doi.org/10.51891/rease.v8i11.7746

A FRAGILIDADE DO ORDENAMENTO JURÍDICO QUANTO AO CIBERCRIME: CRIMINOSOS POR TRÁS DE UMA TELA, VÍTIMAS EXPOSTAS EM SUAS VIDAS REAIS

THE FRAGILITY OF THE LEGAL ORDER REGARDING CYBERCRIME: CRIMINALS BEHIND A SCREEN, VICTIMS EXPOSED IN THEIR REAL LIVES

Alícia Castro Ramos[1]
Jackson Novaes Santos[2]

RESUMO: O presente estudo tem por objetivo identificar e contextualizar o fenômeno dos cibercrimes, apresentando os conceitos pertinentes. A era tecnológica chegou, e com ela a insegurança dos usuários com os crimes digitais. O tipo de pesquisa a ser utilizada no presente estudo será descritiva, tendo como base um levantamento de dados através das fontes: legislação brasileira e internacionais, artigos e notícias relacionadas ao Crime Digital; e fontes secundárias: serão feitas análises dos trabalhos de especialistas (artigos). Para tanto busca-se explanar as vulnerabilidades e as lacunas que o ordenamento jurídico vigente possui enquanto tal tema. No Brasil, o conceito de cibercrime é mais amplo, pois pode ou não estar conectado à internet. É inegável que a internet tornou-se parte de nossas vidas, mas, como se tem notado, essa segurança não é infalível e o conceito do cibercrime está fortemente em debate. A evolução dos meios digitais gerou oportunidades para novos tipos de condutas criminosas e a jurisprudência ainda não consegue acompanhar os mesmos, deixando assim grande fragilidade para a resolução da prática de tais delitos. A resolutividade para a problemática tem sido o uso das leis já existentes, e abordagem os direitos fundamentais reconhecidos pela Constituição Federal de 1988. Mas é evidente que apenas essas soluções não são inteiramente eficazes, sendo assim, havendo a necessidade da criação de novas leis protetoras e mais rigor nas fiscalizações das leis já existentes contra a fragilidade do usuário, que por ventura poderá transfigura-se no futuro em uma vítima.

Palavras-chave: Cibercrimes. Crime digital. Tecnologia. Vulnerabilidade.

[1]Discente do curso de Direito da Faculdade de Ilhéus, Centro de Ensino Superior, Ilhéus, Bahia.
[2]Docente do curso de Direito da Faculdade de Ilhéus, Centro de Ensino Superior, Ilhéus, Bahia.

ABSTRACT: This study aims to identify and contextualize the phenomenon of cybercrime, presenting the relevant concepts. The technological era has arrived, and with it the insecurity of users with digital crimes. The type of research to be used in this study will be descriptive, based on a survey of data through sources: Brazilian and international legislation, articles and news related to Digital Crime; and secondary sources: analyzes of specialist works (articles) will be carried out. Therefore, we seek to explain the vulnerabilities and gaps that the current legal system has as such a topic. In Brazil, the concept of cybercrime is broader, as it may or may not be connected to the internet. It is undeniable that the internet has become part of our lives, but, as has been noticed, this security is not infallible and the concept of cybercrime is strongly under debate. The evolution of digital media has generated opportunities for new types of criminal conduct and jurisprudence is still unable to keep up with them, thus leaving a large number of volunteers for resolving the practice of such crimes. The solution to problems has been the use of existing laws, and the approach to fundamental rights recognized by the Federal Constitution of 1988. But it is clear that only these solutions are not fully effective, therefore, there is a need to create new protected laws and more rigor in the inspections of existing laws against user compression, which may eventually become a victim in the future.

Keywords: Cybercrime. Digital crime. Technology. Vulnerability.

INTRODUÇÃO

A integração e à amplificação da internet otimizou a troca de informações, o alcance do espaço virtual tem tomado proporções imensas, conjuntamente ao aumento da quantidade de usuários. A presente pesquisa possui como objetivo examinar a ocorrência dos crimes cibernéticos, exaltando os perigos causados por um regramento insuficiente sobre tal temática.

Um grande problema ainda reside no rastreamento dos infratores, tendo em vista que a busca pelos indivíduos infratores se torna extremamente difícil, pois por vezes o autor do crime reside em outro país ou mascara seu endereço do Protocolo de Internet para diversos servidores tornando difícil ter conhecimento da sua localização. Sendo que as dificuldades não param por aí.

