CRIMES CIBERNÉTICOS: A APLICAÇÃO DA LEGISLAÇÃO BRASILEIRA AOS CRIMES VIRTUAIS PRATICADOS EM PALMAS – TO

Victor Castro Silva [1]
Igor de Andrade Barbosa[2]

RESUMO
O presente trabalho tem como objetivo compreender a aplicação da legislação brasileira aos casos de crimes virtuais ocorridos em Palmas – TO. Com o avanço tecnológico, a sociedade contemporânea está cada vez mais conectada ao mundo virtual, haja vista que, com o advento da internet, mudou-se a forma de realizar algumas atividades do cotidiano das pessoas, como por exemplo: se comunicar, fazer compras, se relacionar, entre outras. Mas, junto com todas as melhorias trazidas pela internet, passou a surgir também, novos crimes, estes agora, praticados de forma virtual através da rede mundial de computadores. Diante disso, pergunta-se: de que maneira a legislação brasileira está sendo aplicada aos crimes cibernéticos? Para responder a essa indagação, o presente trabalho abordará temas como: a síntese histórica do computador e da internet, assim como também, a definição de crimes virtuais e crimes cibernéticos e também, a legislação pertinente aos crimes cibernéticos. Serão abordadas, também, as mudanças no combate aos crimes virtuais após a promulgação das leis 12.737 de 2012 e 12.735 de 2012.

Palavras – Chave: Internet. Leis. Tecnologia.

ABSTRACT
This paper's aims is to understand the application of Brazilian law to the cases of virtual crimes in Palmas - TO. With technological advancement in contemporary society, its increasingly connected to the virtual world, considering that, with the advent of the internet, the way of carrying out some daily actives of people has changed, such as: communicating, shopping, relate, among others. But, along with all the improvements brought by the internet, new crimes have come to light, these now, being practiced virtually through the world wide web. Therefore, we ask: how is brazilian law being applied to cyber crimes? To answer this question, the present work will address topics such as: the historical synthesis of the computer and the internet, as well as the definition of cyber and cyber crimes, as well as the pertinent legislation for cyber crimes. They will also be discussed the changes in the fight against cybercrime following the enactment of laws 12.737 of 2012 and 12.735 of 2012.

Keywords: *Internet. Laws. Technology.*

1 INTRODUÇÃO

A internet, a rede mundial de computadores, é uma das principais responsáveis pela globalização e, sem dúvida, é a ferramenta mais utilizada pela sociedade contemporânea. Com o avanço tecnológico e o advento da internet, foi possível fazer coisas extraordinárias, como por

1 Bacharel em Direito pelo Centro Universitário Católica do Tocantins. E-mail: v.castro1790@hotmail.com
2 Professor do curso de Direito do Centro Universitário Católica do Tocantins – E-mail: igor.barobsa@catolica-to.edu.br

exemplo, a troca de informações intercontinentais de forma instantânea. Atualmente, é quase improvável que uma pessoa com discernimento afirme não ter nenhum contato com o mundo virtual.

Segundo Gomes (2018), em 2018, o Brasil terminou o ano com um número de aproximadamente 116 milhões de pessoas com acesso à rede mundial de computadores. Isso equivale a 64,7% de todas as pessoas acima dos 10 anos de idade. Logo, nota-se que a maior parte da população tem uma grande facilidade em ter acesso à internet, seja para trabalhar, fazer compras, trocar informações ou até mesmo para o próprio lazer.

De acordo com Machado (2014), no ano de 2011, os sistemas computacionais no Brasil chegaram a ter quase o triplo de ataques, se comparado com o ano de 2012. Em 2012, foram registrados um total de 399.515 (trezentos e noventa e nove mil e quinhentos e quinze) problemas referentes a vírus, tentativas de fraude ou códigos maliciosos, enquanto no ano de 2010, esses números eram de apenas 142.844 (cento e quarenta e dois mil e oitocentos e quarenta e quatro) registros.

Diante disso, é evidente que a internet trouxe inúmeras melhorias para a sociedade, mas junto com os benefícios, vieram os malefícios. Com as facilidades proporcionadas pela internet, surgiram diversos crimes virtuais. Os criminosos se aproveitam do anonimato que a internet lhes proporciona, para praticar os mais variados tipos de condutas delituosas.

O Código Penal vigente no Brasil é de 1940 e precisa ser atualizado, já que condutas que antes eram justas, hoje já não são mais e as condutas que hoje são justas, futuramente não serão. Sendo assim, é necessário que o Direito trate de tipificar e punir de forma efetiva os crimes praticados de forma virtual, com o auxílio da internet. O Direito é uma ciência social evolutiva e tem como obrigação acompanhar a evolução da sociedade da qual tutela os bens jurídicos dos cidadãos.

Portanto, ao mesmo tempo que internet revolucionou a vida das pessoas, serviu também, para mostrar a enorme fragilidade frente à tecnologia que hoje lhes é oferecida.

