UNIVERSIDADE TIRADENTES – UNIT

CURSO DE GRADUAÇÃO EM DIREITO

TRABALHO DE CONCLUSÃO DE CURSO

CRIMES CIBERNÉTICOS: A evolução da criminalidade na internet e a deficiência das leis específicas no Brasil

Fabrício Tavares de Jesus [1]
Karina Ferreira Soares de Albuquerque [2]

Aracaju
2020

[1] Acadêmico em Direito, UNIT. Email: fabricio_gaviao@hotmail.com

[2] Mestre em direito econômico e socioambiental pela PUC Paraná. Especialista em direito público pela UNIT. Especialista em direito processual pela Universidade Federal de Santa Catarina. Formada em direito pela Universidade Federal de Sergipe. Professora adjunta da Universidade Tiradentes (UNIT). Advogada. Email: karinaalbuquerque@ig.com.br

FABRICIO TAVARES DE JESUS
Karina Ferreira Soares de Albuquerque

CRIMES CIBERNÉTICOS: A EVOLUÇÃO DA CRIMINALIDADE NA INTERNET E A DEFICIÊNCIA DAS LEIS ESPECÍFICAS NO BRASIL

Trabalho de conclusão de curso – Artigo – apresentado ao curso superior de Direito da Universidade Tiradentes – UNIT, como requisito parcial para obtenção de grau de bacharel em Direito.

Orientadora: Profº. Karina Ferreira Soares de Albuquerque

Aprovado em: _____/_____/_____

Banca Examinadora:

_____
Karina Ferreira Soares de Albuquerque
Universidade Tiradentes

_____
Professor Examinador
Universidade Tiradentes

_____
Professor Examinador
Universidade Tiradentes

Aracaju

2020

RESUMO

O presente trabalho tem por objetivo analisar a evolução da tecnologia e como ela afeta a vida em sociedade, principalmente no âmbito da criminalidade, de forma que surgem os crimes virtuais, tendo como elemento discutido a deficiência de leis específicas, bem como as repercussões dos ataques à honra e à imagem de um indivíduo através da internet. Dessa forma, se ver a fragilidade do ordenamento jurídico quanto ao posicionamento tanto da jurisprudência quanto das leis para tipificarem condutas criminosas em relação a tais crimes. Com essa evidência, será exposto e assim discutido a lei 12.737/2012, conhecida como “Carolina Dieckmann”, a lei 12.965/2014, intitulada de “Marco Civil”, e a Nova lei da Proteção de Dados, enfatizando a importância das mesmas, e a necessidade de penas mais severas. Contudo, serão apresentadas possíveis soluções à indagação central do presente artigo, a qual se refere aos possíveis meios de coibir o exercício arbitrário, e assim, contribuir com discussões e reflexões em no que alude a temática apresentada, desta forma buscando soluções ao tema apresentado.

Palavras-chave: Crime Cibernéticos; Crimes Virtuais, internet.

ABSTRACT

The present work aims to analyze the evolution of technology and how it affects life in society, especially in the scope of criminality, in a way that cyber crimes arise, having as an element discussed the deficiency of specific laws, as well as the repercussions of attacks to the honor and image of an individual through the internet. Thus, one can see the fragility of the legal system regarding the positioning of both jurisprudence and laws to typify criminal conduct in relation to such crimes. With this evidence, Law 12,737 / 2012, known as “Carolina Dieckmann”, Law 12,965 / 2014, entitled “Marco Civil”, and the New Data Protection Law will be exposed and discussed, emphasizing their importance, and the need for more severe penalties. However, possible solutions will be presented to the central question of the present article, which refers to the possible means of restraining arbitrary exercise, and thus, contributing to discussions and reflections in what the theme presented is all about, thus seeking solutions to the theme presented.

Keywords: Cyber Crime; Virtual Crimes, internet.

1. INTRODUÇÃO

O presente artigo visa demonstrar os aspectos gerais dos crimes virtuais, disponibilizando ao leitor um maior entendimento a cerca desse assunto e também a legislação existente para tais conflitos, além de tornar públicos os impactos dessa nova criminalidade que surge na sociedade.