São muito comuns os crimes cometidos na internet relacionados tanto à pessoa, como injúria, calúnia, difamação, ameaça, crime de falsa identidade, divulgação de material confidencial, ato obsceno, apologia ao crime e estupro virtual, quanto à ataques cibernéticos,

como aqueles promovidos por hackers que ao se utilizarem de vírus, infectam computadores de usuários e empresas e logo em seguida solicitam dinheiro em troca dos dados sequestrados, tal qual violação de sistemas de segurança.

Atualmente um dos grandes combates do Direito é garantir aos usuários a proteção no ambiente virtual. Por isso é importante a prevenção e cuidado sobre como é divulgado e exposto informações pessoais, pois, por mais simples e inocente pareça ser, a mesma pode usada de diferentes formas para obter dados que possibilitam os crimes cibernéticos. É fundamental obtermos conhecimento sobre quais os crimes mais comuns cometidos por esses infratores e as leis que buscam conferir proteção jurídica às pessoas expostas a esses delitos.

A Lei de crimes cibernéticos nº 12.737/12, trouxe para o ordenamento jurídico penal brasileiro o novo crime de "Invasão de Dispositivo Informático", consistente na conduta de "invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com 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".

A Lei do Marco Civil, lei nº 12.965/14, garante e discute temas como a neutralidade da rede, proteção de dados, registro de conexão, responsabilidade por danos e também a necessidade de uma requisição judicial para ter acesso às informações. Isto é, toda e qualquer aplicação na Internet está garantida e sob responsabilização, porque o Marco Civil da Internet garante o exercício da cidadania nos meios digitais. A Lei Geral de Proteção de Dados nº 13.709/18, foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo.

A Lei fala sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado, englobando um amplo conjunto de operações que podem ocorrer em meios manuais ou digitais.

Os direitos fundamentais reconhecidos pela Constituição Federal de 1988 e a Emenda Constitucional (EC 115), que inclui a proteção de dados pessoais entre os direitos e garantias fundamentais. A importância dos direitos à privacidade e proteção de dados pessoais estar

elencado no art. 5º da Constituição Federal é que os direitos fundamentais são garantias com o objetivo de promover a dignidade humana e de proteger os cidadãos.

O direito à privacidade e à proteção de dados pessoais é essencial à vida digna das pessoas, principalmente nesse contexto de total inserção na vida digital. A Convenção sobre o Cibercrime adoptada em Budapeste em 23 de Novembro de 2001, a Convenção foi elaborada pelo Comitê Europeu para os Problemas Criminais, com o apoio de uma comissão de especialistas.

Foi o primeiro tratado internacional sobre os chamados cibercrimes. Até junho de 2021 tinha sido assinada por 66 países, além de usada por outros 158 como orientação para suas legislações nacionais.

2 REFERENCIAL TEÓRICO

2.1 O Conceito de Cibercrime

O aumento do alcance da rede mundial de computadores trouxe inúmeros benefícios, como também, vulnerabilidades para seus usuários. O nosso meio de vida foi modificado e antes os crimes que eram cometidos de forma física agora são praticados no meio virtual, prejudicando tanto quanto antes.

Devido sua constante evolução, os cibercrimes estão sempre acompanhando o seu ritmo e inovando, porém, a legislação tem dificuldades para acompanhar o mesmo. Com isso surge a problemática na proteção dos dados da comunidade. Cassanti (2014) afirma que:

> Toda atividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, base de ataque ou como meio de crime é conhecido como cibercrime. Outros termos que se referem a essa atividade são: crime informático, crimes eletrônicos, crime virtual ou crime digital (CASSANTI, 2014, p.03).

Em sentido amplo, a criminalidade informática engloba toda atividade criminosa realizada por computadores ou meios de tecnologia da informação. Em sentido stricto, a criminalidade informação engloba crimes, de acordo com Simas (2014), o meio informático surge como parte integradora do tipo legal, ainda que o bem jurídico protegido não seja digital.

A informática pode ser um instrumento de práticas de crimes tradicionais, isto é, que não necessitam de suporte informacional para serem realizados, nem sendo parte legal. A

este disso, podemos citar crimes cometidos a honra e a dignidade da pessoa humana, que podem ser cometidos com recurso em meio informático para divulgação (e-mail, redes sociais).

