CRIMES VIRTUAIS: Uma análise sobre a adequação da legislação penal brasileira

Gustavo Brandão Koury Maues
Funcionário público do tribunal de justiça do Estado do Pará, Professor da Faculdade de Belém – FABEL. Mestrando em Direitos Fundamentais pela Universidade da Amazônia – UNAMA. Mestre em Derecho de Los Negocios Internacionales pela Universidad Complutense de Madrid, UCM. Graduado em Direito pela Centro Universitário do Estado do Pará – CESUPA. E-mail: kourymaues@gmail.com.

Kaique Campos Duarte
Advogado, mestrando em Direitos Fundamentais pela Universidade da Amazônia – UNAMA. Especialista em Direito Penal e Processual penal pela Universidade Estácio de Sá – UNESA. Graduado em Direito pela Faculdade Ideal – Faci | Wyden. E-mail: kaique.ma1507@gmail.com.

Wladirson Ronny da Silva Cardoso
Professor da Universidade do Estado do Pará – UEPA. Doutor em Antropologia Social pela Universidade Federal do Pará – UFPA. Mestre em Direitos Humanos e Inclusão Social pela Universidade Federal do Pará –UFPA. Graduado em Filosofia pela Universidade Federal do Pará – UFPA. Líder do Grupo de Estudos e Pesquisa em Filosofia Moderna e Contemporânea – COGITANS. E-mail: wladirson.cardoso@gmail.com.

RESUMO

O presente artigo pretende realizar uma breve análise sobre o Direito Digital, visando o aprofundamento do tema acerca dos crimes na internet, vez que houve mudanças paradigmáticas na sociedade contemporânea em virtude da globalização e dos avanços tecnológicos, principalmente no mundo da comunicação que evoluiu assustadoramente com o surgimento da rede mundial de computadores. Nesse diapasão, a internet, tornou-se um novo caminho para a realização de delitos já praticados no mundo real, ampliando-se o número de ações relacionadas aos crimes na internet, em decorrência de uma gama de possibilidades de se praticar a violência no meio cibernético. Assim, o controle destas condutas tem sido tema de discussão no Direito, residindo às principais divergências na necessidade de legislação específica e nas dificuldades de resposta do Estado a tais delitos informáticos. Então, pretendendo adequar o Direito às mudanças tecnológicas que transformam continuamente a sociedade brasileira, foi editada a Lei nº 12.737/2012 que possibilitou avanços no combate aos crimes virtuais. Dessa forma, este artigo irá averiguar a adequação da legislação penal brasileira em vigor e as medidas adotadas pelas autoridades competentes no combate a essa criminalidade.

Palavras-chave: Direito Penal. Direito Digital. Crimes Virtuais. Internet.

ABSTRACT

This article aims to analyze the Digital Law in order to research further about the internet crimes, once that there were changes in contemporary society's paradigms due to the globalization and the technological advances, especially in what concerns the communication world, after the emergence of the internet.

In this diapason, the virtual network became a new way of committing crimes that were already committed in the real world, amplifying the number of legal actions related to virtual crimes, considering the variable ways of committing a crime in the cybernetic world. Thus, the control of these behaviors has become a topic in Law's discussions, with most of the divergences showing up in the necessity of specific legislation and the difficulties in obtaining a response from the Estate about such crimes. Therefore, in order to adequate the Law to the new technological changes that continuously transform Brazilian society, it was edited the law No 12.737/2012 that made possible to advance in the combat against virtual crimes. This way, this paper will evaluate the adequacy of the current Brazilian Criminal Law and the measures adopted by the authorities to overcome this issue.

Key-words: Criminal Law. Digital Law. Virtual Crimes. Internet.

1 INTRODUÇÃO

O mundo globalizado é marcado pelo surgimento de tecnologias que possibilitam a alta circulação de informações, pessoas e mercadorias. A internet é exemplo emblemático desta contemporaneidade, pois influência a vida de milhares de pessoas. Hoje, por exemplo, as relações sociais, também, são balizadas pela internet. É comum, negócios jurídicos serem celebrados, encontros, reuniões, relacionamentos se estabelecerem via rede mundial de computadores. Este fato permitiu a possibilidade de novos tipos de crimes através da internet, os chamados crimes virtuais. Em virtude disso, o Direito precisou se adaptar à nova realidade para tutelar bens jurídicos e preservar a dignidade da pessoa humana.