Intitulado de “CRIMES CIBERNÉTICOS: A evolução da criminalidade na internet e a deficiência das leis específicas no Brasil” consiste na análise das previsões penais, e diretrizes expressas na Lei nº 12.737/2012, conhecida como Lei “Carolina Dieckmann”, a Lei nº 12.965/2014 intitulada de “Marco Civil”, e a Nova Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018, a qual serão estudadas, minuciosamente, enfatizando a presente temática, e os seus principais elementos constitutivos.

Várias mudanças foram ocorrendo na sociedade no aspecto tecnológico e a mesma medida, o número de vítimas de crimes virtuais só aumenta no mundo todo, de modo que, o alcance da internet tem tomado proporções imensas, tornando assim as medidas de punições e conscientização ainda mais necessárias e urgentes.

Percebemos assim, que há uma grande dificuldade para o ordenamento jurídico resolver tais conflitos devido à vasta proporção que a internet tomou pelo mundo ocasionando muitas mudanças, as quais acabaram não sendo acompanhadas devidamente pela legislação brasileira.

Está pesquisa tem como propósito contribuir para aprimorar os saberes no campo do âmbito jurídico, especialmente ao que pertence a informação relevante e precisa a população a respeito do tema abordado bem como, enfatizar a legislação responsável ao combate a esse crime.

Na busca de encontrar algumas soluções, este artigo aponta alguns problemas basilares, no que tange aos ataques virtuais de criminosos inescrupulosos que ainda persistem em cometer tais atos ilícitos, diante aos crimes cibernéticos, sendo especificada a constituição do Poder Judiciário, que no decorrer do artigo serão analisados.

A principal problemática do estudo se emerge diante das definições de crimes cibernéticos e de possíveis maneiras eficientes no combate a essa natureza de

infração, notoriamente não tutelada como deveria pelo ordenamento jurídico penal brasileiro, acarretando em altos índices de impunidade.

Nesse mesmo diapasão, o mesmo visa contribuir e ajudar no que concerne o tema, e também transparecer o fato de a legislação penal brasileira necessitar urgentemente de modificações no que está relacionado ao direito informático, e, contudo, realizar uma análise sobre os crimes cibernéticos e apontar os principais entraves à identificação e punição dos criminosos.

No que concerne à metodologia empregada, trata-se de uma pesquisa teórica; bibliográfica, tendo em vista que é estrutura a partir de material já publicado tais como livros, artigos, bem como materiais disponibilizados em sites informativos a fim de se tomar nota das divergentes correntes de opinião sobre o assunto, que procurou lapidar o conhecimento científico que já é consolidado sobre o tema; qualitativa, já que as informações levantadas são de natureza descritiva, e de método indutivo, ou seja, na análise de algo específico partindo de uma ideia verdadeira com o intuito de sugerir a verdade.

2. O USO DA INTERNET

Atualmente, a internet pode ser compreendida como o mais abrangente sistema de comunicação global, dados os amplos recursos que oferece a fim de facilitar a vida de seus usuários. No ciberespaço, é possível realizar buscas sobre os mais variados tipos de assuntos, entretenimento, estudo, além de facilitar e otimizar o tempo das relações comerciais. O problema se dá quando usuários mal intencionados a utilizam de maneira lesiva, configurando a prática dos chamados crimes cibernéticos.

Nesse sentido, segundo Augusto Rossini:

> O conceito de ‘delito informático’ poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade. (ROSSINI, 2004)

O surgimento da internet levou a humanidade a se sentir confortável diante da possibilidade de se comunicar sem fronteiras, e, nos dias de hoje, se encontra ligada às necessidades básicas de empresas, casas, escolas.

É de se notar, também, a importância que os sistemas informáticos possuem no atual momento social, ressaltando que a maioria das pessoas, físicas ou jurídicas, depende do seu dispositivo informatizado, que variam de um simples pendrive ou celular, até um computador com banco de dados sigilosos de uma empresa (BRITO, 2013).

A internet deixou as pessoas se sentirem confortáveis diante da possibilidade de serem sem fronteiras, sem muito esforço, e está cada vez mais presente na rotina, influenciando a vida nos mais variados aspectos.

No entendimento de José Manuel Moran (2003):

> “Uma das características mais interessantes da Internet é a possibilidade de descobrir lugares inesperados, de encontrar materiais valiosos, endereços curiosos, programas úteis, pessoas divertidas, informações relevantes. São tantas as conexões possíveis, que a viagem vale por si mesma. Viajar na rede precisa de intuição acurada, de estarmos atentos para fazer tentativas no escuro, para acertar e errar. A pesquisa nos leva a garimpar joias entre um monte de banalidades, a descobrir pedras preciosas escondidas no meio de inúmeros sites publicitários”.

