CENTRO UNIVERSITÁRIO ATENAS

LETÍCIA MOREIRA DOS SANTOS

CRIMES VIRTUAIS: o aspecto jurídico sobre crimes cibernéticos e as possibilidades de prevenção

Paracatu

2022

LETÍCIA MOREIRA DOS SANTOS

CRIMES VIRTUAIS: o aspecto jurídico sobre crimes cibernéticos e as possibilidades de prevenção

Monografia apresentada ao Curso de Direito do Centro Universitário Atenas, como requisito parcial para obtenção do título de Bacharel em Direito.

Área de Concentração: Ciências Jurídicas

Orientadora: Prof.ª Msc. Flávia Christiane Cruvinel Oliveira.

Paracatu

2022

LETÍCIA MOREIRA DOS SANTOS

CRIMES VIRTUAIS: o aspecto jurídico sobre crimes cibernéticos e as possibilidades de prevenção

Monografia apresentada ao Curso de Direito do Centro Universitário Atenas, como requisito parcial para obtenção do título de Bacharel em Direito.

Área de Concentração: Ciências Jurídicas

Orientadora: Prof.ª Msc. Flávia Christiane Cruvinel Oliveira.

Banca Examinadora:

Paracatu – MG, ___ de _____ de _____.

_____
Prof.ª Msc. Flávia Christiane Cruvinel Oliveira.
Centro Universitário Atenas

_____
Profª. Msc. Amanda Cristina de Souza Almeida
Centro Universitário Atenas

_____
Prof. Msc. Altair Gomes Caixeta
Centro Universitário Atenas

RESUMO

A comunicação no mundo sofreu grandes modificações ao longo do tempo, sobretudo com o advento da internet e dos meios de comunicação tecnológicos, elevando a rapidez na troca de informações entre as pessoas, estando elas próximas ou distantes, e com isso, também, evoluíram as práticas criminosas, que antes eram realizadas apenas de forma física, passando, para também, para a forma virtual. O presente trabalho, portanto, investiga se o regramento legal brasileiro atual é suficientemente eficiente para a coerção de crimes cibernéticos, e realizar alguns apontamentos sobre possíveis melhorias no arcabouço legal afeto ao tema, a fim de que se possa obter ações mais contundentes contra este tipo de crime. Espera-se concluir que o país possa avançar, rumo ao atendimento das necessidades das pessoas no sentido da proteção de dados e patrimônio, trabalho pelo qual o legislador pátrio deve primar a fim de que seja possível utilizar-se dos meios digitais com segurança, praticidade e sossego.

PALAVRAS CHAVE: Comunicação. Crime. Cibernético. Legislação. Virtual. Segurança.

ABSTRACT

Communication in the world has undergone major changes over time, especially with the advent of the internet and technological means of communication, increasing the speed in the exchange of information between people, whether they are close or distant, and with that, too, the criminal practices, which were previously carried out only in a physical form, now also taking on a virtual form. The present work, therefore, investigates if the current Brazilian legal regulation is efficient enough for the coercion of cyber crimes, and makes some notes on possible improvements in the legal framework related to the subject, in order to obtain more forceful actions against this type. of crime. It is expected to conclude that the country can move forward, towards meeting the needs of people in the sense of protecting data and assets, a work for which the national legislator must excel so that it is possible to use digital media with safety, practicality and quiet.

KEYWORDS: *Communication. Crime. cybernetic. Legislation. Virtual. Safety.*

SUMÁRIO

1 INTRODUÇÃO

A comunicação mundial mudou drasticamente desde o advento da internet e dos meios tecnológicos, há uma grande rapidez na troca de dados entre pessoas que estão próximas ou muito distantes, o que não havia há cerca de duas décadas atrás onde a comunicação era mais lenta, feita por meio de cartas ou através de e-mails repassados através de um sistema de internet ainda iniciático e que não era tão democrático quanto é hoje.

Os computadores evoluíram muito nas últimas décadas, o que antes eram equipamentos gigantes que preenchiam o ambiente de uma sala de estar, hoje são portáteis e podem ser levados para qualquer lugar por qualquer pessoa, conectando-se à rede mundial de comunicações, a internet, estabelecendo uma conexão completa graças à rede sem fio.

