A ACELERADA EVOLUÇÃO SOCIAL E TECNOLÓGICA GLOBAL COMO VIABILIZADORES DE CRIMES CIBERNÉTICOS, FRENTE AO LENTO DESENVOLVIMENTO DE FREIOS LEGAIS PARA SUA CONTENÇÃO.

Antônio Luciano Bairros Ceron[1]
André Lemuel Ferreira Krieguer[2]
Aldair Marcondes[3]

Recebido em 01/12/2021
Aceito em 20/12/2021

RESUMO
O presente estudo pretende compreender como a legislação penal brasileira tem tratado os crimes cibernéticos. Vivemos a chamada era do conhecimento, onde a globalização juntamente com a tecnologia, transformaram profundamente a sociedade. Embora essa transformação, em sua maioria, tenha vindo para beneficiar a sociedade de uma maneira geral, infelizmente esta evolução proporcionou novas formas de criminalidade. Com o aumento dos crimes cibernéticos, a sociedade se viu diante de uma lacuna não preenchida para combater tais violações. Se fez necessário o surgimento de normas especificas na esfera penal, para tratar desta nova modalidade de crime. Neste trabalho se buscará compreender como anda a legislação brasileira no tocante do assunto, visando identificar quais os pontos já estão regulados e quais ainda necessitam de uma melhor normatização. No cenário atualmente vivido, o assunto tem se tornado cada vez mais relevante e, de uma maneira geral, de interesse de toda a sociedade brasileira.
PALAVRAS-CHAVE: Evolução Tecnológica, globalização, crimes cibernéticos.

THE ACCELERATED GLOBAL SOCIAL AND TECHNOLOGICAL EVOLUTION AS FEASIBILITIES OF CYBER CRIMES, IN FRONT OF THE SLOW DEVELOPMENT OF LEGAL BRAKES FOR THEIR CONTAINMENT

ABSTRACT
This study aims to understand how Brazilian criminal law has dealt with cyber crimes. We live in the so-called knowledge era, where globalization together with technology has profoundly transformed society. Although this transformation, for the most part, has come to benefit society in general, unfortunately this evolution has provided new forms of crime. With the increase in cybercrime, society faced an unfilled gap to combat such

[1] Acadêmico do curso de Direito na Universidade Alto Vale do Rio do Peixe (UNIARP). E-mail: alucianoceron@gmail.com
[2] Acadêmico do curso de Direito na Universidade Alto Vale do Rio do Peixe (UNIARP). E-mail: andrelfkrieguer@gmail.com
[3] Professor do curso de Direito da Universidade Alto Vale do Rio do Peixe (UNIARP). E-mail: aldair@uniarp.edu.br

violations. The emergence of specific rules in the criminal sphere was necessary to deal with this new type of crime. In this work, we will try to understand how Brazilian legislation is doing in relation to the subject, aiming to identify which points are already regulated and which still need a better standardization. In the scenario currently experienced, the subject has become increasingly relevant and, in general, of interest to all Brazilian society.
Keywords: Technological evolution, globalization, cyber crimes.

1. INTRODUÇÃO

A globalização junto com a internet nos trouxe muitos meios para a difusão de informações e conhecimentos diversos, como modelo de comunicação na sociedade contemporânea, podemos enviar, e receber qualquer coisa em questão de segundos, uma sociedade que trabalha em uma velocidade mais rápida que antigamente.

No atual âmbito social estamos todos conectados, e para que isso funcione com ordem, precisamos se prevenir e obter segurança em uma rede que às vezes pode ser instável ao ponto de vista jurídico, onde que muitas vezes os direitos individuais podem ser violados, e são violados constantemente por crimes que ainda não existem uma punição exata e concisa.

Reconhecidos atualmente como uma visão deturpada chamados de Hackers, porém devemos distinguir uma definição de outra, onde que os Hackers – White Het´s são programadores, desenvolvedores, que se encarregam de conhecimentos mais aprofundados e extensos de arquitetura de redes e estruturação do mesmo.

Por outro lado há os Crackers – Black Hat´s, traduzido como aquele que quebra que são os reais criminosos, reconhecidos por usar seu conhecimento para quebrar o sistema, violá-lo e divulgar informações sigilosas sem a permissão de seu respectivo dono, sendo assim violado o direito de privacidade da vítima.

Como acrescenta Milagre (2016) A "sociedade da informação", para muitos, tem, de certa forma, seus riscos, podendo ser chamada atualmente de sociedade dos riscos. Riscos que podem ser aceitos e riscos que devem ser aplacados, e um desses riscos está associado a criminalidade digital. Ao que pode acrescentar, que nem todo o cidadão decidiu adentrar no universo digital, mas foi totalmente imposto a ele, assim sendo uma presa fácil nas mãos de Crackers, especialistas em crimes cibernéticos, que exploram as informações dos sistemas e também dos processos desenvolvidos no meio da tecnologia da informação, pendendo para a prática de delitos.

