

UNILEÃO
CENTRO UNIVERSITÁRIO
CURSO DE GRADUAÇÃO EM DIREITO

SHELLDON DE SOUSA SANTOS

A LEGISLAÇÃO PENAL NA ERA DOS CRIMES DIGITAIS

JUAZEIRO DO NORTE - CE
2020

SHELLDON DE SOUSA SANTOS

A LEGISLAÇÃO PENAL NA ERA DOS CRIMES DIGITAIS

Trabalho de Conclusão de Curso apresentado
à coordenação do Centro Universitário
Leão Sampaio como requisito para a
obtenção do título de Bacharel em Direito.
Orientador: Francisco José Martins Bernardo
de Carvalho

JUAZEIRO DO NORTE – CE

2020

SHELLDON DE SOUSA SANTOS

A LEGISLAÇÃO PENAL NA ERA DOS CRIMES DIGITAIS

Trabalho de Conclusão de Curso apresentado à coordenação do Centro Universitário Leão Sampaio como requisito para a obtenção do título de Bacharel em Direito.

Aprovado em: ____ / ____ / 2020.

BANCA EXAMINADORA:

(Orientador)

(Examinador)

(Examinador)

JUAZEIRO DO NORTE - CE
2020

RESUMO

Com a evolução da internet, das redes sociais e da tecnologia é comprovado seus benefícios relacionados a praticidade de seu uso, a liberdade de expressão sem pudores, e a alta conectividade com todos no mundo, são visíveis e necessários e necessitam de cuidados específicos uma vez que esse impulso crescente na sociedade gera, em muitos casos, a possibilidade real de práticas de crimes cibernéticos. Nesse contexto se faz necessário repensar o papel do Direito, da constituição e das leis aplicáveis para esses atos ilícitos e seus desafios para sanar de forma eficaz esse cibercrime. Visto isso, o artigo tem anseio e objetiva mostrar e analisar, de forma breve, alguns aspectos relevantes no fenômeno acerca dos crimes cibernéticos em nosso país, observando a debilidade do ordenamento jurídico e a jurisprudência das leis para essas condutas criminosas. Para isso a metodologia utilizada no processo de construção do artigo, foi baseada na pesquisa da bibliográfica já existente sobre o tema abordado, na internet, sites confiáveis do ambiente jurídico e plataformas de pesquisas. Conclui-se que apesar das evoluções nesse contexto, o Brasil se apresenta deficiente no que se trata da legislação que pune e aplica as leis envolvidas diretamente nas questões de crimes virtuais, sendo necessária mais preocupação e dedicação para sanar esse problema crescente no meio social, uma vez que estamos cada vez mais ligados ao ambiente virtual e suas facilidades.

Palavras-chave: Crimes Digitais; Legislação Penal; Direito;

ABSTRACT

With the evolution of the internet, social networks and technology, its benefits as to the practicality of its use, freedom of expression without shame, and high connectivity with everyone in the world, are visible and necessary and need specific care since this Increasing momentum in society generates, in many cases, the real possibility of cybercrime. In this context, it is necessary to rethink the role of the Law, the constitution and the applicable laws for these illegal acts and their challenges to remedy this cybercrime. In view of this, the article is eager to show and analyze, in a brief way, some relevant aspects in the phenomenon about cyber crimes in our country, observing the weakness of the legal system and the jurisprudence of the laws for these criminal conduct. For this, the methodology used in the article construction process was based on the research of the existing bibliography on the topic addressed, on the Internet, reliable sites in the legal environment and research platforms. It is concluded that despite the developments in this context, Brazil is deficient in terms of the legislation that punishes and applies the laws directly involved in issues of cyber crimes, requiring greater concern and dedication to solve this growing problem in the social environment, since we are increasingly connected to the virtual environment and its facilities.

Keywords: Digital Crimes; Penal Legislation; Right;

1 INTRODUÇÃO

A evolução tecnológica, em especial a internet, e sua influência essencial dentro da sociedade é um assunto bastante discutido e de grandes repercussões na atualidade. Para além de seus benefícios é necessário discutir sobre o que esse desenvolvimento e facilidades de acesso na modernização global, e suas implicações negativas desse processo de crescimento social.

Algumas implicações negativas podem advir dessa evolução digital, no que se relaciona aos crimes de internet, que crescem a cada ano, bem como, a sensação de impunidade devido à ausência de uma legislação mais eficaz para esses crimes, e a eficiência nas questões de julgamento e execução das penas criminais e cíveis.