Com o avanço das tecnologias citadas nos dois parágrafos anteriores, também surgiram os crimes cibernéticos que podem se classificar em algumas categorias como sendo invasão cibernética, fraude, roubo de identidade, pirataria, pornografia cibernética e ciber-violência. Infelizmente, na maioria dos países não é possível estimar a quantidade de crimes virtuais que acontecem, pois apesar da realidade, ainda não existe uma legislação mais dura aplicada ao tema. (BORTOT, 2017)

No Brasil a primeira lei que trata dos crimes virtuais foi promulgada em 2012 e se preocupou apenas em observar o aspecto físico dos crimes virtuais, o seja, é necessário que haja a violação de um direito da vítima como a invasão de um dispositivo de informática, a falsificação de documento particular, falsificação de cartão e/ou interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública. (BRASIL, 2012)

Apesar de recentemente o Brasil ter sido convidado a participar da Convenção do Conselho da Europa contra a Criminalidade Cibernética, que tem o objetivo de reforçar a proteção de dados e da dignidade da pessoa humana, ainda existe uma certa leniência com relação aos crimes virtuais. (BRASIL, 2020)

Pretende-se, portanto, investigar se a legislação brasileira atual tem sido suficiente para a apuração, condenação e coação de crimes cibernéticos.

Apontando quais seriam as possíveis melhorias a serem feitas no regramento legal brasileiro, que resultariam em ações mais contundentes contra este tipo de crime.

Alves (2020, p. 27) auxilia-nos dizendo que os crimes cibernéticos são um contraponto moderno ao crime antigo, pois, antes da era da tecnologia os criminosos assaltavam as casas, usando a comunicação verbal para garantir o sucesso de seu intento, com o advento da internet, os criminosos usam a internet e comunicação online para cometer seus crimes.

1.1 PROBLEMA DA PESQUISA

A estrutura legal e os mecanismos de prevenção adotados no Brasil tem sido suficiente para o enfrentamento, punição e prevenção dos crimes cibernéticos cometidos?

1.2 HIPÓTESE DE PESQUISA

A legislação brasileira ainda é muito frágil com relação ao combate dos crimes cibernéticos trazidos pela obscuridade da globalização, sendo um dos efeitos nocivos da diminuição das distâncias entre as pessoas e a diminuição do tempo na transmissão de imagens, troca de dados e do comércio virtual.

É necessário, portanto, que se faça um competente estudo sobre a temática, a fim de que seja possível criar um arcabouço legal capaz de diminuir a ação criminosa buscando traçar um conceito do crime cibernético por meio do qual se possa promover uma atualização da legislação atual, visando melhorar o controle deste tipo de prática delituosa transformando a internet num campo mais seguro onde se possam realizar atividades cotidianas sem o receio que atualmente constrange a população brasileira.

1.3 OBJETIVOS

1.3.1 OBJETIVO GERAL

Investigar se a legislação brasileira atual tem sido eficiente na prevenção, combate e punição dos crimes virtuais cometidos no país.

1.3.2 OBJETIVOS ESPECÍFICOS

a) Verificar na doutrina jurídica o conceito de crime virtual;
b) Observar a legislação vigente atual para se saber se há um sistema de proteção de dados capaz de dar segurança aos consumidores da internet;
c) Verificar se a estrutura legal e os mecanismos de prevenção que são adotados no Brasil tem sido suficiente para o enfrentamento, punição e prevenção contra crimes cibernéticos;

1.4 JUSTIFICATIVA

Os crimes cibernéticos representam um dos maiores problemas jurídicos e sociais da atualidade, eis que os crimes são recorrentes, atingem a todos os tipos de classes sociais e o Brasil ainda não possui legislação específica que os puna em sua totalidade, sendo apenas uma lei que rege crimes que atingem diretamente algo físico, como a clonagem de um cartão ou a invasão de um computador, por exemplo.