Um mundo onde os crackers são os mais fortes, em uma posição social de poder e muitas

vezes não penalizados por seus atos, onde que a tecnologia demonstra um enorme poder aos programadores, profissionais de segurança, ou a qualquer um que se aprofunde em estudos informáticos, sendo o grande problema apenas o uso deste poder para más finalidades, sendo necessário atualmente a educação digital, que na maioria dos países não se aplica nas escolas.

Com base nesse contexto, a presente pesquisa buscará abordar uma visão histórica e voltada a área jurídica visando analisar as ações de indivíduos que usam da internet como um meio para a invasão da privacidade resultando em um dano a integridade humana.

2. DIREITOS HUMANOS E LEGISLAÇÃO DE CRIMES CIBERNÉTICOS EXISTENTES

Assegurado pelos direitos humanos, inclusive no artigo 5º da Constituição Federal Brasileira, onde são encontrados 77 incisos, e dois parágrafos e o caput, onde nele são garantidos os direitos à vida, liberdade, moradia, segurança. Além de a liberdade de escolha, todo cidadão pode recorrer a justiça, quando necessário for, sem ser oprimido pela mesma.

> 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 (...)

Os Direitos fundamentais como a liberdade, igualdade, segurança e privacidade, são constantemente violados no mundo todo através da internet como o principal meio para se realizar os chamados crimes cibernéticos. E apesar do Marco Civil, da internet com a Lei Carolina Dieckmann (Lei 12.737 de 2012), tais infrações não são devidamente punidas, com a severidade dos fatos, pois tal lei não é apta, por si só, para conduzir de maneira eficaz e solucionar os crimes cibernéticos de forma geral, já que no seu contexto, não existem órgãos de seguranças especializados para esse tipo de crime, evidentemente há uma necessidade da inclusão do Direito Eletrônico como uma legislação específica, com a finalidade de prosseguir com os crimes específicos desta área de forma mais efetiva.(LIMA;TESSMANN;VENTURIN, 2018)

Com o foco nos crimes cibernéticos é evidente que os seus resultados muitas vezes causam danos irreparáveis ao ser humano, principalmente em questões morais, crimes como, assédio moral, bullying cibernético, pornografia infantil, difamação, entre outros crimes que constantemente são cometidos no mundo inteiro, os chamados hackers, crackers, ou até mesmo aquele que utiliza a internet como meio ilícito para se obter a sua vingança tanto desejada,

muitas vezes não recebem a pena apropriada, pois o Direito Penal Brasileiro não se encontra totalmente preparado para esse tipo de delito.

Além de que para buscar as soluções para essa problemática dos crimes de informática, na contemporânea, há a necessidade da adaptação dos princípios constitucionais que norteiam o Direito Penal como um todo, como exemplo o Princípio da Legalidade, previsto no art. 5º, inciso XXXIX, da Constituição Federal, segundo o qual "[...] não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal". (MATA;SANTAGATI, 2013).

A interpretação desta lei, incluindo-a dos Direitos cibernéticos e Penais, nos leva a concluir que os delitos nos meios da informática devem ser específicos com o fim de individualizar o comportamento do criminoso, quando na prática da pena não se obtém nenhuma garantia real ou efetiva que conceba ao criminoso pelo seu ato.

Como resultado, o Direito Penal, necessita de esclarecer os detalhes do Crime para que se torne válido e eficaz, não cabendo, entretanto, uma lei genérica devendo identificar a conduta delituosa de forma detalhada evitando, assim, a ameaça de direitos individuais.

3. TEORIA TÉCNICA, COMPORTAMENTO E CRIME

O Brasil atualmente adota o princípio da Legalidade, ou seja, não há crime sem lei anterior que o define, assim evitando muitas vezes injustiças no sistema jurídico, porém em relação aos crimes cibernéticos a técnica para criar leis deveria ser outra em visão de Juristas, e atuantes da tecnologia da informação.

> Neste contexto, há muito tempo se cobrava uma legislação no Brasil que cuidasse de crimes eletrônicos. Tal mora pode ser atribuída também ao péssimo modo de se legislar sobre o tema adotado no Brasil que, por vezes, tentou condenar técnicas informáticas (ao invés de condutas praticadas por diversas técnicas), técnicas estas que são mutantes, nascem e morrem a qualquer momento, de acordo com a evolução dos sistemas, novas vulnerabilidades e plataformas tecnológicas. Para isso apresentamos uma proposta de sistematização e que deve ser considerada quando se legisla sobre crimes informáticos. Nominamos a proposta de TCC – Técnica, Comportamento e Crime. A proposta é detalhada na sequência. (MILAGRE; JESUS, 2016, p.26).