Quanto às ocorrências de crimes cibernéticos, o Estado do Tocantins também apresenta um grande número de casos. Segundo a TV Anhanguera (2019), em um ranking contendo todos os crimes virtuais praticados no Estado do Tocantins, o estelionato virtual aparece em primeiro lugar como o crime virtual com mais ocorrências, com 223 registros, de acordo com informações da Polícia Civil. Nesse ranking está também, o furto qualificado com abuso de confiança, em segundo lugar, com 67 ocorrências; os crimes contra a honra, como injúria e difamação aparecem em terceiro lugar, com 58 casos registrados.

Nessa perspectiva, diante da evolução da tecnologia, do uso essencial da internet pela sociedade e dos crimes praticados através dela sem que haja a devida punição aos autores desses delitos, faz-se necessário observar de que maneira é feito o combate a essas condutas ilícitas. Portanto, o presente trabalho tem como objetivo compreender a aplicação da legislação brasileira aos casos de crimes virtuais ocorridos em Palmas – TO.

2 PROCEDIMENTOS METODOLÓGICOS

Este estudo foi realizado por meio de método dedutivo, pois abordou diversos casos através de estudos já realizados, com o intuito de se chegar a uma conclusão lógica. Em relação à natureza da pesquisa, considera-se uma pesquisa básica, pois teve como objetivo, melhorar e enriquecer as teorias científicas a respeito do tema abordado. A pesquisa é de cunho bibliográfico com o auxílio de livros, artigos, periódicos, monografias e leis.

De acordo com o objetivo abordado no artigo, considera-se um estudo descritivo e explicativo, pois foi realizado um levantamento sobre os casos de crimes virtuais ocorridos em Palmas – TO. Foi realizada uma análise qualitativa a respeito de como é a aplicabilidade da legislação brasileira frente aos crimes virtuais praticados em Palmas – TO.

Este estudo utilizou como embasamento algumas leis, tais como: Constituição Federal de 1988; Código Penal Brasileiro (Decreto – Lei Nº 2.848, de 07 de dezembro de 1940); Lei 12.737 de 2012 e Lei 12.735 de 2012 (leis estaduais). Visando a melhor compreensão do tema, foram realizadas visitas *in loco* à Delegacia de Repressão a Crimes Cibernético (DRCC) de Palmas, localizada no **complexo II** de Delegacias Especializadas - Avenida Teotônio Segurado, Quadra. 202 Sul, Conj. I, Lote: 04, Plano Diretor Sul, Palmas - TO.

São abordados, portanto, os principais casos de crimes cibernéticos praticados na cidade de Palmas após a publicação da Lei 12.737 de 2012, popularmente conhecida como Lei Carolina Dieckmann, tais como: crimes contra a honra (injúria e difamação), estelionato virtual, furto de dados, compartilhamento de fotos íntimas, entre outros.

3 DESENVOLVIMENTO

3.1 SÍNTESE HISTÓRICA DO COMPUTADOR

O computador é um aparelho eletrônico que produz, envia, recebe e armazena informações de maneira prática e automática. Durante a segunda metade do século XX e agora XXI, essa ferramenta eletrônica tem evoluído juntamente com a sociedade, de forma até bem mais rápida! Com isso, o número de computadores usados em todo o mundo só tem crescido, tendo em vista que o computador se tornou algo comum do cotidiano de toda a sociedade.

Segundo Diana (2019), a palavra computador significa calcular e, tendo em vista que a palavra vem do verbo “computar’’, nesse passo é possível inferir que a necessidade do homem em calcular deu ensejo a criação de uma ferramenta rudimentar, o “ábaco”, instrumento de origem chinesa criado o século V a.c., uma das primeiras máquinas de contar. Neste contexto, é límpido deduzir que, baseado nas necessidades do homem, foi possível alcançar a tecnologia atual que a humanidade

utiliza no computador.

Com o passar do tempo, acompanhando diversas áreas da matemática, como por exemplo, a engenharia, o computador foi se aperfeiçoando e sofrendo várias transformações até se tornar o que conhecemos hoje. Ainda de acordo com Diana (2019), a história do computador está basicamente dividida em quatro períodos: Primeira Geração (de 1951 a 1959), Segunda Geração (de 1959 a1965), Terceira Geração (de 1965 a 1975) e Quarta Geração (de 1975 até os dias atuais). Sendo:

> **Primeira Geração (1951-1959):**
> Os computadores de primeira geração funcionavam por meio de circuitos e válvulas eletrônicas. Possuíam o uso restrito, além de serem imensos e consumirem muita energia.
> **Segunda Geração (1959-1965):**
> Ainda com dimensões muito grandes, os computadores da segunda geração funcionavam por meio de transistores, os quais substituíram as válvulas que eram maiores e mais lentas. Nesse período já começam a se espalhar o uso comercial.
> **Terceira Geração (1965-1975):**
> Os computadores da terceira geração funcionavam por circuitos integrados. Esses substituíram os transistores e já apresentavam uma dimensão menor e maior capacidade de processamento. Foi nesse período que os chips foram criados e a utilização de computadores pessoais começou.
> **Quarta Geração (1975-até os dias atuais):**
> Com o desenvolvimento da tecnologia da informação, os computadores diminuem de tamanho, aumentam a velocidade e capacidade de processamento de dados. São incluídos os microprocessadores com gasto cada vez menor de energia. Nesse período, mais precisamente a partir da década de 90, há uma grande expansão dos computadores pessoais. Além disso, surgem os softwares integrados e a partir da virada do milênio, começam a surgir os computadores de mão. Ou seja, os smartphones, iPod, iPad e tablets, que incluem conexão móvel com navegação na web. (DIANA, 2019, p. 01)

Verifica-se que os computadores atuais integram e permanecem na quarta geração. Observando este contexto, percebe-se que, anteriormente, a evolução dessas máquinas se dava de forma mais lenta, o que é contrário ao que ocorre nos dias atuais, pois, o que antes demorava anos para se desenvolver, hoje evolui em meses, semanas ou até mesmo em horas. Com a sociedade não é diferente, tendo em vista que com o passar do tempo a sociedade tem se desenvolvido de forma cada vez mais rápida.

O primeiro computador do mundo é chamado ENIAC (*Eletronic Numerical Integrator and Computer)*, ou traduzido para o português, Computador e Integrador Numérico Eletrônico, construído entre os anos de 1943 e 1946. Conforme HD Store (2018, p. 01):

> O conjunto inteiro que formava o computador ocupava uma área de 180m², praticamente o dobro de um apartamento médio no Brasil. O Eniac funcionava por meio de 70 mil resistores e 18 mil válvulas e precisava de 200 mil watts de energia para funcionar. Construído entre 1943 e 1946, período final da guerra, ele só foi ligado um ano depois. O processamento de dados era feito através de cartões perfurados manuseados por funcionárias do exército, reconhecidas hoje como as primeiras programadoras da história. Apesar de não possuir armazenamento e ter sido superado em poder em pouco tempo, o Eniac, em seu tempo de vida, conseguiu realizar mais cálculos do que a humanidade em toda a sua história anterior àquele ponto. Esse é o tipo de dado que revela o poder da informática e como essa primeira

> máquina se tornou o início de uma revolução universal para a nossa espécie (HD STORE, 2018. P.01).

3.2 SÍNTESE HISTÓRICA DA INTERNET

A internet foi criada durante a Guerra Fria[3] (1945 – 1991), mais precisamente, no ano de 1969, nos Estados Unidos. Na época, o mundo estava vivendo o apogeu da Guerra Fria, em que as duas principais grades potências, EUA e União Soviética, disputavam por hegemonia e poder.

Quando da sua criação, a internet tinha o nome de Arpanet (*Advanced Research Projects Agency Network)*. Temendo ataques dos inimigos e com o intuito de facilitar e de garantir a troca de informações entre cientistas e militares, a internet (Arpanet) foi desenvolvida pelo Departamento de Defesa dos Estados Unidos, por um professor da Universidade da California, sendo este, o responsável por enviar o primeiro E-mail da história.

Inicialmente, o uso da internet era restrito e apenas os Estados Unidos possuía acesso, passando a se expandir no ano de 1982 para outros países como a Suécia e a Holanda. Somente no ano de 1987, pela primeira vez, nos Estados Unidos, a internet foi liberada para uso comercial. De acordo com Silva (2001, p. 01):

> Em 1992, começaram a surgir diversas empresas provedoras de acesso à internet naquele país. No mesmo ano, o Laboratório Europeu de Física de Partículas (Cern) inventou a World Wide Web, que começou a ser utilizada para colocar informações ao alcance de qualquer usuário da internet. Desde então, a difusão da rede foi enorme. Hoje, a internet tem mais de 250 milhões de usuários em todo o mundo (SILVA, p. 01).

Mas, só foi a partir da década de 1990, com o surgimento de novos navegadores, como por exemplo: Mozilla Firefox, Google Chrome, Internet Explorer, Opera, entre outros, que a internet se propagou por todo o mundo, aumentando o número de usuários. Logo, surgiram também, um grande número de redes sociais, como: Orkut, MSN, Facebook e Twitter, chats e sites.

No ano de 1994, a internet passou a ser disponibilizada para o público em geral. No Brasil, a responsável pela comercialização foi a EMBRATEL, escolhendo cinco mil usuários para testar o serviço em caráter experimental, vindo a funcionar de forma definitiva somente no ano posterior (ARRUDA, 2011).