No ciberespaço, é possível realizar buscas sobre os mais variados tipos de assuntos, entretenimento, estudo, além de facilitar e otimizar o tempo das relações comerciais. O problema se dá quando usuários mal intencionados a utilizam de maneira lesiva, configurando a prática dos chamados crimes cibernéticos.

Conforme Valzacchi (2003, p. 129-177), a utilização da internet em aulas pode chegar a ser proveitoso, para ele:

> “Aprender a aprender e a desenvolver a criatividade são habilidades críticas na sociedade onde o conhecimento se renova com

> velocidades inesperadas. Através de diálogos entre os pares, entre alunos e professores ou em comunidades de aprendizes".

À vista disso, é fundamental meios mais competentes para garantir a proteção e segurança dos indivíduos, que devem gozar de sua vida intima e privada, tal como assegura a Constituição Federal de 1988 em seu Artº 5º, V:

> "5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".

Neste sentido, enfatiza-se a importância de uma legislação firme e coesa a fim de proteger e assegurar a acessibilidade desse material somente pelos seus proprietários, punindo com vigor quaisquer invasores.

3. LEI CAROLINA DIECKMANN

No Código Penal brasileiro, anteriormente não existia artigos específicos que tratassem dos crimes que se realizam no meio digital. Somente em 30 de novembro de 2012, com a edição da Lei Nº 12.737, que o Código Penal foi modificado, sendo acrescentados os artigos 154-A, 154-B, 266 e 298 para punição dos crimes cometidos na internet.

Essa lei de 2012 ficou conhecida por todos como a "Lei Carolina Dieckmann" (atriz), que foi sancionada pela então Presidente da República, Dilma Rousseff, depois de algumas fotos íntimas da atriz ter sido vazado por uma invasão em seu computador pessoal. A mesma qualifica atos como adentrar computadores (hacking), roubar senhas, violar dados de usuários e divulgar informações privadas.

A então lei proposta pelo deputado Paulo Teixeira (PT-SP), recebeu o nome "extraoficial" porque, no trâmite do projeto na Câmara de Deputados, Carolina Dieckmann teve fotos divulgadas sem autorização. A nova lei identifica como crime

justamente casos como o da atriz, em que há a invasão de computadores, tablets ou smartphones, conectados ou não à internet, com o objetivo de desfigurar ou destruir dados ou informações.

A lei modificou o Código Penal, e assim foram acrescidos os artigos 154-A e 154-B, além de alterar os artigos já existentes, 266 e 298, conforme se verifica:

> "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 à terceiro, a qualquer título, dos dados ou informações obtidas.
> § 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.
> Art. 154-B – Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime e 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.

Nesse sentido, vejamos a titulo exemplificativo, decisões no sentido de que resultou na prática de crime, uma vez que a Lei nº 12.737/12, também conhecida como lei Carolina Dieckmann, acrescentou ao código Penal o art. 154-A. Vejamos:

> **RECURSO ORDINÁRIO EM HABEAS CORPUS. PIRATARIA DE SOFTWARES E CONCORRÊNCIA DESLEAL. INTERVENÇÃO DOS INTERESSADOS (FUTUROS QUERELANTES) NO REMÉDIO CONSTITUCIONAL. POSSIBILIDADE. MEDIDA CAUTELAR DE BUSCA, APREENSÃO E VISTORIA, VISANDO AO PREPARO DE FUTURA E EVENTUAL AÇÃO PENAL PRIVADA. CABIMENTO DO WRIT. NULIDADE. PROVA ILÍCITA. AFRONTA AO DISPOSTO NO ART. 154-A (ACRESCIDO AO CP PELA LEI N. 12.737/2012). EXAME APROFUNDADO DOS ELEMENTOS QUE INSTRUÍRAM O PEDIDO. INVIABILIDADE.** 1. Embora a regra seja a impossibilidade de intervenção de terceiros em sede de habeas corpus, o certo é que tal entendimento é flexibilizado quando se trata de ação penal privada, exatamente como na espécie, permitindo-se, por conseguinte, que o querelante participe do julgamento. Precedentes do STJ e do STF (RHC n. 41.527/RJ, Ministro Jorge Mussi, Quinta Turma, DJe 11/3/2015). 2. Embora o habeas corpus seja remédio constitucional voltado à garantia do direito de locomoção, esta Corte tem admitido o seu cabimento em feitos voltados à discussões sobre a legalidade de medidas assecuratórias, em razão da possibilidade da medida, eventualmente, motivar restrição ao direito ambulatorial do paciente (REsp n. 865.163/CE, Ministro Og Fernandes, Sexta Turma, DJe 1º/7/2011). 3. A questão referente à possibilidade do acesso a dados armazenados em um computador de uso pessoal e exclusivo, protegido por senha individual, sem autorização do seu usuário ou sem que haja decisão judicial autorizando-a, não foi efetivamente