Como referência de grandes autores e influenciadores da área de Direito informático, em sua obra chamada Manual de Crimes informáticos, José A. Milagre e Damásio de Jesus, abordam uma nova forma de tipificar os crimes informáticos, pela proposta chamada TCC (Técnica, Comportamento e Crime).

Por muitos anos, a legislação anda a passos atrasados em relação a tecnologia, por vez novas tecnologias surgem, e com elas novas técnicas também nascem, com diferentes intuitos, podendo eles ser bons, ou maus.

3.1 TÉCNICA

A palavra técnica em sua tradução, se refere a um conjunto de procedimentos ligados a uma arte ou ciência, podendo ser eles exercidos através de métodos, procedimentos, através de softwares ou algum processo informático que pode caracterizar um comportamento distinto, podendo ela ser tanto manual, ou automatizada.

Em exemplo do legislador, ao equiparar o cartão de débito ou crédito ao documento particular abordando sobre a falsificação de documentos (Lei n. 12.737/2012), interpretando ao pé da letra, que sem o documento particular se torna impossível realizar a conduta "falsificar". Sendo assim o legislador foi específico ao objeto, que hoje em dia, há inúmeros documentos que não se encontram materialmente e sim digitalmente, ou qualquer meio posterior.

Logo, segundo Milagre e Jesus (2016), "alguém que falsifica um documento que está contido em um suporte *token* ou pendrive, pelos princípios penais, praticaria fato atípico", limitando-se assim ao objeto do comportamento de forma imprudente, podendo equiparar o documento particular a informações, declarações eletrônicas estando ou não em suporte material, de qualquer tipo de natureza.

3.2 COMPORTAMENTO OU CONDUTA

De acordo com a teoria finalista a conduta para o direito é o fato típico, ou seja, a conduta é a ação ou omissão que produz um resultado reprovável pelo Direito Penal, podendo ser crime ou contravenção penal. Sendo seus elementos a conduta, resultado, nexo causal e tipicidade.

Começando pela conduta, segundo Welzel (apud LEITE, 2017), é a "ação humana é exercício de atividade final, ou seja, dirige a sua conduta sempre à determinada finalidade", a ação, por sua finalidade, baseia-se no que o homem pode prever dentro de certos limites, as consequências possíveis de sua conduta, sendo assim, a conduta se distingue em ação, omissão, e comissivo por omissão.

Partindo ao segundo ponto, a conduta dolosa, ocorre quando o agente quer o resultado e assume o risco de produzi-lo (art. 18, I, Código Penal).

Sendo ela dividida pela vontade ou dolo direto, quando o agente quer o resultado, e o assentimento ou dolo eventual, quando o agente assume o risco de produzir o resultado.

E por último a conduta culposa, quando o agente produz uma conduta mas não queria o resultado, mas objetivamente previsível, sendo um comportamento voluntário e desatencioso, voltado a um determinado objetivo, lícito ou ilícito, produzindo um resultado ilícito, não desejado, porém previsível, que por sua vez podia ser evitado. Dolo é regra, a culpa exceção (LEITE, 2017).

Resumidamente, a conduta para a teoria "TCC", é uma ação realizada por meio de uma ou mais técnicas, cometida por um ou mais agentes, por ação ou omissão, por meios tecnológicos, redes de computadores, dispositivos informáticos, etc…

Como exemplo da técnica "sql injection", o agente praticou o comportamento de "invasão de sistema informático", porém analisando quais foram os resultados de sua conduta e sua real intenção. (MILAGRE; JESUS, 2016)

3.3 CRIME

Por fim, o que define crime para os atuantes da Tecnologia da Informação, seria um ou vários comportamentos, que utiliza uma ou várias técnicas, podendo ser praticada por apenas um agente, ou até mesmo vários, ofendendo assim um ou mais bens ou objetos jurídicos protegidos pelo Direito. Como exemplo citado de invasão de sistema informático, pode ser ou não considerado crime, dependendo do país em que é praticado, e da sua real finalidade.

Segundo a sistematização de Milagre e Jesus (2016), não se pode legislar sobre técnica, qualquer uma dessas tentativas resulta em uma legislação pouco eficaz, que não produz a verdadeira justiça, com rápida obsolescência, tornando apenas o Direito mais esparso e sem uma norma racional e ampla necessitando criar ramificações de diversas leis.

