.2 Conceito de crimes cibernéticos; 2.2 Os principais crimes praticados no ambiente virtual; 2.2.1 Pornografia infantil ; 2.2.2 Sites fraudulentos; 2.2.3 Sequestro de dados (*Ransomware*); 2.2.4 Estelionato; 2.3 Como agir ao ser vítima do crime virtual; 2.4 Dos crimes cibernéticos no ordenamento jurídico; 2.4.1 Lei 12.737/2012 - Lei Carolina Dieckman; 3. Das condutas fraudulentas virtuais não tipificadas; 4. Conclusão; 5. Referências.

1 INTRODUÇÃO

Inicialmente será feita uma breve explanação sobre o avanço do uso da internet na sociedade atual, com a descrição dos principais riscos aos quais todos os usuários estão expostos. Nesta esteira, com o intuito de introduzir o tema central do artigo e esclarecer, de maneira ampla, como ocorre a investigação de crimes cibernéticos, serão apresentados alguns conceitos relacionados à coleta de provas no ambiente virtual.

Ao longo do presente artigo será apresentada parte dos crimes virtuais mais praticados na atualidade (pornografia envolvendo crianças e adolescentes, clonagem do WhatsApp, falso e-mail de sites de vendas online, anúncio duplicado ou do intermediador de vendas, e os sites de comércio eletrônico e outros modos de atuação dos criminosos).

No desenvolvimento da leitura apresentamos quais são as principais vítimas de crimes virtuais especificamente o tipo de crime para cada perfil de vítima, e relatar a consequência do crime que traz para pessoa que acaba sendo vítima, do menor prejuízo até ao mais grave que pode levar uma vítima desse crime até ao suicídio.

Discorreremos também sobre o ordenamento jurídico que rege sobre os crimes cibernéticos que resultou na Lei nº 12.737/2012 (Lei Carolina Dieckmann) que, foi proposto em referência e diante de situação específica experimentada pela atriz, em maio de 2012, que teve arquivos copiados de seu computador pessoal, 36 (trinta e seis) fotos em situação íntima e conversas, que acabaram divulgadas na Internet. Com a alteração, o Código Penal Brasileiro ganhou o acréscimo dos artigos 154-A e 154-B no Capítulo IV, que trata dos crimes contra a liberdade individual, mais precisamente na seção dos crimes contra a inviolabilidade dos segredos. Por fim, conclui-se que ainda há tempo para combater o crescente número de crimes cibernéticos, com a consequente aplicação de punição a quem os pratica.

2 DESENVOLVIMENTO

2.1 ASPECTOS HISTÓRICOS E O AVANÇO DA TECNOLOGIA

Antes de entrar em conceitos mais específicos, é importante salientar o contexto histórico sobre a tecnologia onde foi criado o primeiro computador do mundo, que foi durante a segunda guerra mundial onde o exército dos Estados Unidos precisava de um computador específico capaz de realizar cálculos balísticos e tábuas de bombardeamento de forma rápida e ágil e que pudesse ser programável. No dia 15 de Fevereiro de 1946 entrou em operação o primeiro computador programável de uso geral moderno da história, com a siglas ENIAC, (Electronic Numerical Integrator and Computer), feito pelos pesquisadores norte-americanos John Eckert e John Mauchly, da Electronic Control Company, chegando a pesar 30 toneladas e ocupando uma área de 180 m² sua produção custou aproximadamente R\$ 6 milhões em relação a moeda de hoje, a ENIAC contava com hardware equipado com 70 mil resistores e 18 mil válvulas de vácuo que em funcionamento consumiam aproximadamente 200 mil watts de energia. 75 anos após á esse marco, a tecnologia vive um avanço exponencial tão grande em que consiste em um computador que ocupava tanto espaço comparado a um simples smartphone que cabe no bolso da calça e que guarda tantas informações em seu imensurável gigas de memória é de se assustar com tamanha evolução. Nos tempos de hoje guardamos dados bancários, documentos pessoais, confidenciais, dados de empresa resumindo, deixamos praticamente nossas vidas sob um simples aparelho.