> decidida pelo Tribunal local, pois o tema está atrelado ao mérito, o qual deve ser analisado e valorado pelo Juízo a quo (juízo natural), no momento adequado. As provas apresentadas no pedido de busca, apreensão e vistoria e seu devido valor não podem ser apreciados pela via do remédio constitucional, que restringe a ampla defesa e a dilação probatória, sendo inviável seu reexame neste momento. 4. No caso, não é manifesto o alegado constrangimento ilegal, porque a decisão que deferiu a medida não se baseou somente nos documentos obtidos, supostamente, de maneira ilícita. Outros meios de prova, tais como pareceres técnicos atestando a cópia e reprodução dos códigos de programação dos jogos de propriedade das empresas e prova testemunhal indicando a existência de esquema criminoso, fundamentaram o deferimento da medida. 5. Recurso ordinário em habeas corpus improvido. Agravo regimental prejudicado.
>
> (STJ - RHC: 66571 RJ 2015/0318540-9, Relator: Ministro SEBASTIÃO REIS JÚNIOR, Data de Julgamento: 16/06/2016, T6 - SEXTA TURMA, Data de Publicação: DJe 30/06/2016).

Para a caracterização do tipo não importa se o dispositivo informático, objeto material sobre o qual recai a ação criminosa, está conectado ou desconectado na internet. Ou seja, a invasão tanto pode ser através da rede mundial de computadores, quanto de forma direta, por meio de uma ação física sobre o dispositivo informático. Mais ainda, esta violação há de ser indevida com burla do sistema de segurança da informação do dispositivo que põe a salvo os dados ali armazenados de propriedade do dono do dispositivo.

Nesta esteira, é relevante para a prática do tipo que não haja autorização, seja expressa, seja tácita, do proprietário do dispositivo informático para acesso dos dados nele armazenados. Isso, considerando que terceiro pode violar o dispositivo com autorização do seu dono para fins de manutenção, por exemplo. Assim, a mera violação não é suficiente para caracterizar a perpetração do tipo.

> Art. 266 – Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento: Pena – detenção, de um a três anos, e multa. Parágrafo único – Aplicam-se as penas em dobro, se o crime for cometido por ocasião de calamidade pública. § 1° Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. § 2° Aplicam-se as penas em dobro se o crime e cometido por ocasião de calamidade pública.
>
> Art. 298 – Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro: Pena – reclusão, de um a cinco anos, e multa. Falsificação de cartão. Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito".

Frisa-se, porém, que essas alterações nos artigos 266 e 298, CP somente vigorarão após o período de "vacatio legis" legalmente estabelecido e não poderão retroagir a fatos antecedentes.

Ao perceber a possibilidade de invasão, o estado assumiu para si a forma de exercício do poder de punição que lhe incumbe, assegurando a privacidade dos usuários. As alterações do Código Penal são visíveis no sentido de responsabilizar o indivíduo que invadir, ou enganar as ferramentas de segurança, com o objetivo de violar a intimidade digital de outrem.

4. INVASÃO DE PRIVACIDADE E CRIME CONTRA HONRA

Um direito fundamental e próprio ao ser humano que se vale de pilar para a personalidade e a liberdade de pensamento do ser humano, é a privacidade, contudo, a mesma vem vivenciado inúmeros ataques no ambiente virtual. Mesmo a privacidade garantindo a liberdade, o montão desta vai de encontro com a segurança.

Por mais que a lei resguarde a descrição à intimidade e à privacidade, com o uso imoderado da internet, os próprios usuários vêm usando dessa regalia com a má utilização das redes sociais. A precisão de disseminar informações no mundo

virtual não se limita somente às opiniões e convicções do indivíduo, de caráter discriminatório ou não, mas também, dados pessoais, como telefone ou endereço.