Neste sentido, este estudo justifica-se na necessidade social de se debater amplamente a necessidade de haver legislação que puna e coíba crimes cibernéticos amplamente, eis que, por enquanto, tais crimes ainda são punidos graças à jurisprudência e a interpretação dos juízes.

Este estudo será de grande valia tanto para o debate acadêmico, como também servirá de referência para a construção de um sistema legal que preveja a conceituação de crimes cibernéticos, como também a devida previsão punitiva dos mesmos, que é do que o sistema penal brasileiro ainda carece.

Tais crimes são um problema social grave, ofendem tanto o patrimônio como também a honra das pessoas e a dignidade da pessoa humana, haja vista que não são cometidos apenas com o sentido de lesar as riquezas das pessoas, mas também com o intento de denegrir a imagem de outrem com calúnia, difamação e outras modalidades criminosas que afetam diametralmente a honra das pessoas.

1.5 METODOLOGIA DO ESTUDO

A pesquisa foi inicialmente bibliográfica, buscando em livros, artigos, periódicos, na legislação brasileira e publicações de revistas de cunho jurídico, buscando informações que sejam o suficiente para embasar a teoria proposta na presente pesquisa. Gil (2018) preleciona que a pesquisa bibliográfica é desenvolvida com base em material que já foi elaborado, e que é constituído principalmente por livros e artigos científicos.

Consideramos também a pesquisa explicativa que segundo os dizeres de Gil (2018) tem como preocupação central identificar os fatores que são determinantes para que determinados fatos ocorram. Trilha-se também por este caminho com vistas a conhecer mais profundamente a realidade do tema proposto, encaminhando-se para a razão o porquê de ainda não se haver uma legislação que puna com rigidez os crimes praticados no meio virtual.

Opta-se ainda pelo método dedutivo que se trata de um processo de análise de informação que propicia uma conclusão, de forma que os pesquisadores se valem da dedução para encontrar um resultado final que satisfaça o seu intento. Quis-se com esta opção, permitir que a pesquisa tenha um ponto onde o pesquisador possa também sugerir e demonstrar a partir da observação realizada com a pesquisa, possíveis ações que possibilitem melhora no tema querido. (MENEZES, 2020)

1.6 ESTRUTURA DO TRABALHO

O segundo capítulo analisa o conceito existente de crimes cibernéticos, como também as suas formas de atuação.

No terceiro capítulo busca-se compreender como a legislação brasileira a respeito de crimes virtuais tem impactado este tipo de ação, e qual tem sido a movimentação dos legisladores a este respeito.

No quarto capítulo procura-se responder à pergunta problema no sentido de se observar se a legislação existente no Brasil e já em aplicação tem sido suficiente para coibir e punir os crimes virtuais em território nacional.

O quinto capítulo dedica-se a conclusão deste trabalho de conclusão de curso, e, adiante, passam-se as referências bibliográficas utilizadas para a construção deste.

2 O CONCEITO DE CRIME CIBERNÉTICO

Para que se inicie a discussão é necessário compreender o que é crime, e para tanto, faz-se necessário recorrer à Lei de Introdução ao Código Penal Brasileiro, que em seu artigo 1° define crime como a infração penal que a lei comina pena de reclusão ou de detenção, isolada, alternativa ou cumulativamente com pena de multa. Também se considera crime a contravenção ou infração penal a que a lei comina, isoladamente a pena de prisão simples ou de multa, ou as duas, de maneira alternativa ou cumulativa.

Nucci (2015) define crime como toda conduta típica, antijurídica e culpável. É dizer que crime é tudo aquilo que contraria ao que está disposto na lei e no ordenamento jurídico de um país. De maneira que os crimes virtuais, ou cibernéticos, são atividades ilegais realizadas valendo-se da tecnologia, com o objetivo de acessar ou comprometer sistemas computacionais.

Bortot (2017), ensina que crimes cibernéticos são condutas ilegais que são praticadas por criminosos a partir de um equipamento eletrônico, que pode ser um computador, uma rede de computadores ou celulares. Ações estas que incluem a disseminação de vírus, e que visem derrubar a infraestrutura de rede ou sites, ou ainda, que queiram dar espaço para a prática de condutas criminosas.