2.1.1 A sociedade e o uso da internet

De acordo com informações coletadas da pesquisa TIC Domicílios 2019 – mais importante levantamento sobre acesso a tecnologias da informação e comunicação, realizado pelo Centro Regional para o Desenvolvimento de Estudos sobre a Sociedade da Informação (Cetic.br), vinculado ao Comitê Gestor da Internet no Brasil –, três a cada quatro brasileiros acessam a internet, o que corresponde a 134 milhões de pessoas, que, em regra, utilizam smartphones e outros dispositivos móveis (99%), computadores (42%), TVs (37%) e videogames (9%) (VALENTE, 2020).³

Com base nos dados expostos acima, constata-se que a expansão e facilidade de acesso a internet vem sendo a cada dia mais útil, uma vez que, nos permite um

³ Disponível em <https://agenciabrasil.ebc.com.br/geral/noticia/2020-05/brasil-tem-134-milhoes-de-usuarios-de-internet-aponta-pesquisa>. Acesso em 24 de novembro de 2020.

amplo acesso a informações, entretenimento, lazer, conhecimento, serviços bancários e além de nos proporcionar um maior conforto em fazer compras sem sair de casa, através dos sites de vendas online. Ou seja, a internet resultou em uma maior facilidade e praticidade na vida de seu usuário, sendo de grande importância para o cidadão brasileiro, como pôde ser analisado através dos dados da pesquisa citada anteriormente.

Diante de infinitas modernizações na área da informática e tecnologia, é fundamental que o cidadão tenha certo conhecimento nessa área, pois a mesma servirá como ferramenta facilitadora, tanto em tarefas domésticas quanto em laborais, como citado anteriormente.

Ressalta-se que um dos fatores importantes que contribuíram para o aumento no acesso a internet, é a popularização dos computadores, uma vez que, cada vez mais é possível encontrar, máquinas com preços acessíveis, além de uma maior facilidade de acesso à internet, possibilitando a grande maioria da sociedade de possuir acesso à rede.

Entretanto, a popularização e o avanço da tecnologia fizeram com que surgissem novos hábitos, hábitos que facilitam a vida do usuário, que os possibilitam de cumprir com seus afazeres em tempos menores, como por exemplo, a comunicação feita antigamente era feita através de cartas, atualmente basta digitar em seu teclado, seja em um computador ou aparelho celular, e clicar em enviar. Contudo, além dos pontos positivos com o avanço da tecnologia, também surgiram pontos negativos, como a decadência no convívio social, que foi substituído pelo meio virtual, e o mais importante dos pontos negativos, os crimes cibernéticos, que surgiram em consequência da popularização tecnológica e no aumento de usuários conectados a rede.

2.1.2 Conceito de crimes cibernéticos

Para entendermos melhor sobre os crimes cibernéticos, é necessário frisar que os crimes cibernéticos são todas aquelas ações que utilizam os computadores ou dispositivos móveis, como ferramenta para a prática de crimes, ou seja, é um crime a qual necessita da internet como meio de praticá-lo, com o objetivo de causar transtorno e/ou prejuízo a outrem ou de obter vantagens ilícitas, como por exemplo,

vantagens financeiras ou favorecimentos sexuais, entre outros; crimes estes, que na maioria das vezes o usuário da internet se torna vítima sem perceber, seja pela instalação de algum programa desconhecido ou o fornecimento de dados pessoais através de sites ou emails.

2.2 OS PRINCIPAIS CRIMES PRATICADOS NO AMBIENTE VIRTUAL

Atualmente, houve um significativo aumento no número de usuários de internet, porém como consequência deste aumento, o número de crimes praticados no meio virtual também aumentou, além da implementação de novas modalidades de crimes cibernéticos pelos criminosos, que assolam os usuários podendo qualquer um a qualquer momento ser a próxima vítima, sendo mediante internet ou por exemplo o golpe do boleto ou de uma multa de trânsito ou conta de luz, por mais que a pessoa não faça o uso da internet ainda pode ser uma vítima de fraude, devido as ferramentas que ela oferece, portanto foi selecionado os crimes mais cometidos nos tempos atuais e como agir ao ser vítima do referido crime.

2.2.1 Pornografia infantil

A mídia social vem crescendo cada vez mais em popularidade de crianças e adolescentes nos tempos de hoje em que é normal uma criança de pelo menos aos 10 anos ter um smartphone e está logada em aplicativos mais populares como, whatsapp, instagram, facebook, tal crescimento dessa população específica infelizmente vem acompanhada de crimes de pornografia infantil, isto porque uma certa parte seria devido a uso de livre desses aplicativos principalmente aos que são livres para o público exemplo o instragram, e consequentemente lhes deixando vulneráveis para a prática desse tipo de crime.