É percebido diariamente o aumento das escalas de crimes virtuais, o surgimento cada vez maior de meios alternativos e dispositivos, com cada vez mais especificidade e ousadia por parte dos criminosos, gerando repercussões diretas na vida das vítimas, seja psicologicamente, socialmente, patrimonial e etc.

Em estudos de Trentin (2012) se percebe que a comunicação virtual entre as pessoas se acentua de uma forma jamais vista, o que, de maneira positiva, contribui para o fenômeno da globalização na medida em que cria novas oportunidades às práticas comerciais, novos relacionamentos, velocidade e acesso irrestrito à informação entre outras vantagens. Por outro lado, cresce também a utilização desse importante meio tecnológico para a prática de atos ilícitos

Fagundes (2017) discorre que o aumento na ocorrência desse tipo de crime diariamente, e ao contrário do que muitas vezes se imagina, as repercussões não são apenas em face do particular, outras consequências desses atos criminosos podem se refletir nas questões de caráter econômico e político de um país.

De acordo com Sydow (2014) o Estado democrático tem o dever de garantir a seus cidadãos o desenvolvimento pacífico e a coexistência de semelhantes em igualdade de condições, agindo como mantenedor da ordem social. Nesse sentido, acaba por interferir na nova sociedade de informação, no chamado meio ambiente virtual, elaborando normativas que impõem limites à internet e à troca de informações por meio da tecnologia.

O autor acima afirma ainda que os crimes de âmbito virtual devem ser analisados sobre diversas perspectivas devido a suas grandes peculiaridades como não haver contato físico entre os agressores, ocorre em um ambiente sem povo,

governo ou território, além de não gerar, a princípio, sensação de violência para um segmento social específico não havendo padrões para o seu acontecimento.

Visto isso, o artigo apresentado objetiva esclarecer o que são os crimes de cunho digital e como estes delitos influenciam a vida em sociedade, e suas repercussões em âmbito jurídico, buscando aperfeiçoar e especificar a legislação que rege esses crimes virtuais no Brasil, de maneira que seja eficiente no processo de punição aos responsáveis por esses atos.

No desenvolver do trabalho serão abordados conceitos e alguns tipos mais comuns de delitos na internet. Buscará seguir desenvolvendo a legislação que representa e pune esse tipo de crime, bem como a necessidade de aperfeiçoamento dessas leis sobre esses crimes, objetivando explicar alguns aspectos relevantes no fenômeno acerca dos crimes cibernéticos em nosso país, observando a debilidade do ordenamento jurídico e a jurisprudência das leis para essas condutas criminosas.

2 METODOLOGIA

Mediante a necessidade de entender melhor e adequar o tema às normas e legislações existentes, o artigo foi modulado a partir de pesquisas bibliográficas, através de artigos, páginas na internet que tenha relevância acadêmica de forma a analisar textos existentes que cumpram com a necessidade do artigo e permeie todos os assuntos abordados, sendo a temática bem construída com bibliografia, não sendo necessário pesquisa de campo.

3 CRIMES DIGITAIS

Hodiernamente o ambiente social está relacionada, em sua grande maioria, aos aparelhos digitais e a tecnologia da internet, mensagens, aplicativos de interações sociais, e-mails, vídeos, todo aparato tecnológico que facilita a vida das pessoas.

O Direito é diretamente afetado pela movimentação tecnológica, Trentin (2012), explica que devido a adesão das pessoas no processo tecnológico cada vez mais crescente, é inerente que se haja sua regulamentação para que as relações

evoluam e passem a ser desenvolvidas em ambiente virtual, possibilitando relacionamentos horizontais e não hierárquicos entre os participantes e bom desenvolvimento social.

Apesar das vantagens adquiridas com esse processo de evolução digital é sabido que o processo de criminalidade nesse ambiente virtual vem aumentando consideravelmente e muitos usuários utilizam-se dessa conectividade mundial como uma porta para a prática ilícita desse recurso.

Com a popularização da Internet em todo o mundo, milhares de pessoas começaram a se utilizar deste meio. Contemporaneamente se percebe que nem todos a utilizam de maneira sensata e, acreditando que a internet é um espaço livre, acabam por exceder em suas condutas criando novas modalidades de delito: os crimes virtuais. (CONTE, 2016, p. 183).