O Código Penal Brasileiro foi criado em 1940, quando ainda não havia a influência do advento da internet, que se deu em média trinta anos depois, e evoluiu, no Brasil particularmente, a partir da década de 90. Não havia, portanto, nenhuma lei que tipificasse ou previsse punição para os crimes virtuais. Até que em 2012, a Lei n 12.737 acrescentou os arts. 154-A e 154-B ao Código Penal, trazendo a forma pela qual os crimes virtuais são cometidos e quais são as penas aplicadas aos mesmos (ALVES, 2020).

Os artigos citados tem a seguinte redação:

> Art. 154-A Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
>
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
>
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
>
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações 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 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. (BRASIL, 2012)

Em 2014, foi criado o marco civil da internet que trouxe as conceituações do mundo virtual, suas formas legais de uso e estabeleceu as garantias e direitos à privacidade cibernética, que são as condições para o pleno exercício de acesso ao mundo virtual (ALVES, 2020).

Contudo, isto ainda não basta para que crimes que atingem a dignidade da pessoa humana e causam danos patrimoniais às pessoas todos os anos sejam coibidos de maneira exemplar e tornem a não ocorrer. Há a necessidade de se debruçar sobre as possibilidades legislativas, buscando a formação de um arcabouço legal que seja capaz de movimentar o setor de informação, bem como promover uma ampla e irrestrita tipificação dos crimes, o que facilitará as condenações e persecuções penais.

Segundo (2016) ensina que a partir de um conceito analítico, crime cibernético é toda espécie de “ação típica, antijurídica e culpável, cometida contra ou pela utilização do processamento analítico de dados ou transmissão”.

É importante destacar a partir desta conceituação que os crimes que são cometidos no ambiente virtual, ou contra dados e sistemas de funcionamento de uma máquina informatizada, são consequência direta da evolução dos equipamentos de comunicação e da internet. (DA SILVA, 2014)

A maior parte dos autores jurídicos brasileiros ainda não construiu um conceito estabelecido do que é o crime cibernético, e ainda há uma certa confusão a respeito de quem seriam as vítimas dos crimes cibernéticos, como por exemplo, se acreditar que o crime seja contra a máquina, que não possui personalidade jurídica.

Para tanto, os crimes cibernéticos podem ser divididos em duas vertentes, como sendo os crimes cibernéticos puros e os crimes cibernéticos impuros.

Carneiro (2012, apud Damásio, 2003) ensina que os crimes cibernéticos puros ou próprios são aqueles que são praticados por computador e se realizem ou se consumem também em meio eletrônico. Neste tipo de crime, a informática, não em si, mas a segurança dos sistemas, a titularidade das informações, a integridade de dados, da máquina e dos periféricos, é que está sob a proteção legal.

São, portanto, crimes nos quais é necessário que o agente criminoso precise imprescindivelmente de um computador para realizar os ataques de maneira remota ou direta. Assim sendo, pode-se dizer que não estão envolvidas apenas a invasão e a captura dos dados salvos em massa, mas também a intenção ruidosa de modificar, adulterar ou destruir dados existentes no computador. (VIANA, 2003)

Com relação aos crimes cibernéticos impuros, sabe-se que são aqueles praticados com o uso do computador, utilizando o computador como um mero instrumento para a realização do crime.

Damásio (2003) afirma que “são aqueles crimes em que o agente se vale do computador para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço real, ameaçando ou lesando outros bens, não computacionais ou diversos da informática”.

Cabette (2013) ainda nos auxilia um pouco mais com relação a conceituação dos crimes cibernéticos, levando em consideração que podem abranger a interferência no uso legal de um computador, a divulgação de material ofensivo, como por exemplo pornografia, pornografia infantil, jogos, apostas e conteúdos racistas. Também ameaçar comunicações, extorsão, falsificação, roubo de identidade, fraudes financeiras, roubo de internet e serviços telefônicos e vendas diretas, interceptação ilegal de comunicações, espionagem e lavagem de dinheiro.