As principais formas de atuação dos criminosos em relação à criança basicamente é se passando por uma outra da mesma idade assim, lhe atraindo como uma nova amizade e em seguida lançar sua isca o criminoso irá persuadindo a vítima até conseguir o que deseja.

As penas previstas para quem for flagrado cometendo o crime de pornografia infantil está na letra da lei do art. 241-A do Estatuto da criança e adolescente, onde diz que

“quem exportar, comercializar, distribuir, divulgar etc”, pena de 3 a 6 anos , e multa. O método mais eficaz para evitar este tipo de crime é o acompanhamento constante do país em inspecionar os conteúdos que seus filhos acessam e principalmente manter o diálogo, para evitar a prática dos criminosos tendo em mente que seus filhos nunca estão 100% seguros na internet, outras formas de prevenção é sempre estar atento ao comportamento da criança.

2.2.2 Sites fraudulentos

Um dos principais cibercrimes cometidos são os sites fraudulentos devido a grande movimentação de compras via internet e sua praticidade se tornou um alvo para os criminosos em fraudar sites mais conhecidos popularmente para aparentar ser seguro e o usuário se sentir mais confiante em comprar algum produto. Basicamente os criminosos copiam o layout de empresas conhecidas lançam uma suposta promoção por exemplo uma black friday e colocam um produto bem abaixo do valor de mercado, fazendo que a vítima se sinta maravilhada com aquela promoção vindo a comprar o produto, achando que está fazendo um bom negócio acaba não verificando a parte mais simples que é os dados do sacador, sendo os dados do CNPJ e razão social.

Esse tipo de crime é um dos mais cometidos no Brasil de acordo com a pesquisa feita pelo Serviço de Proteção ao Crédito (SPC)¹ no ano 2018 e 2019 relata que 54% dos consumidores brasileiro já foram vítimas de alguma fraude dados mostrados de consumidores que identificaram que foram vítimas pois existem aquelas que ainda não tomaram ciência que foram enganadas.

¹ Disponível em

https://www.spcbrasil.org.br/uploads/st_imprensa/release_fraudes_v6.pdf. Acesso em 28 de abril de 2021.

2.2.3 Sequestro de dados (*Ransomware*)

Ransomware é uma espécie de *malware* que os cibercriminosos instalam no computador do usuário sem que este tenha a mínima noção; diante dessa “invasão” os criminosos vão trabalhando às escondidas, em segundo plano, e acabam criptografando todos os arquivos, arquivos estes, que ao tentar abrir irá aparecer uma mensagem pedindo uma certa quantia para que os dados do usuário sejam

liberados, ou seja, um verdadeiro seqüestro de dados. Ressalta-se que, os cibercriminosos mantêm seu aparelho celular ou computador bloqueado até que o pagamento pedido por eles seja efetuado.

Este tipo de crime geralmente é praticado quando o usuário abre um email mal intencionado ou ao visitar sites maliciosos, por isso é de extrema importância que para evitá-los o usuário deve ter um bom antivírus, além de sempre manter atualizado o sistema operacional, os navegadores e os *softwares*.

Atualmente, mais precisamente na data do dia 29 de Abril de 2021, o Tribunal de Justiça do Rio Grande do Sul⁴, informou publicamente que sofreu um ataque cibernético, no qual os criminosos invadiram o sistema e corromperam diversos arquivos, e que segundo alguns sites da web os criminosos requisitaram R\$ 5.000.000,00 (cinco milhões de reais) em troca de liberar totalmente o acesso aos sistemas invadidos, e não vazarem os dados que os mesmos corromperam. O desembargador Antonio Vinicius Amaro da Silveira⁵, do Conselho de Comunicação do TJ, afirmou em entrevista que a invasão se trata de um ataque de Ransomware.

2.2.4 Estelionato

O *scamming* pode ser configurado também como estelionato, uma vez que, o criminoso utiliza-se na internet para obter vantagens e realizar golpes contra um usuário. Este criminoso almeja primeiramente a confiança do usuário, para obter dados pessoais e delicados do mesmo, com o intuito de desviar seus recursos, ou fazer com que o mesmo confie nele a ponto de transferir-lhe determinado valor em espécie ou crédito.

Esses golpes são bastante praticados no mundo virtual, sendo que a qualquer momento podemos ser vítima de tal crime; sendo que, um dos exemplos praticados

⁴ Disponível em <https://g1.globo.com/rs/rio-grande-do-sul/noticia/2021/04/29/tj-rs-diz-que-sistema-de-informatica-do-tribunal-foi-alvo-de-ataque-hacker-e-muito-grave.ghtml> Acesso em 11 de maio de 2021.