Outros casos que pode inferir são quando a informática surge como elemento integrador, isto é, podendo o bem jurídico protegido não ser unicamente com a informática, como é o caso de crimes contra softwares em que o bem jurídico protegido é autoral.

Cibercrimes são os delitos penais cometidos por meio digital ou que estejam envolvidos com a informação digital. Foi tipificado na lei nº 12.737/2012, que o conceitua, no art. 154-A como:

> 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 (BRASIL, 2012).

A nossa doutrina penal estabelece pena de detenção de 3 (três) meses a 1 (um) ano e multa. Além disso, a referida Lei adverte que a pena incorre quem produz, oferece, distribui, vende ou difunde dispositivos ou programas de computadores que tem por objetivo permitir a prática da conduta criminosa; se resulta em prejuízo econômico; e, se da invasão resulta obtenção do conteúdo.

A pena de reclusão repercute em 6 (seis) meses a 2 (dois) anos e multa, caso a conduta criminosa tornar-se grave. Ainda, aumenta-se a pena se atingir ou praticar contra a Administração Pública municipal, estadual ou federal. Os recentes ataques de hackers e vazamentos de dados pessoais de milhões de brasileiros chamaram a atenção para a urgência do combate aos cibercrimes.

O número de crimes virtuais cometidos pela internet vem aumentado de modo alarmante, segundo especialistas reunidos em audiência pública interativa na Comissão de Ciência e Tecnologia. A prática de crimes na internet assume várias denominações, entre elas, crime digital, crime informático, crime informático-digital, *high technology crimes, computer related crime*. Não existe consenso quanto à expressão, quanto à definição, nem mesmo quanto à tipologia e classificação destes crimes, contudo, atendendo aos diversos instrumentos legislativos, consideramos ser de especial interesse utilizar a denominação de cibercrime

2.2 A Fragilidade do Ordenamento Jurídico

O ordenamento jurídico brasileiro contemporâneo, apesar das existências dessas garantias já citadas na pesquisa, ainda não está preparado para assegurar a segurança jurídica necessária para a sociedade mediante os crimes no âmbito virtual.

A conjectura de estudar e analisar sobre cibercrimes, sua evolução e a conjuntura jurídica, diante desses estudos, capaz de transpor de forma célere os desafios que hoje o ordenamento jurídico brasileiro enfrenta ao reprimir os delitos virtuais. A Lei nº 12.737/12, conhecida como Lei Carolina Dieckmann, uma forma de tentativa do Estado de reprimir essas novas condutas praticadas no âmbito virtual, fez-se necessário à criação de tipos penais que ainda não eram previstos na legislação.

A Emenda Constitucional nº 115/2022, de relatoria da senadora Simone Tebet (MDB-MS), adiciona o direito à proteção de dados pessoais no rol de direitos e garantias fundamentais ao cidadão, além de fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

Isso permite que seja dada maior segurança jurídica ao país na aplicação da Lei Geral de Proteção de Dados Pessoais, atraindo ainda mais investimentos internacionais para o Brasil.

Apesar dos referidos direitos estarem garantidos pela legislação vigente, ainda existe lacunas legislativas que podem dificultar e até mesmo impossibilitar a aplicabilidade para o fim almejado, vindo a criar uma insegurança jurídica.

2.3 A Internet e o Cibercrime

Segundo o autor Cardozo (2017), a internet causou o surgimento de crimes cometidos tanto pelo meio virtual que atingem bens jurídicos tradicionalmente já tutelados no Código Penal, quanto aos crimes contra bens jurídicos novos, a saber os componentes dos dispositivos informáticos, seus dados e sistema, que têm legislação recentemente adotada para tutelá-los.

Ainda de acordo com o autor, é importante ressalvar que, os criminosos atuantes na área informatizada veem neste, uma nova forma de delinquir, devido ás vulnerabilidades deixadas pelos usuários desprovidos de conhecimentos técnicos, que se utilizam da

tecnologia informática para realizar as tarefas mais básicas e cotidianas sem precisar sair de casa (a exemplo do pagamento de contas), e que do mesmo modo, passam o dia conversando com amigos reais e virtuais por meio de sites mensageiros e redes sociais, mas normalmente não se preocupam na proteção de sua privacidades (CARDOZO, 2017).

E neste cenário, o mesmo autor afirma que essa vulnerabilidades deixadas pelos usuários, é que acabam permitindo ou até mesmo facilitando a vida dos criminosos, especialistas nesta área informatizada a faceta de cometer delitos na internet ou contra esta.