Mas, somente em 1996, até mesmo pela melhoria na qualidade dos serviços prestados, foi que a internet teve o seu maior avanço no Brasil, com um aumento significativo de usuários, assim como também, de provedores. A prova mais marcante desse avanço no Brasil veio no final deste mesmo ano, quando o cantor Gilberto Gil lançou sua música usando a internet, conversando com

3 A Guerra Fria, que teve seu início logo após a Segunda Guerra Mundial (1945) e a extinção da União Soviética (1991), é a designação atribuída ao período histórico de disputas estratégicas e conflitos indiretos entre os Estados Unidos e a União Soviética, disputando a hegemonia política, econômica e militar no mundo.

internautas enquanto cantava uma versão acústica ao vivo (MULLER, 2018).

Diante de todo o exposto, há de observar o quão rápido evoluiu o computador e a internet, além de como mudou de forma significativa a vida de toda a população e alcançou desde os mais ricos aos com menores condições financeiras, isto porque, existem no mercado produtos tecnológicos com os mais variados preços.

3.3 CRIMES VIRTUAIS E CRIMES CIBERNÉTICOS

São muitas as denominações referentes aos crimes praticados no mundo virtual, dentre elas as mais comuns são: Crimes Virtuais ou Crimes Cibernéticos. Ainda não se chegou a um consenso sobre qual seria a melhor terminologia para a prática dos crimes relacionados à tecnologia.

Os atos ilícitos praticados no ambiente virtual, de acordo com Zuliani *et al.* (2012, p. 276), "são as ações antijurídicas realizadas por intermédio dos sistemas informáticos com o objetivo de causar danos ao sistema ou possibilitar a obtenção de uma vantagem econômica para o agente.''

Segundo Tavares; Reis (2014, p. 29), "crime de informática é aquele praticado com auxílio do sistema de informática ou contra, podendo ser compreendido aqueles crimes praticados contra o computador e também seus acessórios e os perpetrados através do computador.''

No mundo jurídico, existem alguns conceitos para ato ilícito. No Direito Penal, segundo Greco (2017, p. 451), ato ilícito é:

> Ilicitude, ou antijuridicidade, é a relação de antagonismo, de contrariedade entre a conduta do agente e o ordenamento jurídico. (...) Se a conduta típica do agente colidir com o ordenamento jurídico penal, diremos ser ela penalmente ilícita.

Tendo em vista que o Código Penal não trouxe uma definição clara sobre o que é crime, a doutrina tem procurado definir o conceito de ilícito penal sob três aspectos, sendo eles: aspecto formal, aspecto material ou substancial e aspecto analítico. (MIRABETE e FABBRINI, 2010).

Já para o Direito Civil, segundo o artigo 186 e 187 do Código Civil de 2002, tem-se ato ilícito quando:

> Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito;
> Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes.

Vale ressaltar que o ato ilícito civil se difere do ato ilícito penal, tendo em vista que, para que o ato ilícito penal ocorra, basta que o agente tenha uma conduta contrária ao que está disposto na Lei, causando com isso, uma lesão ou expondo a perigo, um bem jurídico tutelado pelo Direito Penal.

Por outro lado, para que ocorra o ilícito civil, o indivíduo tem que, além de praticar uma

conduta que viole direito alheio, causar um dano a quem teve o direito lesado. Importante saber que, ao agente que comete um ilícito penal, pode chegar a ter a sua liberdade privada, enquanto que no ilícito civil, o agente será obrigado a reparara o dano causado por ele.

Seguindo os ensinamentos de Hungria, nas palavras de Jesus (2015, p. 203), temos:

> Não há diferença substancial ou ontológica entre ilícito penal e o civil. Em sua essência, não há diferença entre eles. A diferença é de natureza legal e extrínseca: o ilícito penal é um injusto sancionado com a pena; o civil é o injusto que produz sanções civis. Somente se atentando à natureza da sanção é que podemos determinar se nos encontramos em face de um ou de outro (JESUS, 2015, p. 203).

A legislação brasileira é vasta, no entanto, nota-se que ela necessita de uma legislação específica para tratar dos delitos praticados no ambiente virtual. É perceptível a carência de normas jurídicas que tornem eficaz o combate às condutas ilícitas praticadas no ciberespaço. Isso se dá pelo fato de que a internet, assim como muitos crimes praticados através dela, são respectivamente novos para o nosso ordenamento jurídico. (SOARES, 2016).

Portanto, nota-se que o crime cibernético é toda conduta típica, antijurídica e culpável, praticada no ambiente virtual através de um computador ligado à internet contra um sistema computacional, ainda que o computador seja um mero instrumento para a prática de crimes comuns, com o objetivo de obter vantagens pecuniárias ou de somente causar danos aos dispositivos informáticos.

Em se tratando dos autores dos delitos informáticos, nas nobres palavras de Vidal (2015, p. 07), temos:

> Na informática existe usuários chamados “crackers” que visando diminuir a segurança dos computadores e, por consequência, da própria internet, observa-se a utilização de diversos mecanismos que se dispõem, sobretudo, ao compartilhamento de dados sem o consentimento do seu legítimo detentor, ou seja, invade os computadores com a finalidade de causar danos, de cometer ilícitos, de se aproveitar das falhas existentes no sistema para obter vantagem indevida (VIDAL, 2015, p. 07).