Ponderando os crimes contra a honra do ponto de vista objetivo, o mesmo caracteriza-se por o sentimento do indivíduo em relação a sua própria dignidade. Há três espécies de crimes eventualmente praticados no meio virtual, sendo eles: Calúnia, Difamação e Injúria. Insultar a honra de alguém (calúnia artigo138), espalhar boatos eletrônicos sobre pessoas (difamação artigo 139), insultar pessoas considerando suas características ou utilizar apelidos grosseiros (injúria artigo 140).

Por mais que estas condutas estejam tipificadas no Código Penal vigente, nos artigos 138, 139 e 140, as penas são moderadas e quando ocorrem no mundo digital, seu reparo se torna bem mais complexo. Desta forma, ver-se crucial agravar as penas em uma lei específica, e esmiudar condutas quando tratar-se de crimes contra a dignidade cometidos na internet.

5. LEI MARCO CIVIL DA INTERNET

Em 23 de abril de 2014, foi sancionado no Brasil a lei Nº 12.965 conhecida como Marco Civil da Internet que estabelece princípios, direitos e garantias para o uso da internet no Brasil.

O Marco Civil da Internet, formou-se do conflito ao discutível PL 84/99, e teve grande participação popular. Durante sua concepção, foram executadas consultas públicas, a qual dividiram-se em duas fases: uma com ampla diversidade de opiniões, incluindo a sociedade civil e as mais variadas empresas, nacionais e internacionais, do ramo digital, e outra, também com participação popular, mas pleiteando cada dispositivo proposto na primeira fase.

Esta foi produzida com o intuito de preencher as lacunas de nosso sistema jurídico no tocante aos crimes virtuais. Inicialmente, trata dos fundamentos e conceitos, elencando os direitos dos usufruidores. Tipifica princípios, tais como liberdade, neutralidade e privacidade, além de determinar garantias, direitos e deveres no ambiente virtual. Um destaque se dá ao direito e garantia a inviolabilidade da intimidade e da vida privada.

Por mais que a Lei estabeleça sanções para a inobservância de algumas de suas normas, não prevê qualquer tipo de infrações cibernéticas propriamente ditas.

Desta forma, podemos dizer que o Brasil está carente de legislação pertinente, pois nesse aspecto, o conjunto de normas brasileiras não acompanha as necessidades sociais.

6. NOVA LEI GERAL DE PROTEÇÃO DE DADOS

A lei de proteção de dados (LGPD) é a lei nº 13.709, aprovada em agosto de 2018 e com vigência a partir de agosto de 2020. No Brasil, uma Medida Provisória adiava o início da vigência da LGPD para 2021, mas o Senado converteu, no dia 26 de agosto, a MP no Projeto de Lei de Conversão 34/2020 e excluiu o artigo que definia o adiamento.

De acordo com o art. 5º, XII, da constituição brasileira de 1988, a proteção de dados pessoais é um direito fundamental. O Marco Civil da Internet toca neste assunto no âmbito da Internet brasileira e estabelece que a proteção do dado pessoal é um direito do usuário, bem como o não fornecimento dos mesmos. No entanto, a lei aborda vagamente sobre o assunto.

A nova lei quer criar um cenário de segurança jurídica, com a padronização de normas e práticas, para promover a proteção, de forma igualitária e dentro do país e no mundo, aos dados pessoais de todo cidadão que esteja no Brasil. E, para que não haja confusão, a lei traz logo de cara o que são dados pessoais, define que há alguns desses dados sujeitos a cuidados ainda mais específicos, como os sensíveis e os sobre crianças e adolescentes, e que dados tratados tanto nos meios físicos como nos digitais estão sujeitos à regulação.

Outro elemento essencial da LGPD é o consentir. Ou seja, o consentimento do cidadão é a base para que dados pessoais possam ser tratados. Mas há algumas exceções a isso. É possível tratar dados sem consentimento se isso for indispensável para: cumprir uma obrigação legal; executar política pública prevista em lei; realizar estudos via órgão de pesquisa; executar contratos; defender direitos em processo; preservar a vida e a integridade física de uma pessoa; tutelar ações feitas por profissionais das áreas da saúde ou sanitária; prevenir fraudes contra o titular; proteger o crédito; ou atender a um interesse legítimo, que não fira direitos fundamentais do cidadão.