⁵ Disponível em <https://g1.globo.com/rs/rio-grande-do-sul/noticia/2021/04/29/tj-rs-diz-que-sistema-de-informatica-do-tribunal-foi-alvo-de-ataque-hacker-e-muito-grave.ghtml> Acesso em 11 de maio de 2021.

em nosso dia-dia, que podem estar acontecendo em nossa frente, são a venda de veículos no meio virtual e os sites de relacionamentos.

2.3 COMO AGIR AO SER VÍTIMA DO CRIME VIRTUAL

Cada tipo de crime virtual tem uma maneira de agir ao ser uma vítima, mas basicamente todas compreendem coletar o máximo de evidências possíveis relacionadas ao crime praticado em questão, e se dirigir imediatamente a uma delegacia especializada, para que seja registrado um boletim de ocorrência caso não haja, procure a delegacia mais próxima.

Ressalta-se que, caso o crime se trate de divulgação de imagens íntimas ou ofensivas no Google, a vítima deve enviar um pedido de remoção de pesquisas para o Google e aguardar para que estas sejam retiradas do ar.

2.4 DOS CRIMES CIBERNÉTICOS NO ORDENAMENTO JURÍDICO

2.4.1 Lei 12.737/2012 - Lei Carolina Dieckman

Qual a relevância da atriz sobre a lei promulgada no código penal brasileiro? Inicialmente atriz Carolina Dieckman foi vítima de crime cibernético em 2011, onde teve seu computador invadido por hackers e foram divulgadas suas fotos íntimas, a partir desse fato e a grande repercussão que teve, foi elaborada a presente lei que puniria atos cometidos pela prática de invasão de dispositivo tipificando tal conduta sob lei 12.737/2012 sendo acrescida no decreto-lei nº 2848 com os artigos 154-A, 154-B do Código Penal Brasileiro que diz “Invadir dispositivo informático alheio, conectado ou não à rede de computadores,” pena de 3 meses á 1 ano, pena e multa podendo ocorrer aumento de pena.

O fato ocorrido com a atriz de fato trouxe um grande dano moral e psicológico a ela, mas por outro lado trouxe ao legislativo o quão foi necessário atualizar as normas penais referente a crimes cibernéticos devido ao grande avanço da tecnologia, sendo que muitas pessoas foram vítimas desse mesmo crime até o presente caso da atriz vir á tona.

3 DAS CONDUTAS FRAUDULENTAS VIRTUAIS NÃO TIPIFICADAS

Como visto no decorrer deste presente artigo, os crimes virtuais vêm ganhando cada vez mais espaço em nosso dia a dia, por diversos fatores, entre eles o crescente número de usuários de internet devido ao atual cenário mundial pela qual estamos passando, o surto da COVID 19. Diante deste momento caótico, onde a população passa grande parte do dia conectada à internet, os criminosos aproveitam para praticar os crimes virtuais. Segundo o deputado Vinicius Carvalho⁶, “um em cada cinco brasileiros foi alvo do golpe de *phishing* em 2020. Este golpe ocorre quando um criminoso cria página falsa para simular um *site* verdadeiro para roubar dados e desviar recursos da vítima”, justificou.

“De acordo com o Centro de Denúncias de Crimes Cibernéticos do FBI, durante a pandemia que ainda assola todo o planeta, houve um aumento de 300% de ataques cibernéticos nas principais economias”⁷, acrescentou o parlamentar.

No ano de 2014, foi criada a Lei nº 12.965/14, considerada o Marco Civil da Internet, com o intuito de preencher o nosso ordenamento jurídico no tocante aos crimes virtuais, sendo que esta Lei contribuiu bastante na penalização dos crimes cibernéticos, porém não foi suficiente; a escassez das tipificações penais relacionadas aos crimes citados anteriormente e pelo fato dos artigos criados na referida lei não abarcar por completo as atividades praticadas nos crimes virtuais, gera um grande problema a nossa legislação, uma vez que, quem pratica tais crimes ficam impunes devido a falta de tipificação, e devido ao fato de que as lacunas não preenchidas ficam a mercê de outras legislações.

A criação da Lei nº 12.737/2012, Lei Carolina Dieckmann, também representou um grande avanço em nosso ordenamento jurídico com relação aos crimes cibernéticos, uma vez que, incrementou o Código Penal com uma nova tipificação penal, vejamos:

⁶ Disponível em

https://www.moneytimes.com.br/camara-aprova-projeto-que-endurece-penas-em-crimes-ciberneticos/amp/?_twitter_impression=true, acesso em 29 de abril de 2021.