Soares (2016) ensina que crimes digitais ou virtuais são delitos de informática ou qualquer atividade não autorizada, que geralmente são as condutas destrutivas, infrações como intercepção de comunicações, incitação ao ódio e a discriminação, distribuição de materiais que contenham conteúdo ilegal, como pornografia infantil e outros.

Diante do exposto, crimes cibernéticos são todos aqueles atos ruidosos que estão intrinsecamente ligados ao uso de dados em rede, valendo-se de computadores ou qualquer outro meio tecnológico que tenha acesso à rede mundial de computadores, visando algum malefício a outrem ou ao coletivo.

3 A LEGISLAÇÃO BRASILEIRA E O SISTEMA DE PROTEÇÃO DE DADOS

A Lei 12.965 de 2014, mais conhecida como Marco Civil da Internet, afirma que o acesso à internet é essencial para o exercício da cidadania, e, desta maneira, estão assegurados os seguintes pontos:

> I a inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
> IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização; V - manutenção da qualidade contratada da conexão à internet; (BRASIL, 2014).

Diante disto, apesar de ser o acesso à internet é uma condição de cidadania, não são todas as pessoas que tem acesso a este meio, bem como, não são todas as pessoas que possuem estes direitos assegurados de forma plena, como a garantia da inviolabilidade dos dados, sigilo do fluxo de suas comunicações e mantendo seguras também a intimidade e a vida privada, ainda mais quando se trata de investigação e punição de crimes virtuais.

O Brasil recebe o advento da internet a partir de 1988, inicialmente em São Paulo e no Rio de Janeiro. Desde sua concepção tiveram algumas leis citadas no primeiro capitulo como a Constituição Federal de 1988 que trata a respeito das proteções dos dados e ainda anterior a constituição federal, como forma de prevenção a lei 7.232/84, que dispõe sobre a Política Nacional de Informática e outras providências.

Em 2012 foram promulgadas as leis n° 12.735 e 12.737, que alteram o Código Penal e o Código Penal Militar e a Lei de Preconceitos, tipificando crimes no uso de sistemas eletrônicos e digitais e também os crimes contra sistemas informatizados.

Da primeira, quisemos colacionar os seguintes excertos, que indicam que deverão ser criados meios de combate a este tipo de crime pelos órgãos da polícia judiciária.

> LEI Nº 12.735 - Art. 1 º Esta Lei altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. (...)

> Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.
> Art. 5 º O inciso II do § 3o do art. 20 da Lei nº 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação:(...)
> II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio (BRASIL, 2012)

E a segunda norma, de número 12.737, de 30 de novembro de 2012, que dispôs sobre a tipificação de delitos informáticos e alterou o Código Penal, lei conhecida midiaticamente como “Lei Carolina Dieckmann”, tendo em vista o vazamento criminoso de fotografias íntimas da atriz que havia acontecido seis meses antes da promulgação destas normas.

Senão, vejamos:

> Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.
> Art. 2º O Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:“Invasão de dispositivo informático
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido.
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
> § 5 º 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 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 (BRASIL, 2012)

Pode-se perceber pelos excertos colacionados acima que o Poder Legislativo não se preocupou com os crimes cibernéticos em si, mas sim com um momento pelo qual o país passava, quando uma pessoa de renomada fama teve suas imagens íntimas expostas, e também visando assegurar as pessoas que se encontrarem nos cargos de poder nomeados no §5º da lei colacionada anteriormente. Os crimes praticados na internet cotidianamente continuam sendo julgados tendo como base apenas o dano causado pelos infratores.

Em suma, pode-se dizer que o problema maior relacionado aos crimes virtuais não está exatamente na ausência de uma lei que os venha punir, mas em questões técnicas, que sejam capazes de desvendar os infratores, e de quem seria a competência julgadora, tendo em vista o espaço onde o crime fora cometido.