Ainda de acordo com Vidal (2015, p. 07), quanto aos métodos utilizados por esses indivíduos para invadir os sistemas de informática e os computadores, destaca:

> a) Spamming – conduta de mensagens publicitárias por correio eletrônico para uma pequena parcela de usuários; b) Cookies – são arquivos de texto que são gravados no computador de forma a identificá-lo. Assim, o site obtém algumas informações, tais como quem está acessando o site, com que periodicidade o usuário retorna à página da web e outras informações almejadas pelo portal; c) Spywares – são programas espiões que enviam informações do computador do usuário para desconhecidos na rede; d) Hoaxes – são e-mails, na maioria das vezes com remetente de empresas importantes ou de órgãos governamentais, contendo mensagens falsas, induzindo o leitor a tomar atitudes prejudiciais a ele próprio; e) Sniffers – são programas espiões semelhantes ao spywares que são introduzidos no disco rígido e têm capacidade de interceptar e registrar o tráfego de pacotes na rede; f) Trojan horse ou cavalos de Troia – quando instalado no computador, o trojan libera uma porta de acesso ao computador para uma possível invasão. O cracker pode

> obter informações de arquivos, descobrir senhas, introduzir novos programas, formatar o disco rígido, ver a tela e até ouvir a voz, caso o computador tenha um microfone instalado. Como boa parte dos micros é dotada de microfones ou câmeras de áudio e vídeo, o trojan permite fazer escuta clandestina, o que é bastante utilizado entre os criminosos que visam à captura de segredos industriais; e g) Keyloggers é uma forma de spyware que registra cada batida no teclado ou outra atividade num sistema.

Os crimes cibernéticos abrangem os mais variados tipos de condutas delitivas, podendo ser eles classificados como Crimes Virtuais Puros ou Próprios e Crimes Virtuais Impuros ou Impróprios.

Nos Crimes Virtuais Puros, o dano é causado ao computador, ou seja, o agente visa causar um prejuízo material ao aparelho eletrônico. Então, nesta ocasião, o dano é causado através de um computador e seus acessórios, tendo como alvo, outro aparelho eletrônico ou seus acessórios, como por exemplo, a instalação de vírus e o embaraçamento de sistemas.

Já nos Crimes Virtuais Impuros, o aparelho eletrônico é apenas uma ferramenta utilizada pelo autor do fato delitivo para consumar um dano causado no mundo físico, ou seja, lesando ou ameaçando bens distintos da informática. Neste caso, os crimes impuros são delitos comuns praticados com o auxílio do computador.

Podemos listar alguns dos principais Crimes Virtuais Puros: sabotagem do sistema, contaminação por vírus, destruição ou modificação de conteúdo do banco de dados, interceptação de E-mail, entre outros.

Segundo Vidal (2015, p. 09), os principais Crimes Virtuais Impuros são:

> a) estelionato: a conduta do agente será de induzir ou manter a vítima em erro, e com isso, obtendo vantagem ilícita, para si ou para outrem. (...), b) insultos: (...) Artigo 140 do Código Penal, que pune "a injúria que ofende a dignidade ou decoro "; c) calúnia: (...) enquadrado no Artigo 138 do Código Penal; d) difamação: (...) Artigo 139 do Código Penal; e) divulgação de segredo: (...) Artigo 153 do Código Penal; f) escárnio por motivo de religião: (...) Artigo 208 do Código Penal; g) favorecimento da prostituição: Artigo 228 do Código Penal; h) ato obsceno: Artigo 233 do Código Penal; i) escrito ou objeto obsceno: Artigo 234 do Código Penal; j) incitação ao crime: Artigo 286 do Código Penal; l) apologia de crime: (...) Artigo 287 do Código Penal; m) falsa identidade: (...) Artigo 307 do Código Penal; n) preconceito ou discriminação: (...) Artigo 20 da Lei 7.716/89; o) pedofilia: (...) Artigo 241-A, 241-B, 241-C, 241-D e 241-E da Lei no 8.069/90 ECA; p) Privacidade: trata, basicamente, da coleta e mau uso de dados. (...), e q) pirataria de software: (...) copiar dados em CDs, DVDs ou qualquer base de dados sem prévia autorização do autor é entendido como pirataria de acordo com a Lei 9.610/98.

Assim como em todo o País, a capital do Estado do Tocantins, Palmas, também apresenta um grande número de crimes cibernéticos. A capital do Estado conta com uma Delegacia especializada no combate aos crimes virtuais, a Delegacia de Repressão a Crimes Cibernéticos (DRCC).

De acordo com a TV Anhanguera (2019), nos seis primeiros meses do ano de 2019 foram registrados pela delegacia de combate a crimes virtuais de Palmas um total de 218 crimes virtuais praticados na capital. Dentre os principais, podemos citar o estelionato, a extorsão, falsidade ideológica, entre outros.