⁷ Disponível em

https://www.moneytimes.com.br/camara-aprova-projeto-que-endurece-penas-em-crimes-ciberneticos/amp/?_twitter_impression=true, acesso em 29 de abril de 2021.

o artigo 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.”

Antes desta inovação em nosso Código Penal, não havia nenhum dispositivo legal em nosso ordenamento jurídico que tipificasse o crime exposto acima, fazendo com que os criminosos ficassem impunes, porém com a entrada dessa nova tipificação penal, além de quem pratica o crime, aquele que comercializa, distribui ou repassa, incorrerá na mesma pena.

Além da alteração descrita anteriormente, a Lei nº 12.737/2012, também alterou o artigo 266 e 298 do Código Penal, incluindo no crime de interrupção de serviço, os serviços telemáticos ou de informação de utilidade pública; e nos crimes de falsificação de documentos foi incluído a falsificação de cartões de crédito/débito.

Como dito anteriormente, a referida Lei representou um grande avanço ao tipificar tais condutas, pois estas tipificações foram voltadas especificamente para os crimes virtuais, porém não são suficientes e não conseguem abranger todos os crimes ainda não tipificados.

Atualmente, na data do dia 15 de Abril de 2021 foi aprovada com alterações no Plenário a PL 4554/2020, que prevê alterações no Código Penal, Lei 2.848 de 1940, no quesito contra a prática de fraudes eletrônicas, modificando o artigo 155 (furto) do referido código, este é o Projeto de Lei aprovado, mais recente que envolve os crimes virtuais; As novas alterações prevê agravantes quanto a furtos praticados por meio eletrônico, passando a prevalecer a pena de quatro a oito anos de reclusão, em vez da pena anterior que era de um a quatro anos; tais penas ainda são previstas com aumento de penas se o crime for praticado contra idoso, aumentando de um terço ou dobro, e nos caso em que houver a utilização de servidor mantido fora do país a pena inicial será aumentada de um terço a dois terços. O projeto de lei que ainda segue em análise pela Câmara dos Deputados prevê penas mais rígidas e com aumento de pena para os crimes que resultam em prejuízo econômico para as vítimas, valendo ainda para os acusados que se beneficie de dados eletrônicos fornecidos pela vítima mediante ao erro ou a qual ela foi induzida, seja por qualquer meio de comunicação ou operador, tendo apenas que se caracterizar a

ação fraudulenta para tipificar o crime, tendo como objetivo de tentar diminuir o avanço dos cibercrimes pois, até o presente momento nosso ordenamento jurídico ainda contém leis em sentido “vago” com relação aos crimes virtuais, uma vez que, o Brasil não possui um marco legal atualizado com todos as tipificações de crimes virtuais existentes em nosso meio. Diante de tal situação, devido ao aumento gradativo da prática de crimes virtuais e devido a facilidade de propagação, o que faz com que o crime se torne mais ofensivo tanto à vítima quanto ao poder público, o poder judiciário é obrigado a agir de maneiras diversas. Portanto, um aspecto importante a se pensar, seria a criação de uma lei específica para combater e regular os crimes praticados em nosso ambiente virtual, pois tais crimes, por não estarem tipificados diretamente em nosso ordenamento jurídico tem sua pena estendida com relação às leis já existentes, uma vez que, em nosso ordenamento jurídico há várias leis esparsas que tratam do tema em questão.

Um exemplo seria o *scamming*, crime praticado no ambiente virtual que tem semelhanças ao estelionato, com isso a lei que rege o estelionato se estende ao crime virtual *scamming*, pois não há, atualmente, lei específica para tais crimes, com isso torna-se evidente a necessidade da criação de uma lei Específica para reger os crimes virtuais, pois a maioria dos crimes virtuais são tipificados com base no Código Penal vigente, código este que foi criado no ano de 1940, ficando evidente que este já se encontra ultrapassado ao se tratar dos novos crimes praticados, inclusive os crimes virtuais, que surgiram ao decorrer dos anos, sendo que as penas são relativamente “fracas” comparadas ao sofrimento da vítima.

É importante ressaltar que, devido a falta de uma lei específica acerca dos crimes cibernéticos, há uma certa dificuldade no combate aos crimes praticados no meio virtual, uma vez que, na maioria das vezes não a uma legislação aplicável para tal crime, e quando há, geralmente são falhas pois dão margens a dupla interpretação dificultando na aplicabilidade da lei, tendo como consequência a impunibilidade do criminoso.