4 A LEGISLAÇÃO BRASILEIRA SOBRE CRIMES VIRTUAIS E A COAÇÃO A ESTE TIPO DE DELITO

Com relação aos cibercrimes, sabe-se que a privacidade é o ponto focal e é o bem a ser protegido, e como foi possível se perceber da construção deste artigo, a primeira lei que ampara o usuário da internet foi promulgada em 2012, todavia, antes da promulgação desta, outras leis haviam sido criadas para aumentar a segurança das pessoas que se utilizam da internet para lazer, trabalho ou comunicação.

A Lei n° 9.296/1996 menciona que se “constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da justiça”, sem qualquer autorização judicial ou com objetivos que não estejam autorizados ou previstos em lei (BRASIL, 1996).

Em 1998 foi promulgada a Lei n° 9.609 que regulamenta a propriedade dos códigos de um programa a quem o desenvolveu, trazendo uma correlação com as regras de direitos autorais, que, quando violados, pode gerar pena de seis meses a dois anos, ou multa, conforme preleciona o art. 12 da lei em comento, artigo que também trata da venda de produtos piratas em território nacional (BRASIL, 1998).

Em 2008 foi sancionada a Lei n° 11.829, que atualiza o Estatuto da Criança e do Adolescente, que atua diretamente no combate à pornografia infantil na internet. Os artigos que foram adicionados à lei tratam de criminalizar qualquer tipo de troca, disposição, transição ou distribuição, por qualquer forma informatizada ou telematizada, de qualquer tipo de arquivo, contendo cenas de sexo explícito ou qualquer conteúdo pornográfico envolvendo crianças ou adolescentes (BRASIL, 2008).

Mais recentemente, houve a promulgação da Lei 13.709/2018, mais conhecida como a Lei Geral de Proteção de Dados, que tem como objetivo principal a redução dos riscos associados ao uso indevido do processamento de dados pessoais e permitir que os negócios lícitos se desenvolvam no ambiente virtual com maior segurança e tranquilidade. É importante ressaltar que a atuação da LGPD não se restringe aos negócios de empresas brasileiras, mas

também a todos aqueles que fazem negócios em território brasileiro ou que forneçam produtos ou serviços para o mercado brasileiro (TRIFFONI, 2022).

Bortot (2017) ensina que o Marco Civil da Internet trouxe grandes inovações e regulamentações acerca de como os dados que são veiculados a partir da rede mundial de computadores devem ser administrados, todavia, com relação ao combate a crimes virtuais, ainda existe uma lacuna que deve ser preenchida por uma legislação específica e muito bem elaborada, a fim de que os usuários da internet se sintam seguros e amparados com relação a qualquer tipo de conduta criminosa que lhes venha a causar determinados prejuízos.

Para Cruz; Rodrigues (2018) menciona que há ainda um problema grave para a persecução penal contra crimes virtuais, indicando que o ordenamento jurídico brasileiro só permite que a sanção penal seja aplicada quando houver certeza da prática delituosa, sendo fundamental que haja a comprovação da autoria e da materialidade do delito.

Os autores citados anteriormente ainda ressaltam que a preocupação demonstrada por eles no parágrafo anterior se deve ao fato de que a maioria dos crimes não ocorre, em sua maioria, de forma clara, podendo ocorrer na zona obscura da internet, o que dificulta que se encontre o criminoso, ainda que haja um aparato policial competente para a investigação, existem formas múltiplas de se burlar a investigação, e a consequente punição.

Para Pacheco; Costa (2019) existe dificuldade não apenas na dificuldade de se localizar e punir os detratores, mas também na materialidade das provas e no grande número de ataques virtuais, o que demonstra que há uma grande exposição também por parte dos usuários, que acabam por acessar conteúdos perigosos.

Alves (2018) ensina que os crimes cibernéticos crescem constantemente onde as normas jurídicas brasileiras e as medidas preventivas não são suficientes para coibir esta prática ilegal, que cresce vertiginosamente nos últimos anos. O que aparenta, é que existe uma total falta de interesse das autoridades competentes e dos legisladores pátrios no sentido de criar normas que irão contribuir para a consequente diminuição das práticas delituosas que ocorrem na internet.