> Este pode ser, data venia, um dos principais erros de grande parte dos doutrinadores e legisladores sobre o tema: confundirem técnica com conduta. A falta de apoio técnico – especialistas em tecnologia e segurança da informação, em setores legislativos – leva o legislador brasileiro à criação de tipos penais incoerentes. (MILAGRE; JESUS, 2016, p. 28)

Ao se legislar sobre os crimes informáticos, não se poder começar pela análise de técnicas, definindo tipos penais, mas analisando as condutas que podem ser incriminados, que são realizadas de diversas formas (técnicas), e que merecem a consideração do Direito Penal Brasileiro, pois por muitas vezes uma técnica pode ser integrante de uma ou mais

condutas penalmente, porém nem toda a técnica é um comportamento interminável.

4. DEFINIÇÃO DE CRIMES CIBERNÉTICOS

2 Na doutrina brasileira dominante os "crimes cibernéticos são como delito de natureza formal, posto que se consumam no momento da prática da conduta delitiva, independente da ocorrência do resultado naturalístico". (ALMEIDA e AZEVEDO 2015, p.13).

> Trata-se de crime comum (aquele que pode ser praticado por qualquer pessoa), plurissubsistente (costuma se realizar por meio de vários atos), comissivo (decorre de uma atividade positiva do agente: "invadir", "instalar") e, excepcionalmente, comissivo por omissão (quando o resultado deveria ser impedido pelos garantes – art. 13, § 2º, do CP), de forma vinculada (somente pode ser cometido pelos meios de execução descritos no tipo penal) ou de forma livre (pode ser cometido por qualquer meio de execução), conforme o caso, formal (se consuma sem a produção do resultado naturalístico, embora ele possa ocorrer), instantâneo (a consumação não se prolonga no tempo), monossubjetivo (pode ser praticado por um único agente), simples (atinge um único bem jurídico, a inviolabilidade da intimidade e da vida privada da vítima) (MAGGIO 2013, apud ALMEIDA e AZEVEDO 2015, p. 13).

Ainda os crimes virtuais dividem-se em próprio e impróprio.

Nos crimes virtuais próprios elencam-se os crimes praticados pelos criminosos através do uso de todo o sistema digital disponível seja ele físico ou em rede. Nesta modalidade, os agentes infratores se utilizam de computadores ou sistemas de terceiros (invasão), como meio para execução dos crimes. Através deles são acessados hardwares, softwares, ou dados armazenados no computador, com intuito de modificar, alterar, sequestrar ou danificar os mesmos, visando algum lucro ou proveito particular (ALMEIDA e AZEVEDO 2015).

3 Já os crimes virtuais impróprios, os criminosos se utilizam de computadores ou sistemas para cometer ilícitos de bem jurídico já tutelado. Estes crimes já estão tipificados no Código Penal, e a utilização dos meios digitais (máquinas e redes) é apenas uma forma de viabilizar a ocorrência destes crimes, e "se difere quanto a não essencialidade do computador para concretização do ato ilícito que pode se dar de outras formas e não necessariamente pela informática para chegar ao fim desejado como no caso de crimes como: pedofilia" (ALMEIDA e AZEVEDO 2015, p. 10).

5. LEGISLAÇÃO ESPECÍFICA

O Brasil ainda não tem uma legislação tão abrangente e efetiva, mas dispõe ao menos de duas normas específicas de nºs 12.737/12 e 12.965/14.

5.1 LEI CAROLINA DIECKMANN

Vitoriano (2018) nos fala que com o avanço do uso da tecnologia da informação nos últimos tempos, o mundo jurídico precisou incluir no Código Penal os crimes ocorridos no universo virtual.

Assim, conforme Vitoriano (2018), foi sancionada a Lei dos Crimes Cibernéticos (Lei nº 12.737/12), conhecida como Lei Carolina Dieckmann (atriz famosa que teve seus dados roubados na internet), que tipifica os atos de invadir computadores, roubar senhas e dados, divulgando informações particulares na rede.

Com a Lei Carolina Dieckmann começou a ser penalizado mais efetivamente os infratores dos crimes cibernéticos. As sanções passaram a ser aplicadas como a detenção que pode chegar até em dois anos de reclusão, com vários agravantes, como os prejuízos de ordem econômica causado por ataques de infratores cibernéticos, nem como o vazamento de informações na internet de informações sigilosas, dados de segredo comercial ou ainda ligações comerciais privadas. (PINHEIRO e HAIKAL, 2016 *Apud* COSTA e PENDIUK, 2018).

Os autores são mais específicos ao mencionar:

> A Lei n. 12.737/2012 (Carolina Dieckmann), à luz do Código Penal Brasileiro (1988), em seu art. 266, estabeleceu o tipo penal de invasão aos sistemas de informação ilegítima, ampliando o crime de indisponibilização dos serviços públicos, equiparando o cartão magnético ao documento particular para que a falsificação de cartões de débito/crédito se torne punível, porém, o tipo penal exige requisitos para configurar crime (COSTA e PENDIUK, 2018. p. 11).