Importa-se também mencionar ainda que, os crimes efetuados pelo meio virtual poderão atingir várias cidades de um mesmo território, e até mesmo chegar a ultrapassar seus limites internos, atingindo outras nações, fato em que precisam de auxílio de todos os países atingidos pela prática delituosa, para que seja possível punir o criminoso (CARDOZO, 2017).

2.3.1 Cibercrime e a Legislação Brasileira

Com o fim da Segunda Guerra, diversas tecnologias foram criadas, desenvolvidas e aprimoradas, porém, por muito tempo, a acessibilidade a tais instrumentos era restrita ao uso militar. A Internet que conhecemos como um meio acessível à população surgiu na década de 90, vindo a se massificar a partir de então.

Há mais ou menos quinze anos que a Internet conquista rapidamente espaços cada vez maiores na sociedade. Em um momento inicial, chegou-se a acreditar que esse espaço fosse “terra de ninguém”.

Isso facilitou o cometimento de crimes online e o aparecimento de novos delitos, fazendo surgir o termo cibercrime. O direito, visando acompanhar as demandas que surgem na sociedade, busca regular esse ciberespaço que parecia tão abstrato e distante de nossa realidade.

Castro (2003) define o ciberespaço como o espaço de comunicação aberto pela interconexão mundial de computadores e das memórias dos computadores.

> O ciberespaço (que também chamarei de rede) é o mais novo meio de comunicação que surge da interconexão mundial de computadores. O termo especifica não apenas a infraestrutura material da comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo (CASTRO, 2003).

O princípio da legalidade e o princípio anterioridade da lei penal, com previsão legal no artigo 1º do Código Penal e na Constituição Federal de 1988 no artigo 5º, inciso XXXIX, o qual não há crime sem lei anterior que o defina, nem há pena sem prévia cominação legal.

> Em decorrência do princípio da legalidade ou da anterioridade da lei penal, a insuficiência ou a ausência de norma penal tipificando os crimes digitais limita a função punitiva estatal, uma vez que influencia na sensação de insegurança e impunidade, com repercussão negativa para a sociedade brasileira e, em especial, para a comunidade internacional, que há mais de uma década vem chamando a atenção para a necessidade e urgência de controle e prevenção de condutas delituosas no ciberespaço (WENDT; JORGE, 2013).

Desse modo, a legislação brasileira tem dificuldade em acompanhar a evolução tecnológica, pois a cada dia surge um novo delito nesse ambiente, do qual o legislador não é capaz de caminhar em paralelo com essas evoluções, e consequentemente os crimes virtuais não recebem as devidas punições, deixando a sensação de impunidade.

Lei Carolina Dieckmann é a Lei nº 12.737, é uma alteração no Código Penal Brasileiro voltada para crimes virtuais e delitos informáticos. Com o avanço da tecnologia e a democratização e o acesso facilitado às redes sociais, o sistema judiciário brasileiro viu a necessidade de tipificar crimes cometidos no ambiente virtual.

Seu projeto foi apresentado no dia 29 de novembro de 2011 e sua sanção se deu em 2 de dezembro de 2012 pela presidente Dilma Rousseff. Esse foi o primeiro texto que tipificou os crimes cibernéticos, tendo foco nas invasões a dispositivos que acontecem sem a permissão do proprietário.

Vale destacar que, em nosso país, é comum as leis levarem anos para serem aprovadas, mas, nesse episódio, ela foi sancionada por conta da pressão midiática após uma ocorrência com a personalidade famosa, o que fez com que seu processo de aprovação demorasse o período recorde de apenas um ano. A Lei nº 12.737/12 impacta o Direito Penal, pois acrescenta os artigos 154-A e 154-B ao Código Penal Brasileiro. Além disso, altera a redação dos artigos 266 e 298. A norma trata de uma tendência do Direito: segurança no ambiente virtual.

Sua redação prevê os crimes que decorrerem do uso indevido de informações e materiais pessoais que dizem respeito à privacidade de uma pessoa na internet, como fotos e vídeos. O primeiro artigo, 154-A, trouxe o crime chamado Invasão de dispositivo informático, que consiste na invasão de qualquer dispositivo informático alheio, como

computadores, smartphones, tablets etc., independentemente se estiver conectado à internet ou não.