Trentin (2012) afirma que o avanço tecnológico é essencial para a vida das pessoas, e um dos fatores primordiais na movimentação do direito, onde sua principal característica são as inúmeras possibilidades de aberturas para relacionamentos em todos os âmbitos, entre os usuários, sendo necessário, portanto, uma eficiente regulamentação para que essas relações sejam bem desenvolvidas e não haja conflitos nem crimes virtuais.

Para Viera (2012) o crime cibernético se aplica quando há qualquer conduta culpável condenada pelo meio jurídico, ou seja, são condutas típicas, antijurídicas e culpáveis, praticadas utilizando sistemas de informática com seu auxílio ou contra seus sistemas de informática e de comunicação.

Sydow (2014) enfatiza que é dever do Estado democrático de direito, do Direito Penal a garantia de que sua população, dentro do ambiente virtual, tenha um desenvolvimento pacífico e a coexistência de semelhantes em igualdade de condições, agindo como mantenedor da ordem social, impondo limites reais à internet e à troca de informações por meio da tecnologia.

Os crimes digitais apresentam diversas características distintas, sem contato físico direto, sem local preciso em um ambiente sem povo, governo ou território, sem padrões para seu acontecimento, o que dificulta a aplicabilidade de leis para esses atos, visto isso, é importante que a análise desse tema seja feita através de variadas perspectivas buscando diminuir a sensação de impunidade relacionada com esses delitos.

3.1 Conceito

O crime como uma ação ou omissão que se proíbe e se procura evitar, ameaçando-a com pena, porque constitui ofensa (dano ou perigo) a um bem jurídico individual ou coletivo constituindo um desvalor social. Os crimes digitais representam delitos comuns, mas com realização de condutas ilícitas, antijurídicas que envolvam, diretamente, o uso da tecnologia, internet, computadores, do sistema de informação eletrônico.

Estudos de Monteiro (2017) conceituam esses crimes virtuais como atividades que utilizam a rede e o computador para praticar crimes e facilita-los, estando interligados mundialmente em alta conectividade e rapidez, eles também podem ser denominados de crimes digitais, crimes eletrônicos, cibercrimes, crimes cibernéticos.

A definição de crimes cibernéticos é feita por Silva (2016) como um delito de computador que envolva a atuação humana se caracterizando antijurídico, culpável e como fato típico no direito penal, onde o uso desse recurso prejudicou de forma direta outras pessoas ou favoreceu o infrator.

“delito informático” poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade. (ROSSINI, 2004, p. 110.).

Representam todas as condutas previstas em lei que sejam punidas com pena criminal e cuja prática envolva aparatos tecnológicos, seja porque a conduta destina-se contra os sistemas informatizados e contra dados, seja porque o meio tecnológico foi utilizado, embora o crime pudesse ser praticado de outra forma.

Conte (2016) explica que a criminalidade dentro do ambiente virtual tem como uma das características principais um nível de informatização global, e transnacional já que na atualidade quase todos os países fazem uso de sistema informacional online, dessa maneira fica mais possível a pratica de um ato ilícito penal em qualquer lugar da sociedade mundial.

3.2 Tipos de crimes virtuais

É sabido que o mundo virtual se apresenta de maneira convidativa para a sociedade, possibilitando um mundo irreal onde as distâncias são encurtadas, a vida se apresenta mais fácil e a conexão parece ser mais verdadeira, dito isso é de extrema urgência que nesse ciberespaço sejam protegidos os direitos e garantias fundamentais da população.

Siqueira (2017) divide os crimes cibernéticos em duas partes, os que se relacionam como próprios, onde as práticas ilícitas objetivam atingir um sistema informático ou seus dados violando sua confiabilidade, sua integridade e/ou sua disponibilidade, e as condutas impróprias que também são culpáveis, mas que poderiam ter sido praticadas por outros meios que não fossem apenas os virtuais.

De acordo com estudos de Pinheiro (2014) os ciber crimes mais comuns no ordenamento jurídico brasileiro, de caráter mais recorrente, e considerados impróprios, são os que ferem a honra pessoal, as ameaças, discriminações, fraude, falsidade ideológica, onde a possibilidade de anonimato facilita a prática dessas contraversões.