Segundo Costa e Pendiuk (2018), a Lei Carolina Dieckmann permitiu que os usurários das plataformas digitais e serviços de informática, de um modo geral, passassem a ter uma proteção contra hacker mal-intencionados que tem por objetivo apenas cometer algum dano contra estes usuários, seja por sequestro de dados e informações ou ainda pela alteração de informações de grande valia tanto de uso pessoais bem como de grandes corporações públicas ou privadas.

As sanções aplicadas aos delinquentes digitais fizeram com que as empresas passassem a ter uma maior proteção jurídica contra espionagem digital. Mas vale a ressalva que os usuários também passam a ser responsáveis pela proteção de seus dispositivos a fim de não facilitar a ação dos criminosos do mundo virtual (PINHEIRO e HAIKAL, 2016 *Apud* COSTA e PENDIUK, 2018).

5.2 MARCO CIVIL DA INTERNET

Conforme explicação de Martins (2015), a Lei 12.965/14, denominada de Marco Civil da Internet, é quem regula os direitos e deveres dos internautas, estabelecendo assim os princípios e garantias que rege a relação entre usuários e as empresas provedoras do acesso e serviços de internet.

O referido autor diz ainda que dentre as inovações, tal lei permite a retirada de circulação daqueles conteúdos que causem danos a terceiros. Essa retirada de conteúdos danosos é feita mediante ordem judicial.

Acerca do MARCO CIVIL destaca-se:

> O Marco Civil da Internet foi idealizado como uma carta que definisse os princípios-chave da internet e as regras de proteção aos seus usuários, estabelecendo condições mínimas e essenciais para tanto. A iniciativa do projeto foi da Secretaria de Assuntos Legislativos do Ministério da Justiça em parceria com o Centro de Tecnologia e Sociedade da Escola de Direito da Fundação Getúlio Vargas no Rio de Janeiro.13 Ambos estabeleceram um processo *aberto, colaborativo e inédito*14 para o desenvolvimento de suas normas, visto que seu principal "elemento de inspiração foi a Resolução de 2009 do Comitê Gestor da Internet no Brasil (CGI.br) intitulada *Os princípios para a governança e uso da Internet* (Resolução CGI.br/RES/2009/003/P)." (CGI.BR, 2014). O texto legal foi construído e colocado uma vez mais na plataforma para debate público, entre abril e maio de 2010. Vale ressaltar que o Marco Civil funcionou como uma iniciativa pioneira na ideia de uma democracia expandida. Ele promoveu um amplo debate racional entre os diversos atores que participaram de sua elaboração. No processo de consulta, foram considerados não apenas os comentários formalmente feitos por meio da plataforma oficial, mas também todos aqueles mapeados por meio de redes sociais (como o Twitter), posts em blogs e qualquer outra forma de contribuição que pudesse ser identificada online. Uma vez concluída a redação do texto final, pelo Ministério da Justiça e pelo time de professores da Fundação Getulio Vargas, com base nos comentários públicos recebidos, o texto foi então analisado no âmbito governamental mais amplo[...] (LEMOS, 2014 apud CANCELIER e PILATI, 2017, p. 11).

Costa e Pendiuk (2018), mencionam que o a chamada Lei do Marco Civil da internet teve algumas peculiaridades, como a grande participação da população tanto em fóruns de discussão promovidos na Internet, bem como em consultas públicas promovidas pelo nosso Congresso Nacional.

Pode-se assim observar:

> Um dos temas abordados pela Lei, gerador de debates, é a responsabilidade civil, por divulgar conteúdos em rede. A Lei envolve diversos deveres aos controladores de sites, que devem remover os conteúdos caso haja denúncia, quando devida, traz o dever de indenizar aos que sofreram danos decorrentes de sua publicação, além da guarda de registros de atividades no ambiente digital de sua propriedade (HAIKAL, 2016 *Apud* COSTA e PENDIUK, 2018, p. 4).

O Marco Civil da internet teve várias implicações no trato dos assuntos relacionados aos conteúdos digitais, inclusive na velocidade do tráfego de dados disponibilizados nas redes.

> O mundo digital é largamente afetado com a promulgação da Lei do Marco Civil da Internet, cuja pretensão é proteger e garantir maior privacidade e maior liberdade ao internauta enquanto usuário dos serviços. ” Nesse sentido, o autor afirma que o Marco Civil da Internet tratou do princípio da neutralidade de rede, o qual consiste em garantir igualdade no tráfego de dados, em cujo ambiente todos devem ter acesso igualitário às informações veiculadas e disponibilizadas, seja pelo próprio agente ou por terceiros, sem preferência ao direito. (PINHEIRO 2016 *Apud* COSTA e PENDIUK, 2018, p. 5).