A LGPD ainda determina punição para infrações, de advertência a multa diária de até R$ 50 milhões, além de proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados.

Segundo o Instituto Brasileiro de Geografia e Estatística (IBGE), 70,5% dos domicílios estavam conectados à rede em 2017. Em 92,7% das residências, pelo menos um morador possuía telefone celular, enquanto o telefone fixo era encontrado em apenas 32,1% — um sinal de queda na privacidade.

Com o crescimento do acesso à internet via telefone celular, de 60,3% dos domicílios em 2016 para 69% em 2017, cresce também a utilização desse instrumento para compras, pagamentos e homologações, além de navegação pelas redes sociais. Logo, o consumidor fica mais exposto ao fornecer número de CPF, telefone, endereço e outros dados pessoais, que podem ser utilizados de forma inadequada. A LGPD garante ao titular dos dados a possibilidade de verificar as condições de segurança oferecidas por quem os coletou por meio da exigência de um relatório.

A LGPD lista um conjunto de sanções para o caso de violação das regras previstas, entre as quais destacam-se advertência, com possibilidade de medidas corretivas; multa de até 2% do faturamento com limite de até R$ 50 milhões; bloqueio ou eliminação dos dados pessoais relacionados à irregularidade, suspensão parcial do funcionamento do banco de dados e proibição parcial ou total da atividade de tratamento.

7. POSSÍVEIS SOLUÇÕES

Pode-se dizer que a grande maioria dos crimes virtuais já estão tipificados no ordenamento jurídico brasileiro, contudo, o grande problema é que geralmente os crimes virtuais não se limitam a tipificação já existente, sendo cada vez mais complexos, exigindo mais atenção do legislador para detalhar cada vez mais, através de legislações específicas as condutas praticadas, principalmente, facilitando a possibilidade de punir civil e penalmente o sujeito que as práticas.

Sandra Carla Castro Marques Martins leciona que:

> “Destarte, o mundo cibernético tem sido alvo da atuação crescente de criminosos, que encontram na internet um meio fácil de cometer

> crimes, muitas vezes, aproveitando-se do anonimato, o que é vedado pela Constituição Federal, e da falsa impressão de que são impunes, ou pela falta de legislação específica, ou pela dificuldade na investigação criminal em encontrar os autores. É importante ressaltar que os usuários facilitam muito a prática destes ilícitos, tornando-se presas fáceis, pois ao acessar informações bancárias utilizando dados sigilosos, bem como a exposição da imagem, sem os devidos cuidados, acabam por favorecer a criminalidade cibernética". (Martins, 2012, p.78)

No combate aos crimes cibernéticos o Ministério Público Federal apresenta o projeto para atuação do mesmo, sendo assim uma forma de chegar a esses criminosos, da seguinte forma:

Elaboração de Termos de cooperação para suprir as lacunas da lei; Criação de hotline (canal de denúncias) e banco de dados únicos para o recebimento das comunicações; Criação de delegacias especializadas com maior capacitação e estrutura; Criação de grupos especializados nas unidades das Procuradorias da República; Treinamento e capacitação dos setores periciais e criação de Núcleos Técnicos.

Um dos passos importantes para punir tais delitos é de imediato fazer a denúncia e ter em mãos os dados referentes ao crime. A pessoa lesada precisa armazenar tudo que possa ajudar na comprovação. Entre os dados, estão os e-mails, fotos da tela (prints), informações do infrator (endereço de e-mail que foi enviado para você, por exemplo), mensagens em rede sociais e tudo que venha a servir de prova.

Medidas de prevenções também são de extrema importância, desta forma é necessário investir em segurança de informação, para assim proteger dados, arquivos e informações que estão em dispositivo eletrônicos ou até mesmo em nuvem, instalar um antivírus confiável, fazer o uso de redes seguras, mais confiar ou cadastrar seus dados pessoais e bancários em sites não confiáveis e nem envie por e-mail. O criminoso só precisa ter acesso ao seu computador, uma rede, um software ou um hardware, sem se sequer está presente fisicamente no local. Essas são algumas providencias que se tomadas podem proteger a todos.

8. CONSIDERAÇÕES FINAIS

Com essa pesquisa, conclui-se que a sociedade digital está evoluindo muito rápido e o Direito deve acompanhar esta mudança, aprimorar-se, renovar seus institutos e criar novos capazes de continuar garantindo a segurança jurídica das relações sociais, sob pena de ficar obsoleto.