O ato deve ser praticado mediante violação de mecanismo de segurança e ter o objetivo de adulterar, obter ou destruir dados sem autorização do proprietário do dispositivo. A norma também se aplica a quem instalar vulnerabilidades nos dispositivos para obter vantagens ilícitas.

Aquele que produzir, oferecer, distribuir, vender ou difundir um programa de computador ou dispositivo que permite a prática também sofrerá as consequências do crime. A ação desse crime procederá mediante representação, ou seja, o Ministério Público somente oferece a denúncia se o ofendido solicitar, exceto nos casos em que o crime for cometido contra a administração pública (direta ou indireta) ou seja, qualquer poder do governo municipal, estadual ou da União, como também empresas concessionárias de serviços públicos (TOURINHO FILHO, 2012).

A pena do crime de invasão de dispositivos é a de detenção entre 3 meses e 1 ano mais multa, mas há um aumento de 1/6 da pena caso resulte em prejuízos econômicos à vítima. Quando o crime resulta na obtenção de conteúdo de comunicações privadas, segredos comerciais ou industriais, controle remoto de dispositivos ou dados sigilosos, a pena será de reclusão de 6 meses a 2 anos mais multa, isso se o ato não constituir crime mais grave.

Nesse último caso, a pena ainda aumenta em 2/3 se houver transmissão, divulgação ou comercialização dos dados obtidos. Por fim, a pena pode aumentar de 1/3 até metade se o crime for praticado contra as seguintes autoridades:

- Prefeito, governador ou presidente da república;
- Presidente do Supremo Tribunal Federal (STF);
- Presidentes dos órgãos legislativos municipais, estaduais ou da União, como Senado Federal, Câmara Municipal, Câmara Legislativa etc.;
- Dirigentes máximos da administração municipal, estadual ou federal.

A Lei nº 12.965/14 do Marco Civil da internet, prevê como princípios que regulam o uso da internet no Brasil, enumerados no artigo 3º, dentre outros, o princípio da proteção da privacidade e dos dados pessoais, e asseguram, como direitos e garantias dos usuários de internet, no artigo 7º, a inviolabilidade e sigilo do fluxo de suas comunicações e

inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial.

O artigo 10º, § 1º, que trata de forma específica da proteção aos registros, dados pessoais e comunicações privadas, é bem claro quanto à possibilidade de fornecimento de dados privados, se forem requisitados por ordem de um juiz, e diz que o responsável pela guarda dos dados será obrigado a disponibilizá-los se houver requisição judicial.

Caso o responsável se recuse a fornecer os dados solicitados pelo juiz, poderá responder pelo crime de desobediência, previsto no artigo 330 do Código Penal (TJDFT, 2015). No Marco Civil, o legislador infraconstitucional pendeu para a liberdade de expressão por se tratar de lei cujo objeto se encontra diretamente vinculado à expressão humana e, portanto, ao aludido princípio. Não poderia a lei, todavia, refutar a primazia da dignidade da pessoa humana e de seus corolários. A igualdade, a integridade psicofísica e a solidariedade encontram na identidade de relevância com a liberdade e assim deverá ser feito na ponderação (TOURINHO FILHO, 2012).

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n° 13.709/2018, foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo. A Lei fala sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado, englobando um conjunto de operações que pode ocorrer em meios manuais ou digitais.

No âmbito da LGPD, o tratamento dos dados pessoais pode ser realizado por dois agentes de tratamento, o Controlador e o Operador. Além deles, há a figura do Encarregado, que é a pessoa indicada pelo Controlador para atuar como canal de comunicação entre o Controlador, o Operador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.

Tema principal da Lei, o tratamento de dados diz respeito a qualquer atividade que usa um dado pessoal na execução da sua operação, como, por exemplo: coleta, produção, recepção, classificação, armazenamento, eliminação, uso, acesso, reprodução, transmissão, distribuição, processamento, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2012).

A Emenda Constitucional nº 115/2022, acrescenta o direito à proteção de dados pessoais no rol de direitos e garantias fundamentais ao cidadão, além de fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

Isso permite que seja dada maior segurança jurídica ao país na aplicação da Lei Geral de Proteção de Dados Pessoais, atraindo ainda mais investimentos internacionais para o Brasil. A importância dos direitos à privacidade e proteção de dados pessoais estar elencado no art. 5º da Constituição Federal é que os direitos fundamentais são garantias com o objetivo de promover a dignidade humana e de proteger os cidadãos.