Um fato destacado por Costa e Pendiuk (2018) é que embora o Marco Civil pregue pelo uso com responsabilidade do uso do princípio de liberdade de expressão, ainda é encontrado algumas dificuldades em se remover os conteúdos ofensivos e uma forma rápida. Assuntos envolvendo conotação sexual no ambiente virtual de menores de 18 anos aparados pelo ECA (Estatuto da Criança e Adolescente), tem prioridade quase que instantânea para ser retirado do ar, inclusive com plataforma específica online para denúncia e tomadas de mediadas urgentes. As demais ocorrências as publicações para serem retiradas das plataformas digitais, necessitam de requerimento direcionado ao Juiz, que analisará tais informações, decidindo ou não para retirada dos conteúdos das plataformas que se encontram.

Seguindo o pensamento os autores destacam:

> O mundo digital existe para todos, devendo o internauta repensar na publicação e compartilhamento dos conteúdos considerados abusivos. Na atualidade, vive-se na era digital, um mundo que exige transparência e pela impossibilidade de escondê-los, pois além dessas informações se espalharem muito rapidamente, existem inúmeros meios para rastreá-los, sem anonimato. O Marco Civil da Internet representa um passo importante na proteção de valores na era digital, embora, ainda haja muito o quê fazer nesse campo (PINHEIRO 2016 *Apud* COSTA e PENDIUK, 2018, p. 5)

Vale ressaltar que a tecnologia por si só não causa prejuízos, muito pelo contrário, veio para revolucionar a vida da humanidade e nos dias de hoje é impossível de se imaginar o mundo sem as inovações promovidas pela tecnologia. A forma como ela é utilizada, bem como as intenções dos seus usuários faz com que muitas vezes a tecnologia seja tratada como vilã. O Marco Civil da Internet veio com a finalidade de regular o mundo digital, criando princípios que visam a segurança pública dos usuários das plataformas digitais. Além de proteger o cidadão de uma forma mais direta, legislando e punindo os infratores digitais, o Marco Civil busca promover a conscientização dos usuários diretos para que os mesmos sejam peças chaves nos combates aos criminosos digitais. Segurança e prudências são necessárias em todos os níveis da sociedade (PINHEIRO 2016 *Apud* COSTA e PENDIUK, 2018).

6. A DIFICULADADE EM SE CRIAR FREIOS PARA CRIMES CIBERNÉTICOS

Segundo Nunes e Madrid (2019), dentre as dificuldades para se criar freios na esfera penal para conter os crimes virtuais, deve-se destacar a competência para julgar estes crimes, visto que é necessário determinar o tempo e o local do crime, que pode ocorrer inclusive fora do Brasil e afetar os usuários aqui estabelecidos.

Além do mais, segundo os mesmos autores, nossa Lei não consegue acompanhar o desenvolvimento quase que frenético dos crimes relacionados ao ambiente virtual. A todo momento surgem dispositivos novos, ferramentas virtuais atualizadas, gerando uma nova possibilidade de crime virtual. Eis então um grande impasse em nossa legislação. Não se pode punir alguém, sei norma anterior que defina o crime praticado, sendo assim como uma nova conduta do agente infrator, o mesmo se torna impune, pois ainda não existe regulamentação sobre tal crime.

No mesmo sentido Padovez e Prado (2019) vem contribuir com o assunto. O sentimento de impunidade que cerca os ambientes virtuais, são sentidos tanto pelos usuários que se sentes desprotegidos ao utilizar as plataformas digitais, bem como pelos delinquentes que se encorajam a praticar os crimes devido ao anonimato que os protegem. Os órgãos repressores ao cometimento destes crimes, sejam eles judiciários ou mesmo investigativos, sentem a falta de leis mais específicas para combater os mesmos, sendo assim muito difícil a identificação e punição dos criminosos.

Sobre o tema verificasse ainda que:

> O Direito em si não consegue acompanhar o frenético avanço proporcionado pelas novas tecnologias, em especial a Internet, e é justamente neste ambiente livre e totalmente sem fronteiras que se desenvolveu uma nova modalidade de crimes, uma criminalidade virtual, desenvolvida por agentes que se aproveitam da possibilidade de anonimato e da ausência de regras na rede mundial de computadores. (PINHEIRO, 2009 apud DULLIUS, 2012, [n.p.], apud ALMEIDA e AZEVEDO, 2015, p. 9).

O Estado muitas vezes tem o seu interesse de agir pautados em meras inclinações políticas e não efetivamente relacionado a importância relativa as garantias e proteções aos cidadãos. Infelizmente esse cenário também é aplicado no direito virtual e sua regulamentação, influenciando diretamente na forma dos criminosos em agir nos meios cibernéticos, onde a lacuna deixada pela demora ou falta de ação do Estado acaba tornando propício dos crimes e sua propagação em ambiente virtual (ALMEIDA e ROQUE, 2017).