Alves (2018) ainda menciona que apenas será possível controlar os crimes cibernéticos com a criação de leis que punam com maior rigor e com a

criação de um aparato tecnológico e científico que seja suficiente para que os investigadores tenham capacidade suficiente para identificar os detratores e acabar com as práticas delituosas.

Viana (2017) auxilia na construção deste pensamento no sentido de que também concorda que a legislação brasileira não acompanha a evolução dos crimes virtuais, mencionando ainda que o ordenamento brasileiro não se mostra eficaz para que todas as pessoas que usam a internet se sintam seguras neste ambiente.

5 CONSIDERAÇÕES FINAIS

Muito se fala dos crimes praticados na internet, mas pouco se estuda sobre os mesmos a fim de se traçar um parâmetro ideal de suas implicações jurídicas e da forma que estes crimes assumem perante o ordenamento jurídico brasileiro e internacional, bem como, de que maneira são investigados, tratados e punidos pelas autoridades legais do país.

Sabe-se que o conceito de crime cibernético ainda está em construção, mas de uma maneira ou de outra, ainda se é possível estabelecer meios ideais para a proteção de dados e de pessoas que estão continuamente utilizando a internet como meio de diversão, negócio ou educação.

Pelo fato de a legislação brasileira ainda estar sendo construída nesse sentido, é que ainda existe uma sensação de impunidade para os criminosos que praticam este tipo de crime. Todavia, isto não se deve apenas ao fato de inexistir um arcabouço legal acerca da temática, mas também pela dificuldade da polícia e do poder judiciário em encontrar o criminoso, identificando a autoria e a materialidade dos crimes.

Há que se dizer, por fim, que o Código Penal brasileiro já abarca algumas tipificações e punições de crimes que venham a ser cometidos contra pessoas ou patrimônio de outrem por via da internet. As leis que foram aprovadas nos últimos dez anos não fizeram tanto efeito no ordenamento jurídico, uma vez que não possuem a profundidade que se esperava das leis que regem um assunto tão complexo como os cibercrimes.

Faz-se necessário, portanto, a utilização da interpretação extensiva que, ao contrário da analogia, busca a verdadeira finalidade da norma de forma que a lei alcance os casos advindos dos crimes cibernéticos, como por exemplo, utilizar-se dos artigos que tratam dos crimes de furto, dano e estelionato, visando a proteção de danos a dados informáticos.

Em suma, deve-se considerar que a intenção do legislador é de proteger o utilizador da internet e buscar a punição dos infratores, todavia, é necessário que se façam as adequações necessárias, inserindo na norma termos técnicos específicos, como também dirimir melhor quais podem ser os danos gerados às vítimas.

REFERÊNCIAS

ALVES, Marco Antônio. DINIZ, Thiago Dias de Matos. CASTRO, Viviane Vidigal de. **Criminologia e cibercrimes.** RECAJ – UFMG – Belo Horizonte, 2020. Livro Digital. Disponível em: https://www.conpedi.org.br/wp-content/uploads/2020/12/Livro-8-Criminologia.pdf. Acesso em 24 de outubro de 2021.

ALVES, Maria Hiomara dos Santos. **A evolução dos crimes cibernéticos e o acompanhamento das leis específicas no Brasil.** Disponível em: https://jus.com.br/artigos/64854/a-evolucao-dos-crimes-ciberneticos-e-o-acompanhamento-das-leis-especificas-no-brasil. Acesso em 28 de julho de 2022.

BEZERRA, Clayton da Silva. AGNOLETTO, Giovani Celso. **Combate ao crime cibernético doutrina e prática: A visão do delegado de polícia.** 1. Ed. – Rio de Janeiro; Mallet Editora, 2020.

BORTOT, Jéssica Fagundes. **Crimes cibernéticos: aspectos legislativos e implicações na persecução penal com base nas legislações brasileira e internacional.** Ano 2017. VirtuaJus, Belo Horizonte, v. 2. ISSN 1678-3425.