Outro delito que, apesar de novo, já é bastante comum na cidade de Palmas é o “sequestro’’ da rede social WhatsApp. As denúncias de pessoas que tiveram seu WhatsApp sequestrado chegam quase que diariamente.

O golpe se dá quando a pessoa, vítima do crime, recebe um link de pessoas mal-intencionadas, com notícias relacionadas a alguma mudança no aplicativo e, a partir do momento que a vítima clica no link, automaticamente o criminoso passa a ter acesso a sua conta do aplicativo. O intuito do golpe é enviar mensagens para toda a agenda da vítima se passando por ela, informando que está com alguma dificuldade e pede para que as pessoas façam uma transferência bancária para a sua conta.

Em Palmas, no ano de 2018, a Polícia Federal realizou uma operação na qual prendeu hackers que agiam no Estado do Tocantins e em mais outros três Estados. Essa quadrinha de hackers era suspeita de desviar cerca de R$ 10 milhões de diversas contas bancárias. Os criminosos usavam moedas virtuais e empresas falsas para fazer a lavagem do dinheiro obtido de forma ilícita. O golpe era aplicado quando as vítimas acessavam suas contas bancárias de forma virtual, através do computador ou até mesmo pelo celular. (G1, 2018).

Segundo Santos (2019, p. 01):

> Para a delegada da DRCC, Milena Lima, é prematuro falar em aumento de casos de 2017, quando a Delegacia foi implantada, para o ano de 2018. Entretanto, ela alerta sobre a diversificação dos crimes cometidos. “Com a universalização do uso da internet, é natural que os meios para o cometimento de crimes se renovem, de modo que o ambiente virtual se torne cada vez mais atrativo. Os crimes continuam os mesmos, o que muda é o modo de agir’’, afirma.

Diante de todo o exposto, por ser algo recente e ainda de difícil controle por parte das autoridades, a internet aumentou a sensação de liberdade do ser humano, pois o ato de separar as pessoas por um dispositivo de troca de informação acaba proporcionando a elas o anonimato. Todas essas mudanças estimuladas pelos avanços tecnológicos fizeram com que surgisse um novo padrão de sociedade pós-moderna e de sistemas responsáveis por sua regularização e organização, como o Direito (VIDAL, 2015).

O Direito é um conjunto de princípios e normas que regem uma determinada sociedade. Logo, tendo em vista que o Direito é responsável por tutelar os bens jurídicos dos indivíduos que compõe determinada comunidade, tem a obrigação de modificar-se à medida que essa respectiva sociedade evolui, a fim de garantir os direitos atinentes aos cidadãos, assim como também, impor seus deveres e obrigações.

À vista disso, a maior compreensão e domínio da tecnologia por parte do Direito tem como objetivo oferecer uma maior segurança às pessoas que constantemente fazem o uso da internet. Caso contrário, os crimes praticados no ambiente virtual se tornarão cada vez mais comum, e o pior, sem as medidas adequadas para combatê-los.

Portanto, é necessário entender como é feito o combate aos crimes praticados com o auxílio da internet, como por exemplo, os casos ocorridos em Palmas – TO, para que a população saiba com exatidão o que fazer para se prevenir desses tipos de crimes e, caso seja vítima, que saiba a quem recorrer.

3.4 LEGISLAÇÃO PERTINENTE AOS CRIMES CIBERNÉTICOS

Além das vantagens e novidades que a internet trouxe, a rede mundial de computadores também se mostrou como um ambiente propício para o cometimento de crimes, uma vez que, indivíduos mal intencionados se aproveitam do anonimato proporcionado pela internet para praticar as mais diversas condutas criminosas, tendo em vista que os vestígios deixados por essas condutas criminosas são mínimas, tornando o combate a esses delitos quase que impossível (NETO, 2008).

O combate a esses crimes cometidos no ambiente virtual mostra-se ineficaz, tendo em vista que o Código Penal vigente no Brasil é de 1940, ou seja, já está arcaico no que diz respeito aos crimes cibernéticos, já que ao tempo de sua criação, nem se cogitava a existência de uma rede mundial de computadores que proporcionaria uma mudança radical na vida de toda a sociedade, tanto no que diz respeito às mudanças benéficas como às maléficas.

O ordenamento jurídico brasileiro conta com algumas leis específicas para combater os crimes virtuais. Entre elas, podemos destacar a mais conhecida, a Lei 12.737 de 2012, popularmente conhecida como Lei Carolina Dieckmann.

Essa lei já tramitava no Congresso Nacional desde o ano de 2011, mas só veio a ser sancionada em 2012, pela então presidente Dilma Rousseff, após a atriz Carolina Dieckmann ter tido o seu computador invadido por hackers que usaram suas fotos íntimas para extorqui-la. O caso ganhou grande repercussão nacional, o que fez com que essa Lei torna-se uma realidade, modificando o Código Penal, incluindo alguns artigos e modificando outros, tais como: artigos 154 – A e 154 – B, além dos artigos 266 e 298. O artigo 154 – A e o 154 – B, tratam, respectivamente, da invasão de dispositivo informático e da ação penal. Vejamos:

> 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.
> **Ação penal**
> 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.