4 CONCLUSÃO

Conforme foi demonstrado no presente artigo, o avanço da tecnologia vem aumentando ainda mais e consequentemente o número de vítimas de crimes

praticados sob o uso da internet também; durante a elaboração do artigo identificamos que as normas e políticas de prevenção contra esses crimes ainda continuam vulneráveis, onde na maioria das vezes a polícia só é acionada quando o fato já se consumou, na maior parte dos crimes denunciados os criminosos não são encontrados e não deixam rastros. Esse tipo de crime é uma ameaça silenciosa que gera muitos prejuízos, haja vista que, na maioria deles tem objetivo de roubar informações pessoais de extrema importância a qual trata-se de bens e valores ou da vida íntima de uma pessoa. Mesmo após entrar em vigor a Lei nº 12.737/2012 - Carolina Dieckman no âmbito do direito penal, os crimes cibernéticos continuam ocorrendo sem haver nenhuma redução, isso devido à dificuldade de achar os autores destes crimes e ainda pior, devido a lei apresentar lacunas no âmbito penal onde mostra o quanto a legislação brasileira deve se adequar e elaborar leis e políticas de combate aos crimes cibernéticos que, vem crescendo de maneira progressiva a chegar a ponto, de ser costume uma pessoa ser vítima desses crimes.

Por fim, salienta-se a importância da discussão ao artigo exposto devido à cristalina situação de exposição que vivemos frente aos novos crimes cibernéticos, e aos que já existem e estão se aperfeiçoando. A uma extrema urgência na criação de novas leis, para abrangerem completamente as práticas dos crimes virtuais, além de poder acompanhar a evolução tecnológica e tratar especificamente cada tipo de crime. Ressalta-se que, enquanto não chegarmos a tal feito, a melhor maneira de não ser vítima é se prevenir contra propostas, ofertas absurdas e não oferecer dados pessoais para ninguém, pois a cada dia os criminosos vêm se aperfeiçoando e encontrando novas ferramentas e novas maneiras de aplicar novos golpes.

5 REFERÊNCIAS

JESUS, Damásio de. MILAGRE, José Antonio. **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2016.

SYDOW, Spencer Toth. **Crimes Informáticos e suas vítimas**. São Paulo: Saraiva, 2º Ed. 2015.

SILVA, Ângelo Roberto Ilha da. **Crimes Cibernéticos**. São Paulo: Saraiva, 2º Ed. 2017.

WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Crimes Cibernéticos: ameaças e procedimentos de investigação**. São Paulo: Brasport, 2013.

CRESPINO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 15 de outubro de 2020.

SILVEIRA, Artur Barbosa da. Os crimes cibernéticos e a Lei nº 12.737/2012 Conteúdo Jurídico, Brasília-DF. Disponível em: <https://conteudojuridico.com.br/consulta/Artigos/43117/os-crimes-ciberneticos-e-a-lei-no-12-737-2012>. Acesso em: 26 out 2020.

VALENTE, Jonas. O Brasil tem 134 milhões de usuários de internet, aponta pesquisa, Brasília-DF: 26 maio 2020. <https://agenciabrasil.ebc.com.br/geral/noticia/2020-05/brasil-tem-134-milhoes-de-usuarios-de-internet-aponta-pesquisa>. Acesso em: 16 de maio de 2020.

<https://chcadvocacia.adv.br/blog/saiba-como-agir-caso-seja-vitima-de-um-crime-virtual/> Acesso em: 07 de abril de 2021.

https://www.google.com/url?q=https://www.moneytimes.com.br/camara-aprova-projeto-que-endurece-penas-em-crimes-ciberneticos/amp/?__twitter_impression%3Dtrue&sa=D&source=editors&ust=1619560650779000&usg=AOvVaw2lC6SkjysvnQuP7FEk67OH. Acesso em: 27 de abril de 2021.

<https://www.telesintese.com.br/tj-rs-recupera-sei-apos-ataque-cibernetico-ransomware/>. Acesso em: 11 de maio de 2021.

<https://g1.globo.com/rs/rio-grande-do-sul/noticia/2021/04/29/tj-rs-diz-que-sistema-de-informatica-do-tribunal-foi-alvo-de-ataque-hacker-e-muito-grave.ghtml>. Acesso em: 11 de maio de 2021.