Pinheiro (2016), faz uma importante reflexão acerca do tema:

> [...]o ciberespaço vulnerável, pois grande parte das autoridades públicas e líderes empresariais não tratam da segurança digital como prioridade absoluta na pauta de estratégias de seus país. No entanto, esse amadorismo, por um lado e grupos armados e profissionais, de outro, estão se organizando a cada dia (PINHEIRO 2016 *Apud* COSTA e PENDIUK, 2018, p. 15)

Diante do exposto acima, nota-se a necessidade de um plano comum, envolvendo diversos países, bem como a iniciativa privada e pública, onde deveria ser formado um compromisso onde ações conjuntas fossem tomadas por todos com intuito de reprimir de maneira global os ciberterroristas, os todas as nações e entidades poderiam fazer uma troca de informações e, tecnologias e ferramentas proporcionando assim um alcance de nível mundial no combate dos criminosos digitais. (PINHEIRO 2016 *Apud* COSTA e PENDIUK, 2018)

7. CAMINHOS PARA REPRESSÃO DOS CRIMES CIBERNÉTICOS

A impunidade no ciberespaço gera um ambiente propício para propagação de delinquentes virtuais. "Os criminosos virtuais aproveitam da fragilidade das leis, a ausência de fronteiras e da tecnologia para se manterem nas práticas delitivas. De modo que surge a necessidade de novos operadores da era digital". (ANDRADE, 2015 *Apud* ALMEIDA E ROQUE, 2017)

Os autores destacam ainda que a carência de profissionais com conhecimento de como agir na área de crimes cibernéticos, acaba se tornando mais uma barreira para coibir tais atos. O pouco conhecimento de procuradores, promotores e até juízes, faz com muitos crimes fiquem impunes, "pois, quando não possuem muito conhecimento desta tecnologia ficam mais inseguros por medo de cometer algum ato abusivo em relação ao direito de privacidade. " (MELO, 2008 *Apud* ALMEIDA E ROQUE, 2017)

A efetivação do acordado na Convenção de Budapeste de 2001, é a maneira mais eficiente de alcance global para frear os crimes cibernéticos. Mas a falta de adesão dos países a mesma, inclusive o Brasil, é um entrave para o seu sucesso. (ALMEIDA e ROQUE 2017).

Em suma a Convenção de Budapeste de 2001 consiste em:

> [...] persiste a necessidade de estabelecer normas globais e padrões para reger a conduta e comportamento no mundo virtual. Apesar da necessidade, as políticas nacionais e regionais podem colidir com essa normatização global. Isto exige regulamentação universal ou global considerando o impacto transnacional e arrebatador inerente do cybercrime. Apesar da dificuldade intrínseca na harmonização ou unificação de políticas criminais e penais, sendo uma manifestação de poder soberano e autoridade, as participações no ciberespaço têm instigado os Estados a trilharem por uma nova época de cooperação em matéria de direito penal e público território irregular e vacilante. [...] O objetivo principal da Convenção é harmonizar a legislação penal material e procedimentos de investigação internas. Eram duas as principais preocupações dos redatores da Convenção: a primeira era assegurar que as definições fossem flexíveis a ponto de se amoldar aos novos tipos de crimes e seus métodos e a segunda era manter-se sensível aos regimes jurídicos dos Estados-nação. Estas preocupações foram especialmente desafiadoras na área de direitos humanos, porque os estados têm diferentes valores morais e culturais. Por exemplo, os países europeus têm um grau muito mais elevado de proteção da privacidade do que os Estados Unidos (CHAWKI; WAHAB, 2006, apud ALMEIDA e ROQUE 2017, p. 3).

Além do mais, Almeida e Roque (2017), a regulamentação do Direito Virtual, passa muitos pelos interesses e recursos empregados pelo Estado, que pode influenciar positivamente ou negativamente na redução dos crimes virtuais, de acordo com o interesse de agir do Estado.

Como já visto anteriormente, o anonimato concedido aos criminosos virtuais e digitais é o principal dificultador da normatização jurídica que vise combater os crimes por eles praticados. São várias as tangentes proporcionadas aos mesmos e por mais que se busque o controle jurídico é muito difícil de se chegar de formar rápida e conciso a estes tipos de criminosos. Essa falta de normatização faz muitas vezes o acesso positivo a informação ser comprometido, como por exemplo o acesso a diversos bancos de dados disponíveis para o uso público, que engrandeceria muitos estudos e pesquisas. Sendo assim, fica evidente que não basta combater condutas delinquentes no meio digital. Se faz necessário a efetiva punição através de uma regulamentação forense mais efetiva e célere. (ALMEIDA e ROQUE, 2017).