Sobre os crimes de natureza imprópria Crespo (2015) discorre que esses crimes não apresentam diferença significativa no modus operandi, mesmo que seja diferente o modo de ação delitiva não há necessidade real de conhecimentos técnicos para a sua prática, já nos crimes considerados de caráter próprio, dependem diretamente de entendimento específico sobre informática e sua aplicabilidade.

Complementando o autor citado acima, Almeida (2016) descreve os crimes em ambiente virtual próprios como aqueles onde a prática ilícita se utiliza do sistema informático do sujeito passivo, no qual o computador como sistema tecnológico é usado como objeto e meio para execução do crime. Pode ser utilizado como exemplo dessas práticas criminosas, a invasão a dispositivos e interceptação informática, como por exemplo, a invasão de computador ou celular para o roubo de dados ou informações pessoais.

O centro de Estudos, Resposta e Tratamento de Segurança do Brasil (cert.br) no ano de (2016), elucida que os crimes próprios de maior ocorrência no Brasil são os relacionados aos de segurança em rede, "scan", classificados como notificações de varreduras em redes de computadores, com o intuito de identificar quais

computadores estão ativos e quais serviços estão sendo disponibilizados por eles, permitindo associar possíveis vulnerabilidades aos serviços habilitados em um computador.

A maior dificuldade na prática desses delitos em ambiente jurídico, seria obter de forma efetiva sua conceituação dentro do judiciário sendo fatigante para a legislação penal, uma vez que, o crescimento e a evolução da tecnologia agem de forma célere deixando, em muitos casos, desatualizado os processos penais e produzindo lacunas constitucionais que levam a impunidade nesses crimes tecnológicos.

4 LEGISLAÇÃO E COMPETÊNCIA

O dinamismo que envolve todo o ambiente da internet injunge ao meio legislativo e aos legisladores que se desafiem com intuito de conter as práticas delitivas cometidas nesse ambiente virtual, que são heterógenas e mutáveis, e afetam pessoas, organizações, negócios colocando em dúvida a segurança e credibilidade dos mesmos perante a sociedade.

Filho (2016) discorre que o convívio humano na rede mundial de computadores sofre diuturnamente alterações, sobretudo em razão da criação de novos aplicativos, novos dispositivos e novas funções já existentes, daí a dificuldade em enquadrar condutas perante a legislação já existente desafiando o cotidiano das forças investigativas e do poder judiciário, por sua vez estes elementos constantemente se reportam ao legislativo para aprimoramento do conjunto normativo.

A legislação relacionada aos crimes virtuais ainda é recente, até o ano de 2012 não se mencionava punições e leis voltadas para esses delitos e apenas após episódios de ataques a sites do governo e a divulgação de fotos íntimas da atriz Carolina Dieckmann, duas leis foram sancionadas com maior urgência, a Lei 12.735/201215, conhecida popularmente como “Lei Azeredo”, e a Lei 12.737/201216, conhecida como “Lei Carolina Dieckmann”.

Souza (2017) destaca também a importância da Lei 12.965/2014, conhecida como Marco Civil da Internet, sancionada pela ex-presidente Dilma Rousseff, sendo responsável por regular e estabelecer princípios, garantias, direitos e deveres para o seu uso, para os usuários e também para o próprio Estado. Devido a sua grande

aplicabilidade tributária, e eficiência, serve de incentivo e modelo para legislações fora do Brasil, em resposta aos crimes cibernéticos.

Para além dessas legislações ainda se apresentam na nossa legislação a lei de combate a pornografia infantil na internet Lei nº 11.829/2008; a Lei nº 9.609/1998, que trata da proteção da propriedade intelectual do programa de computador; a Lei nº 9.983/2000, que tipificou os crimes relacionados ao acesso indevido a sistemas informatizados da Administração Pública; a Lei nº 12.034/2009, que delimita os direitos e deveres dentro da rede mundial, durante as campanhas eleitorais.

Um dos grandes desafios legislativos está em identificar os praticantes ativos dos delitos virtuais, Siqueira (2017) explica que as nuances tecnológicas facilitam a fuga e a ocultação dos autores dos crimes, principalmente em função do grande número de usuários da internet e das inúmeras possibilidades dentro dessa rede virtual. Mesmo com os avanços ao combate da criminalidade virtual a legislação vigente ainda apresenta falhas consideráveis deixando a desejar em vários aspectos, restando muito a ser feito quanto a criminalidade digital.