Com o crescimento constante da tecnologia e o crescente número de usuários virtuais, é de suma importância a constituição de uma lei que defina as condutas criminosas cometidas no mundo digital, com penas mais severas e condizentes aos resultados danosos que estes produzem.

Por conseguinte, reforça-se ainda além do mais a urgência em renovações jurídicas na legislação, no que se refere os crimes cibernéticos e proteção cibernética nacional. A falta de legislação competente se mostra um problema.

De forme crescente, o Brasil se coloca entre os 10 (dez) países que mais utilizam a internet, e mesmo assim não possui um ordenamento jurídico que abarque todas as condutas passíveis de punição, ou seja, os usuários brasileiros não estão nem perto de estarem devidamente protegidos. Nesse diapasão, os cibercriminosos se beneficiam da inevitabilidade do uso da internet no cotidiano dos brasileiros, além da falta de expertise que muitos internautas possuem em relação aos perigos da web.

É notória a deficiência das leis brasileiras em relação aos crimes cibernéticos, faz-se necessário criar uma lei que não mais permita que a internet seja usada de forma prejudicial a seus usuários, sendo que a mesma é a mais ágil forma de comunicação/interação virtual.

Portanto é preciso acreditar que é possível controlar os crimes cibernéticos, e criar leis mais rigorosas e dar aparato tecnológico e científico para que os investigadores no intuito de acabar com tais práticas delituosas.

O Código Penal Brasileiro, apesar de tipificar algumas condutas ocorridas no meio cibernético, institui penas um tanto quanto leves e insuficientes para combater reincidências e novas práticas. Assim, faz-se importante reforçar que devem ser elaboradas normas específicas para tratar de crimes ocorridos no ambiente virtual, visto como a ocorrência dessas condutas tem se tornado cada vez mais frequentes e os danos vivenciados pelas vítimas são bastante traumáticos, tanto de ordem

material quanto psicológica. Por conseguinte, a punição deve ser adequada e correspondente aos danos, a fim de realmente coibir a prática desses crimes

É imprescindível a criação de normas específicas que abarquem de uma forma mais eficaz tais crimes cometidos na internet, pois, por mais que o legislador tenha criado determinadas leis, como visto acima, atenta-se carência no que tange a efetividade da norma, haja vista que cada direito acaba onde outro começa.

Desta forma, conclui-se que a sensação de impunidade das pessoas referente aos crimes cibernéticos se dá pela falta de lei específica, e também pela dificuldade que a polícia e o judiciário encontram para localizar o infrator, identificar a autoria e a materialidade dos crimes e assim aplicar a devida sanção.

REFERÊNCIAS

ALMEIDA, J. et al. **Crimes Cibernéticos**. 2015, 22 fls. Curso de Direito Universidade Tiradentes – UNIT. Disponível em: https://periodicos.set.edu.br/index.php/cadernohumanas/article/viewFile/2013/1217> Acesso em: 12 de nov. 2020.

BRASIL. **Constituição da república federativa do Brasil de 1988**. Brasília: Palácio do Planalto. Disponível em: <https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 12 de nov. 2020

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Brasília, DF, 3 out 1941. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto--lei/del3689.htm>. Acesso em: 12 de nov. 2020.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Brasília. 2012.Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 12 de nov, 2020

PAESANI, Liliana Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil**. 1ª ed. São Paulo, Atlas: 2000.

PINHO, Rodrigo César Rebello. **Teoria geral da constituição e direitos fundamentais**. 12ª ed. São Paulo: Saraiva, 2012.

RITO, Auriney**. Análise da Lei 12.737/12 – "Lei Carolina Dieckmann"**. Acesso em: 12 de nov. 2020

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004. Acesso em: 12 de nov. 2020

SANTOMAURO, Beatriz. **Cyberbulling: a violência virtual**. Publicado em 2010. Disponível em <https://novaescola.org.br/conteudo/1530/cyberbullying-aviolencia-virtual>. Acesso em: 12 nov. 2020.

VALZACCHI, Jorge R. **Internet y educacion: aprendiendo y ensensando em los espacios virtuales**. 2.ed. Versão Digital, 2003. Disponível em: . Acesso em: 12 nov. 2020.