8. CONSIDERAÇÕES FINAIS

Diante do exposto, é possível se compreender que a tecnologia que veio para suprir várias necessidades da sociedade atual, passa também por um processo fraudulento causado por malfeitores do mundo digital, os quais se utilizam de formas criminosas para se apoderar de informações privadas e lesar outras pessoas.

Nesse contexto, a legislação brasileira busca conter esses criminosos, fazendo com que as penas a eles impostas diminuam a ocorrência desta forma de delito. O contraponto é que as penas e as leis não acompanham a celeridade das novas tecnologias e os novos crimes que a cercam.

O fato é que no Brasil, por mais que se tenha alguma normatização, a legislação para estes delitos ainda é incipiente, ou seja, ainda está engatinhando na busca de resultados efetivos frente à dificuldade de identificação dos autores de crimes cibernéticos.

Portanto o interesse de agir do Estado é fundamental para a diminuição da sensação de impunidade no ambiente virtual. Este interesse do agir do Estado vai desde a regulamentação e capacitação de profissionais específicos para combater tais ilícitos até uma maior celeridade na elaboração de Leis que venham coibir os crimes no ambiente virtual.

REFERÊNCIAS

ALMEIDA, Jéssica de Jesus *et al.* **Crimes Cibernéticos**. Ciências Humanas e Sociais Unit-Aracajú - Sergipe, 2015.

ALMEIDA, Julia da Silva; ROQUE, Braynner Victor Silva. **Desafio do direito na regulamentação das relações jurídicas na deep web e dos crimes cibernéticos**. Escola Superior Dom Hélder Câmera. Belo Horizonte – Minas Gerais, 2017

BRASIL. **Constituição da República Federativa do Brasil (1988)**. São Paulo: Saraiva, 2010.

CANCELIER, Mikhail Vieira de Lorenzi, PILATI, José Isasc. **PRIVACIDADE, PÓS-MODERNIDADE JURÍDICA E GOVERNANÇA DIGITAL: O exemplo do marco civil da internet na direção de um novo direito**. Universidade Federal de Santa Catarina. Florianópolis – Santa Catarina, 2017.

COSTA, Roberto Renato Strauhs; PENDIUK Fábio. **DIREITO DIGITAL: O marco civil brasileiro da internet e as inovações jurídicas no ciberespaço**. Universidade Federal do Paraná. Curitiba – Paraná, 2016.

FACHIN, Odília. **Fundamentos de Metodologia**. São Paulo: Saraiva, 2003.

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica**. São Paulo: Atlas, 2003.

LIMA, Alecssandro Moreira. **Crimes Virtuais – O cyberbullyng, o código penal brasileiro e a lacuna vigente**. 2018.

LIMA, Ueslei de Melo Rodrigues de; TESSMANN, Dakari Fernandes; VENTURIN, Edileuza Valeriana de Farias. **Violação dos Direitos Fundamentais em Crimes Cibernéticos e a Necessidade de Inclusão do Direito Eletrônico como Legislação Específica**. Disponível em: <http://www.ienomat.com.br/revista2017/index.php/judicare/article/view/85>. Acesso em: 10 ago. 2020.

NUNES, Mário Vinicius de Azevedo; MADRID, Fernanda de Matos Lima. **CRIMES VIRTUAIS: O desafio do código penal na atualidade e a impunidade dos agentes**. Centro Universitário Antônio Eufrásio de Toledo. Presidente Prudente – São Paulo, 2019.

MARINHO, Guilherme. **Hackers, Crackers e o Direito Penal**. Disponível em: <https://grmadv.jusbrasil.com.br/artigos/407334629/hackers-crackers-e-o-direito-penal>. Acesso em: 09 ago. 2020.

MATA, Leonardo André da; SANTAGATI, Claudio Jesus. **Analogia aos delitos virtuais com ênfase nos Direitos Humanos.** Disponível em: <http://revistas.cua.ufmt.br/revista/index.php/revistapanoramica/article/view/436/119> Acesso em: 10 ago. 2020.

MARTINS, Geisa. **O que é o Marco Civil da Internet?** Disponível em: < https://super.abril.com.br/mundo-estranho/o-que-e-o-marco-civil-da-internet//>. Acesso em: 21 de jun. de 2020.

PADOVEZ, Rafael Silva; PRADO, Florestan Rodrigo. **O direito penal brasileiro no contexto dos crimes cibernéticos.** Centro Universitário Antônio Eufrásio de Toledo. Presidente Prudente – São Paulo, 2019.

VITORIANO, Larissa. **A Lei Carolina Dieckmann atua contra Crimes Virtuais e Possui Grande Influência Midiática.** Disponível em: < https://cpjur.com.br/lei-carolina-dieckmann/>. Acesso em: 21 de jun. de 2020.