Pinheiro (2013) explica que apesar dos crimes tecnológicos no ambiente virtual ainda serem escassos de legislação específica eles se encontram tipificados em textos legislativos já existentes como o Código Penal e legislação esparsa onde a grande novidade para o Judiciário se apresenta no modus operandi, de como o criminoso tem feito uso das novas tecnologias, levando assim aos aplicadores do Direito e a legislação uma renovação de pensamentos e ações penais.

Outro problema no enfrentamento desses delitos virtuais, se relaciona com a falta de capacitação dos profissionais diretamente responsáveis pelo combate desses crimes virtuais, sendo necessário que estejam em constante atualização de suas funções, assim também, os poucos órgãos destinados ao combate desses crimes e a dificuldade em serem criadas mais leis que evoluam com as condutas ilícitas realizadas.

Lima (2014) defende que a melhora nos cumprimentos sobre os crimes cibernéticos se dará através de investigações com maior rapidez na expedição e celeridade na efetividade dos mandados, e por parte da perícia que identificará o delito cometido, bem como, a união entre as forças da segurança pública e o aperfeiçoamento no legislativo.

4.1 Lei 12.735/12 – “Lei Azeredo”

Resultante de um longo processo legislativo, cuja origem remonta ao Projeto de Lei nº 84 de 1999, proposto pelo Deputado Federal Luiz Piauhyllino. Referido projeto de lei originalmente continha dezoito artigos que geraram bastante polêmica, sendo a maioria deles subtraída pelo seu Relator, o Deputado Federal Eduardo Azeredo, cujo sobrenome tornou-se o nome extraoficial da Lei n. 12.735, que foi sancionada em 2012, bem como outros dos artigos aprovados receberam o veto da então Presidente da República Dilma Rouseff.

Wendt (2017) explica que essa lei é responsável por coibir a prática dos crimes informáticos, sendo sancionada, no ano de 2012, e oriunda do projeto de lei da Câmara dos Deputados de nº 84 de 1999, com objetivo de incluir diversas tipificações no Código Penal, mas que não foram aprovadas; entretanto, a expertise da polícia judiciária foi incluída após substitutivo oriundo do Senado Federal. Tramitando por longos treze anos e após diversas modificações, submeteu-se o aludido projeto de lei à sanção presidencial.

O autor menciona ainda que essa lei modificou algumas disposições da Lei de Crimes Raciais, atribuindo discricionariedade ao magistrado para que este, antes até mesmo do inquérito policial, possa ordenar que cesse a exibição de imagens ou símbolos que façam alusão a qualquer esfera de discriminação.

O artigo 4 é citado por Colli (2015) como o responsável por criar órgãos que fossem especializados no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado, uma vez que a maioria desses crimes virtuais se inicia com a localização dos computadores, onde ocorreram os atos delituosos necessitando então de técnicas específicas e mais eficácia na apreensão desses delitos.

Lima (2014) complementa comentando que essa norma trouxe uma perceptível violação a preceitos constitucionais, mais especificamente o disposto no artigo 5º, LVII da Carta Magna, “ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória”. Nesse contexto, é dever do Estado proceder com todas as fases, desde denúncia até processamento e julgamento, além de esperar pelo trânsito em julgado da condenação para, então, aplicar efeitos penais e extrapenais.

Outra contribuição dessa lei, foi a alteração do Código Penal, De acordo com Crespo (2015), foi determinado que os órgãos da polícia judiciária deveriam criar

delegacias especializadas no combate aos crimes digitais. Entretanto, as delegacias criadas até o momento não estão totalmente preparadas para atender as vítimas dos cibercrimes.

Sanches (2018) critica a lei citada e a falta de uma legislação específica aos crimes cibernéticos no Brasil, onde ainda são percebidos lacunas e dúbias interpretações, o que ocasiona em inúmeros casos a saída impune dos criminosos. O autor indaga a necessidade de criação de leis que definam e cumpram as penas destinadas aos crimes digitais.

4.2 Lei 12.737/12 – “Lei Carolina Dieckmann”

Apesar dessas normas não apresentarem grande diferença nas reformas do ordenamento jurídico, foi através dessa lei que muitos avanços no combate a criminalidade virtual foram desenvolvidos, criando novos tipos incriminadores além de servir como referência para debates sobre a inovação no Judiciário. Antes do advento dessa legislação, não havia dispositivo legal que efetivamente tipificasse tal conduta como crime; não havia outra opção senão a impunidade.