O direito à privacidade e à proteção de dados pessoais é essencial à vida digna das pessoas, sobretudo nesse contexto de total inserção na vida digital (BRASIL, 2012).

2.3.2 Cooperação Jurídica Internacional e o Brasil

Em 23 de novembro de 2001, ocorreu a Convenção sobre Cibercrimes na cidade de Budapeste, que entrou em vigor em 1º de julho de 2004. A Convenção trata-se de tipificar os crimes virtuais como infrações de sistemas; as infrações relacionadas aos crimes com computadores; os crimes que envolvem pedofilia; e as violações de direitos autorais. Ainda, trata da competência e cooperação internacional, deixando a critério das partes decidirem quem será a jurisdição mais apropriada para o procedimento legal (KAMINISKI, 2002).

Pode-se afirmar que a Convenção trata basicamente de harmonizar os crimes praticados no âmbito virtual e as formas de persecução. O Brasil adotou à Convenção no ano de 2021. A Convenção de Budapeste tem como objetivo facilitar a cooperação internacional para combater o cibercrime.

Elaborado pelo Comitê Europeu para os Problemas Criminais, com o apoio de uma comissão de especialistas, o documento lista os principais crimes cometidos por meio da rede mundial de computadores e foi o primeiro tratado internacional sobre crimes cibernéticos. Até junho de 2021 tinha sido assinada por 66 países, além de usada por outros 158 como orientação para suas legislações nacionais.

O governo federal considera que, embora o Marco Civil da Internet tenha criado importante estrutura legislativa para o combate aos crimes cibernéticos, os meios digitais não respeitam fronteiras. Por isso é necessário constante refinamento da cooperação e coordenação entre os países (CAPEZ, 2012).

Entre as questões acertadas na Convenção de Budapeste estão a criminalização de condutas, normas para investigação e produção de provas eletrônicas e meios de cooperação internacional. Em seminário feito pela Comissão de Ciência e Tecnologia, Comunicação e Informática da Câmara dos Deputados, o Ministério Público Federal (MPF) defendeu a urgência na aprovação do PDL para oficializar a adesão do Brasil.

O pedido foi feito pelo procurador da República George Lodder, que integra o Grupo de Apoio sobre Criminalidade Cibernética da Câmara Criminal do MPF. Na ocasião, ele ainda defendeu a inclusão, na legislação brasileira, da obrigação de sites e plataformas comunicarem os órgãos de persecução penal sobre caso de crimes praticados por seus usuários.

CONSIDERAÇÃOES FINAIS

Ao final deste trabalho, consegue-se constatar e perceber que existe uma ausência de reconhecimento sobre os cibercrimes, são poucos os autores que abordam especificamente sobre esse tema. Visto que há muito a ser explorado, mostra-se necessário conhecer aspectos jurídicos que envolvem e configuram o tema, visando assim, compreender a legislação existente e formular novas normas constitucionais que tratem especificamente sobre esse tema.

Atualmente, o crime digital não tem ganho a devida atenção, sendo tipificado por apenas algumas leis, sendo que, algumas não são nem especifica para o devido tema. Por essa razão, é necessário chamar a atenção para este ambiente, expondo uma serie de meios que permitam enxergar novas percepções sobre este problema que vem, a internet, embora tenha trazido benefícios, trouxe sérios prejuízos como a criminalidade virtual.

Desta feita, a legislação deve acompanhar essa evolução tecnológica com novos estudos, buscando solução a esses conflitos virtuais, pois, a nossa legislação permite que se faça tudo que a lei não proíbe, assim há a necessidade de punições para esses crimes. Cada vez mais assombrando os usuários da rede.

Surgiram assim instrumentos legislativos internacionais com o objetivo de harmonizar as legislações nacionais para combater eficazmente o cibercrime. Ficou demonstrado que fazer face a este fenómeno não é fácil e apenas se consegue com uma

cooperação internacional das entidades que investigam estes crimes, permitida pelas legislações nacionais, já harmonizadas e em consonância.

Até o presente momento tem-se leis de combates indiretos e as que possuem combates diretos foram criadas em momento de grande repercussão de um dano, os legisladores devem evoluir conforme o sistema criando leis preventivas, antes de atingir muitas pessoas.