Já o artigo 266, trata do crime de interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública. Enquanto o artigo 298 trata da falsificação de documento particular, incluindo-se aqui, o cartão de crédito ou de débito, que até então, não era considerado como documento particular.

A lei Azeredo, como é conhecida a Lei 12.735 de 2012, traz explícito no texto de seu artigo 4º, que a polícia judiciária ficará responsável por estruturar setores e equipes especializadas no combate de crimes praticados no ambiente virtual, assim como também em dispositivos de comunicação ou sistemas informatizados.

Além disso, a recente Lei 12.964 de 2014, denominada de Marco Civil da Internet, estabelece os princípios, as garantias, os direitos e deveres para o uso da internet no Brasil. Essa lei garante aos usuários uma maior proteção no que diz respeito à divulgação de seus dados pessoais.

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no **caput,** de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.
> § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º
> § 3º O disposto no **caput** não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.
> § 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

Quanto à competência para julgar crimes cometidos de forma virtual, nos casos de ameaças cometidas através das redes sociais, como por exemplo, o WhatsApp e o Facebook, o Superior

Tribunal de Justiça tem entendido que o local de consumação do crime se dá no local onde a vítima tomou ciência das ameaças, logo, o juízo competente para julgar um pedido de medida protetiva será o desse respectivo local.

Percebe-se que o ordenamento jurídico brasileiro já possui algumas leis que se dispõe a tratar das condutas ilícitas praticadas no ambiente virtual. No entanto, não são suficientes para coibir de forma concreta os crimes cibernéticos. Necessita, portanto, que o legislador tipifique de forma mais objetiva os ilícitos cometidos na rede mundial de computadores e as suas respectivas punições, com sansões mais severas para assegurar total segurança às pessoas que tenham qualquer tipo de acesso à internet.

4 CONSIDERAÇÕES FINAIS

O combate aos crimes cibernéticos teve uma grande evolução, principalmente após a promulgação das leis 12.737 e 12.735, de 2012. Todavia, percebe-se a necessidade de leis que tratem dos crimes cometidos no ambiente virtual de forma mais punitiva e eficiente, tendo em vista que as referidas leis impõem punições consideradas como brandas para os autores desses crimes.

A Lei 12.737/12 foi criada para saciar os anseios da sociedade, isto é, foi criada de uma forma rápida com o objetivo de dar uma resposta à sociedade no que diz respeito ao combate dos crimes praticados na rede mundial de computadores, principalmente após o episódio envolvendo a atriz Carolina Dieckmann, que teve seu computador invadido por hackers que divulgaram suas fotos íntimas, conduta esta, que até então não era tipificada pelo Ordenamento Jurídico brasileiro.

Pode-se observar que a referida lei foi promulgada de uma forma não tão eficiente. Isso se dá porque com a necessidade de uma lei que tipificasse as condutas delituosas praticadas na internet fez com o que o legislador, ao promulgar a Lei 12.737/12, deixasse diversas lacunas na lei.

No que diz respeito aos crimes cibernéticos cometidos no Estado do Tocantins, o regimento interno da Polícia Civil, aprovado pelo Decreto n. 5.979, de 12 de agosto de 2019, na subseção III, Art. 77, define as atribuições da Divisão Especializada de Repressão a Crimes Cibernéticos (TOCANTINS, 2019, p. 17)

> Da Divisão Especializada de Repressão a Crimes Cibernéticos (DRCC)
>
> Art. 77. Compete à Divisão Especializada de Repressão a Crimes Cibernéticos (DRCC) prevenir, reprimir e investigar as infrações penais praticadas por meio da internet ou com a utilização de sistemas de informática, desde que verificada qualquer das seguintes condições:
> I - a infração penal seja punida com pena privativa de liberdade máxima igual ou superior a 4 (quatro) anos;
> II - a infração penal, ainda que punida com pena privativa de liberdade máxima inferior a 4 (quatro) anos, envolva qualquer das circunstâncias previstas nos incisos I a III do §4º do art. 82 deste Regimento.

Por fim, nota-se que o ordenamento jurídico brasileiro é detentor de uma quantidade

significativa de normas jurídicas, no entanto, carece de leis que tipifiquem de forma efetiva os crimes virtuais, uma vez que, as normas que tratam desses ilícitos ainda não têm uma efetiva aplicação nos casos concretos, pois o Código Penal vigente no Brasil é do ano de 1940, o que inviabiliza a identificação e a punição dos autores de crimes cibernéticos.

REFERÊNCIAS

ANHANGUERA, T. **G1**, 2019. Disponível em: https://g1.globo.com/to/tocantins/noticia/2019/06/27/palmas-tem-mais-de-200-golpes-aplicados-pela-internet-em-seis-meses.ghtml. Acesso em: 02 jun. 2020.