BRASIL, Ministério das Relações Internacionais. **Brasil é convidado a aderir à Convenção do Conselho da Europa contra a criminalidade cibernética.** Disponível em: https://www.gov.br/secretariageral/pt-br/noticias/2020/julho/brasil-e-convidado-a-aderir-a-convencao-do-conselho-da-europa-contra-a-criminalidade-cibernetica. Acesso em 23 de outubro de 2021.

BRASIL, Lei n° 12.737, de 30 de novembro de 2012. Art. 2°. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 23 de outubro de 2021.

BRASIL, Lei 3.914, de 09 de dezembro de 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3914.htm. Acesso em 23 de outubro de 2021.

BRASIL, Decreto Lei n° 2.848, de 07 de dezembro de 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 23 de setembro de 2021.

BORTOT, Jessica Fagundes. **Crimes cibernéticos: aspectos legislativos e implicações napersecução penal com base nas legislações brasileira e internacional.** VirtuaJus, Belo Horizonte, v. 2, n. 2, p. 338-362, 2017.

CABETTE, Eduardo Luiz Santos. Primeiras impressões sobre a Lei nº 12.735 e o crime de
invasão de dispositivo informático, 2013. Disponível em: https://jus.com.br/artigos/23522/primeiras-impressoes-sobre-a-lei-n-12-737-12-e-o-crime-deinvasao-de-dispositivo-informátic. Acesso em 24 de abril de 2022.

CASTRO, Suelen. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação.** Disponível em: https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/. Acesso em 17 de maio de 2022.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa.** São Paulo: Atlas, 2008.

LÓSSIO, Cláudio Joel Brito. NASCIMENTO, Luano. TREMEL, Rosangela. **Cibernética Jurídica: estudos sobre direito digital.** 2020. Eduepb. Paraíba.

MENEZES, Pedro. **Método Dedutivo.** Ano 2020. Disponível em: https://www.todamateria.com.br/metodo-dedutivo/. Acesso em 23 de outubro de 2021.

NUCCI, Guilherme de Souza. **Manual de Direito Penal.** 11. ed. Rio de Janeiro, Forense, 2015.

PACHECO, Gisele Freitas. COSTA, Renato Lopes. **Crimes virtuais e a legislação penal brasileira.** Disponível em: http://fadipa.educacao.ws/ojs-2.3.3-3/index.php/cjuridicas/article/viewFile/269/pdf. Acesso em 28 de julho de 2022.

RODRIGUES, Juliana. CRUZ, Diego. **Crimes cibernéticos e a falsa sensação de impunidade.** Disponível em: http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf. Acesso em 18 de maio de 2022.

SILVA, Eduardo Soares da. BARAKAT, Najah Jamal Daakour. **Crimes Cibernéticos**. Disponível em: https://www.conpedi.org.br/wp-content/uploads/2020/12/Livro-8-Criminologia.pdf. Acesso em 18 de maio de 2022.

SOARES, Bruno Dutra Serafim. **O ordenamento jurídico e os crimes virtuais.** Disponível em: http://dspace.bc.uepb.edu.br/jspui/bitstream/123456789/13948/1/PDF%20-%20Bruno%20Dutra%20Serafim%20Soares.pdf. Acesso em 28 de julho de 2022.

TRIFFONI, Marina de Sousa Alencar. **Cibercrimes: a internet como ferramenta na execução de crimes virtuais e o combate realizado pelo direito penal brasileiro.** Disponível em: https://conteudojuridico.com.br/consulta/Artigos/58324/cibercrimes-a-internet-como-ferramenta-na-execuo-de-crimes-virtuais-e-o-combate-realizado-pelo-direito-penal-brasileiro#:~:text=12.737%2F2012%20que%20disp%C3%B5e%20sobre,com%20legisla%C3%A7%C3%B5es%20mais%20espec%C3%ADficas%20e. Acesso em 28 de julho de 2022.

VIANA, André de Paula. **Crimes virtuais e a necessidade de uma legislação específica.** Disponível em: https://egov.ufsc.br/portal/conteudo/crimes-virtuais-

e-necessidade-de-uma-legisla%C3%A7%C3%A3o-especifica. Acesso em 28 de julho de 2022.