Em conclusão, o ser humano está a cada dia q passa mais dependente da tecnologia, a legislação deve atender as necessidades dos usuários através de leis regulamentadoras do espaço virtual e tornar competentes os profissionais que estão trabalhando com o combate desses crimes, criando mecanismos para a segurança dos usuários, entre outros.

A legislação deve cursar o caminho junto com a evolução virtual, o Cibercrime nunca irá desaparecer, mas pode ser prevenido e combatido se a sociedade for instruída neste sentido.

REFERÊNCIAS

ALMEIDA FILHO, J.; CASTRO, A. **Manual de Informática Jurídica e Direito da Informática.** Rio de Janeiro: Forense, 2005.

ARAS, V. **Crime de Informática. Uma Nova Criminalidade.** Jus Naviga. Teresina, 2001.

BODIN DE MORAES, M. **O princípio da dignidade da pessoa humana. Na medida da pessoa humana.** Rio de Janeiro: Processo, 2016.

BRASIL. **Lei nº 12.737/12, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no** 2.848**, de 7 de dezembro de 1940.** Brasília, 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/212/lei/l12737.htm>. Acesso em: 16 Nov. 2022.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Ministério da Cidadania. Disponível em: <https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd>. Acesso em: 16 Nov. 2022.

BRASIL. **Marco Civil da Internet**. Tribunal de Justiça do Distrito Federal e dos Territórios. Disponível em: <https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/marco-civil-da-internet>. Acesso em: 16 nov. 2022.

CAPEZ, F. **Curso de Direito penal: Parte Geral**. 16 Ed. 2ª. São Paulo: Saraiva, 2012. Vol I.

CARDOZO, A. Competência nos Crimes Cibernéticos. São Paulo, 2017. Disponível em: ‹https://agianes.jusbrasil.com.br/artigos/514359859/competencia-nos-crimes-ciberneticos›. Acesso em: 17 Nov. 2022.

CASSANTI, M. **Redes de indignação e esperança: Movimentos sociais na era da internet.** Rio de Janeiro: Jorge Zahar, 2014.

CASTRO, D. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2003.

CASTRO, C. **Crimes de Informática e seus Aspectos Processuais.** 2º Ed. Ver, ampl e atual. Rio de Janeiro, 2003.

FOGLIATTO, J. **Os crimes cibernéticos e os meios que a polícia utiliza para a identificação dos criminosos.** Jus.com.br. Disponível em: ‹https://jus.com.br/artigos/77225/os-crimes-ciberneticos-e-os-meios-que-a-policia-utiliza-para-a-identificacao-dos-criminosos›. Acesso em: 25 Jun. 2022

KAMINISKI, O. **A informática Jurídica, a Juscibernética e a Arte de Governar.** Revista Consultor Jurídico. 2002. Disponível em: ‹http://www.conjur.com.br/2002-jul-17informatica_juridica_juscibernetica_arte_governar›. Acesso em: 25 Jun. 2022.

RODRIGUES, O. **Responsabilidade civil e Internet: problemas de qualificação e classificação de conflitos nas redes sociais.** Responsabilidade civil e inadimplemento no direito brasileiro. São Paulo: Atlas, 2014.

RODRIGUES, N. **Cibercrimes: Os Desafios Na Atual Legislação Brasileira.** Jus.com.br. Disponível em: ‹https://jus.com.br/artigos/93970/cibercrimes-os-desafios-na-atual-legislacao-brasileira›. Acesso em: 25 Jun. 2022.

SCHREIBER, A. **Lei Carolina Dieckmann: você sabe o que essa lei representa?** - FMP - Fundação Escola Superior do Ministério Público. FMP - Fundação Escola Superior do Ministério Público. Disponível em: ‹https://fmp.edu.br/lei-carolina-dieckmann-voce-sabe-o-que-essa-lei-representa/›. Acesso em: 25 jun. 2022.

SOUSA BRITO, A. **O Cibercrime**. São Paulo, 2014. Disponível em: ‹https://recil.ensinolusofona.pt/bitstream/10437/5815/1/Tese%20Cibercrime%20-%20Diana%20Simas.pdf›. Acesso em: 16 Nov. 2022.

WENDT, E.; JORGE, H. **Crimes Cibernéticos: Ameaças e Procedimentos de Investigação.** 2ª Ed. Rio de Janeiro: Braspost, 2013, p. 1-78.

TOURINHO FILHO, F. **Processo Penal.** 34ª Ed. São Paulo: Saraiva, 2012. Vol. I.