ANHANGUERA, T. G1. **G1**, 2019. Disponível em: https://g1.globo.com/to/tocantins/noticia/2019/02/10/estelionato-virtual-aparece-em-1o-lugar-no-ranking-dos-crimes-praticados-na-internet-no-to.ghtml. Acesso em: 21 out. 2019.

ARRUDA, F. 20 anos de internet no Brasil: aonde chegamos? **TecMundo**, 2011. Disponível em: https://www.tecmundo.com.br/internet/8949-20-anos-de-internet-no-brasil-aonde-chegamos-.htm. Acesso em: 28 out. 2019.

BRASIL. Decreto nº 2.848, de 07 de dez. de 1940. **Código Penal**, Brasília, DF, dez. 1940.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. **Instituto o Código Civil**, Brasília, DF, jan. 2002.

BRASIL. Lei nº 12.964, de 23 de abr. de 2014. **Marco Civil da Internet**, Brasília, DF, abr. 2014.

DIANA, D. B. G. História e Evolução dos computadores. **Toda Matéria**, 2019. Disponível em: https://www.todamateria.com.br/historia-e-evolucao-dos-computadores/. Acesso em: 22 out. 2019.

GARCIA, R. A. C.; CARUZO, W. R.; JÚNIOR, J. W. Z. Crimes Cibernéticos. **Revista Matiz Online**, Matão - SP, 2017.

GOMES, H. S. G1. **G1**, 2018. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/brasil-tem-116-milhoes-de-pessoas-conectadas-a-internet-diz-ibge.ghtml. Acesso em: 21 out. 2019.

GRECO, R. **Curso de Direito Penal**. 19. ed. Niterói, RJ: Impetus, v. 1, 2017.

JESUS, D. D. **Direito Penal**. 36. ed. São Paulo: Saraiva, v. 01, 2015.

JURÍDICO, C. **Consultor Jurídico**, 2018. Disponível em: https://www.conjur.com.br/2018-jun-17/stj-divulga-jurisprudencia-conceitos-crimes-internet. Acesso em: 19 nov. 2019.

MACHADO, L. A. **DireitoNet**, 2014. Disponível em: https://www.direitonet.com.br/artigos/exibir/8772/Crimes-ciberneticos. Acesso em: 21 out. 2019.

MIRABETE, J. F.; FABBRINI, R. N. **Manual de Direito Penal**. 26. ed. São Paulo: Atlas, v. 1, 2010.

MULLER, N. O começo da internet no Brasil. **Oficina da Net**, 2018. Disponível em: https://www.oficinadanet.com.br/artigo/904/o_comeco_da_internet_no_brasil. Acesso em: 28 out. 2019.

NETO, J. A. M. Aspectos Constitucionais e Legais do Crime Eletrônico. **Universidade de Fortaleza - UNIFOR**, Fortaleza - CE, p. 92, mar. 2008.

SANTOS, L. S. D. **Jornal do Tocantins**, 2019. Disponível em: https://www.jornaldotocantins.com.br/editorias/vida-urbana/mais-de-600-crimes-cibern%C3%A9ticos-foram-registrados-no-to-em-2018-conscientiza%C3%A7%C3%A3o-deve-ser-refor%C3%A7ada-1.1723888. Acesso em: 14 nov. 2019.

SILVA, L. W. Internet foi criada em 1969 com o nome de "Arpanet'' nos EUA. **Folha de São Paulo**, 2001. Disponível em: https://www1.folha.uol.com.br/folha/cotidiano/ult95u34809.shtml. Acesso em: 24 out. 2019.

SOARES, B. D. S. O Ordenamento Jurídico e os Crimes Virtuais. **Universidade Federal da Paraíba**, Campina Grande - PB, 2016.

STORE, H. Eniac: Conheça a incrível história do primeiro computador do mundo. **Blog HD Store**, 2018. Disponível em: https://blog.hdstore.com.br/eniac-primeiro-computador-do-mundo/. Acesso em: 23 out. 2019.

TAVARES, A. L.; REIS, R. R. D. Crimes de Informática. **Revista Jurídica**, Anápolis - GO, v. 2, jan. - jun. 2014.

TOCANTINS. Diário Oficial. **Decreto nº 5.979, de 12 de agosto de 2019**, 2019. Disponível em: https://central3.to.gov.br/arquivo/466882/. Acesso em: 05 jun. 2020.

TOCANTINS, G. **G1**, 2018. Disponível em: https://g1.globo.com/to/tocantins/noticia/pf-faz-operacao-contra-hackers-no-tocantins-e-em-mais-tres-estados.ghtml. Acesso em: 14 nov. 2019.
VIDAL, R. D. M. Crimes Virtuais. **Universidade Candido Mendes**, Rio de Janeiro, 2015.

ZULIANI, Ê. S. et al. **Responsabilidade Civil na Internet e nos demais Meios de Comunicação**. 2. ed. São Paulo - SP: Saraiva, 2012.