O crime de invasão de dispositivo informático pode causar prejuízos inestimáveis à vítima, pois sendo crime que atenta contra a liberdade individual e a privacidade, pode causar a exposição pessoal por meio do roubo de informações ou outros dados sigilosos, como ocorreu com a atriz Carolina Dieckmann que deu nome a referida lei quando seu celular foi invadido e fotos íntimas, sem seu consentimento, foram vazadas na rede virtual.

De acordo Almeida (2016) a principal alteração da referida lei foi a inovação do ordenamento jurídico brasileiro por meio da tipificação de um novo tipo penal: a invasão de dispositivo informático, por meio da inclusão do Art. 154-A no Código Penal onde 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.

Ainda em seu artigo 154-A, no § 1º, foi feita uma comparação entre o praticante do crime de invasão e a pessoa que recebe e divulga esses dados sem consentimento da vítima incorrendo assim ato criminoso com aplicação de mesma pena judicial.

Outra mudança, como o autor citado salienta ainda é que essa lei trouxe a inclusão do conceito de crime de interrupção de serviço para incluir os serviços de informática, telemática ou de informação de utilidade pública através da alteração do Art. 266 do CP, agravando-se a pena por meio de sua aplicação em dobro caso o crime seja praticado por ocasião de calamidade pública (§ 2º).

Apesar das falhas jurídicas nesse texto normativo, ele se apresentou como uma evolução positiva no contexto de crimes virtuais, uma vez que, conseguiu tipificar algumas condutas danosas para a sociedade e para a privacidade da população, representando um primeiro contato voltado especificamente para a tutela do bem jurídico no mundo virtual e abrindo caminhos para as discussões importantes sobre o tema vigente no meio judiciário.

4.3 Lei Marco Civil da Internet (12.965/2014)

Fiorillo (2016) explica que essa lei foi responsável por regulamentar o uso da internet no Brasil, estabelecendo princípios, garantias, direitos e deveres a serem observados por provedores e usuários dos serviços de internet, sendo até considerado uma “constituição” representativa da internet, com sua tentativa de disciplinar toda a matéria existente sobre o uso da rede no território nacional a partir de princípios como da neutralidade, privacidade e liberdade de expressão.

O autor afirma ainda que esse advento foi debatido por mais de duas mil pessoas, com o intuito de nortear essa lei sobre a aplicabilidade e garantia de três pilares, para a sociedade, a liberdade, privacidade e neutralidade, onde juntos serão garantidores do cumprimento das normas estabelecidas pra o convívio civil, e a responsabilização dos provedores de serviços.

O objetivo dessa lei, para Fagundes (2017), é que ela pretendia prever as práticas criminosas no ambiente online, prezando assim pela neutralidade da rede, pela liberdade de expressão, e pela privacidade dos seus usuários, evitando que suas informações pessoais sejam vendidas ou ofertadas às empresas sem sua prévia autorização, além de assegurar o sigilo em suas comunicações.

Filho (2016) acrescenta que esse Marco Civil, atribuiu responsabilidade aos usuários das redes de internet sobre o conteúdo consumido/produzido, mesmo

instituindo a obrigatoriedade supra, cabendo assim ao provedor retirar material de circulação, podendo responder em várias esferas judiciais caso não o faça.

Mesmo atingindo seu objetivo em alguns aspectos legislativos essa lei ainda se apresenta de forma pouco eficaz, já que não se desenvolve com a mesma velocidade do mundo virtual sendo assim contra produtiva no processo de introduzir ferramentas judiciais do mundo físico, necessitando assim de maior celeridade e eficiência na sua prática penal.

4 CONSIDERAÇÕES FINAIS

O processo de globalização vem gerando crescimento de novas tecnologias, principalmente no ambiente virtual, e com isso impactos positivos nas tecnologias de informação, mas também originando novos meios que propiciam a prática de crimes virtuais, com o surgimento de novas práticas criminais, impulsionadas pela sensação de liberdade e anonimato que a rede de internet proporciona.

Viu-se que o Direito deve acompanhar de forma igualitária as mudanças tecnológicas aprimorando seus institutos, garantido a segurança jurídica da população nas relações com o ambiente virtual e o crescimento da internet, percebendo a necessidade vigente do meio Jurídico no tema abordado, combatendo diretamente os atos ilícitos ocorridos na área penal e a tipificação dos mesmos, com associação entre ordenamento jurídico brasileiro, verificando os desafios enfrentados nesse ambiente virtual, a eficácia da legislação que penaliza esses crimes diminuindo os atos que se tornam impunes.

Neste diapasão, foi constatado que ainda se apresentam muita impunidade, nos crimes cibernéticos, pelas falhas na regulamentação pela legislação brasileira, sendo primordial o desenvolvimento de leis específicas direcionadas para a reprimenda desses crimes, com criações de estatutos específicos para essas práticas, normatizando as situações atípicas de forma resoluta e eficaz.

Apesar de evoluções positivas sobre a legislação que envolve a aplicação de leis contra os crimes virtuais, o Brasil ainda está aquém do que realmente precisa e da demanda envolvida nesse processo virtual. As leis são esparsas que ainda não contemplam em totalidade o tema proposto, bem como ainda não se aperfeiçoou

códigos específicos e uma conceituação jurídica adequada para esses crimes cibernéticos.

A exiguidade de uma legislação específica que ampare e tenha resolutividade nas condutas atípicas em ambiente virtual reflete na dificuldade de enfrentar e punir de maneira eficaz essas práticas ilegais gerando repercussões graves em todo o âmbito social. Por se tratar de crimes variados e de recente surgimento, é necessário que haja uma multidisciplinaridade no combate a esses crimes virtuais, com a junção entre direito e informática aliados para melhor atuação nessa esfera criminal digital.

REFERÊNCIAS

ALMEIDA, J. et al. Crimes cibernéticos. **Periódicos Grupo Tiradentes**, v. 2, n.3. p. 215-236, 2016.

COLLI, M. Cibercrimes: limites e perspectivas à investigação policial de crimes cibernéticos. Curitiba: Juruá, 2015.

CRESPO, M. F. Crimes digitais. **Saraiva**. São Paulo, 2015, p. 94.

FAGUNDES, J. Crimes cibernéticos: aspectos legislativos e implicações na persecução penal com base nas legislações brasileira e internacional. **VirtuaJus**, v. 2, n. 2, p. 338-362, Belo Horizonte, 2017.

FIORILLO, C; CONTE, C. **Crimes no Meio Ambiente Digital**. 2. ed. São Paulo: Saraiva, 2016.

FILHO, E. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estud. av.**, São Paulo, v. 30, n. 86, p. 269-285, Abr. 2016.

LIMA, S. P. Crimes virtuais: uma análise da eficácia da legislação brasileira e o desafio do direito penal na atualidade. **In: Âmbito Jurídico**, Rio Grande, XVII, n. 128, set 2014.

MONTEIRO, Silvana Drumond. O ciberespaço: termo, a definição e o conceito. *Revista da Ciência da Informação*, v 8 n 3 jun/2017.

PIAUHYLINO, Luiz. PL 87/1999. Projetos de Leis e Outras Proposições, Câmara dos Deputados, disponível em:
<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=15028>.

ROSSINI, A. E. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, p.11^o, 2004.

SANCHES, A. Insuficiência das leis em relação aos crimes cibernéticos no Brasil. Jus.com.br, 2018.

SILVA, Aurélia Carla Queiroga; BEZERRA, Margaret Darling; SANTOS, Wallaz Tomaz. Relações Jurídicas Virtuais: Análise de Crimes Cometidos com o Uso da Internet. **Revista Cesumar Ciências Humanas e Sociais Aplicadas**. v.21, n.1, p. 7-28, jan./jun. 2016.

SIQUEIRA, M. S. et al. Crimes virtuais e a legislação brasileira. (Re)Pensando o Direito. **Rev. do Curso de Graduação em Direito da Faculdade CNEC Santo Ângelo**. v. 7, n. 13 (2017).

TRENTIN, Taise Rabelo Dutra; TRENTIN, Sandro Seixas. Internet: Publicações Ofensivas em Redes Sociais e o Direito à Indenização por Danos Morais. Revista Direitos Emergentes da Sociedade Global, Santa Maria, n. 1, jan./jun/2012.

WENDT, E CASELLI, G. Investigação Digital em Fontes Abertas. **BRASPORT Editora**. Rio de Janeiro. 2017.