Nesta perspectiva e pretendendo adequar o direito às mudanças tecnológicas que transformam continuamente a sociedade (*ubi societas, ibi jus*), foi promulgada a Lei nº 12.737/2012, denominada de Lei Carolina Dieckmann, que "dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências", visando suprir as lacunas legislativas sobre a temática, recordando que o crime constitui fato típico, devendo todas as suas nuances estarem previstas especificamente na norma, sob pena de atipicidade da conduta.

A Lei 12.737/2012 surgiu em meio ao fato escandaloso que ocorreu com a famosa atriz brasileira, sendo a norma jurídica conhecida popularmente como a Lei Carolina Dieckmann. A referida

Lei teve vários elogios no âmbito jurídico, no sentido que veio para garantir mais dignidade aos usuários da internet, prezando pela tutela da honra, privacidade e intimidade das pessoas. Entretanto, houve criticas a mesma, pois inegável foi à grande demora para sua edição, sendo feita apenas quando uma pessoa de notória fama foi vítima da invasão de dispositivo informático.

Busca-se, nesta pesquisa responder a seguinte pergunta: "A legislação penal brasileira é adequada para conter o aumento de crimes no ambiente virtual?". A metodologia a ser utilizada no presente artigo será de cunho científico, tendo por base o método dedutivo, utilizando o procedimento bibliográfico, realizado por meio de levantamento em material teórico e jurídico em bibliotecas institucionais e acervo particular. Além destes, outros recursos, como jornais, periódicos e documentos digitais (e na internet), também serão consultados.

Diante da complexidade do tema, não iremos zerar as dúvidas, todavia o objetivo é pelo menos incitar a discussão e analisar as referências, que constatem se a aplicação da legislação penal a respeito dos crimes virtuais está precisando ou não de melhorias e trazendo mais esclarecimento sobre o assunto que está gerando grandes debates no âmbito jurídico nacional.

2 A REPERCUSSÃO DA INTERNET NO DIREITO

A internet surgiu nos Estados Unidos, na década de 1970, quando o Departamento de Defesa norte-americano criou um sistema que interligava vários centros de pesquisas militares, permitindo a transmissão de informações e dados. Isso só foi possível devido ao acúmulo de estudos sobre a informática e também ao desenvolvimento de computadores (TEIXEIRA, 2007, p.7)

Pouco tempo depois, no final da década de 1980, a tecnologia da internet ampliou-se de forma a estabelecer a comunicação de computadores entre os órgãos estatais, universidades e laboratórios de pesquisas norte-americanos, facilitando a leitura de documentos por meio de códigos (TEIXEIRA, 2007, p.8).

A internet de fato tem início tardio no Brasil, em 1988, através do Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp) e Laboratório Nacional de Computação Científica (LNCC) no Rio de Janeiro. Apenas em 1991 começa seu uso para o público em geral. Atualmente, a internet é a interligação de redes de computadores que existem pelo mundo, que passam a funcionar como

uma só rede, favorecendo a transmissão de dados, sons e imagens de forma espontânea. Essa conexão de redes pode ser feita por sistema telefônico de cabos de cobre ou de fibras óticas, transmissão de ondas de rádio ou via satélite, por sistema de televisão a cabo entre outros. O usuário, para ter acesso à internet, deve se valer de um aparelho denominado de *modem que*, somado ao auxílio de programas, permite a navegação na rede (TEIXEIRA, 2007, p.9).

Com o passar do tempo, a internet deixa de ser utilizada apenas para os fins originais de sua criação. A abertura ao público na década de 1980, leva a ampliação de seu uso para além do viés militar, cultural ou acadêmico. A internet tem sido equiparada a uma grande Enciclopédia, pois sua capacidade de reunir informações, antes pouco acessíveis, é um progresso para a humanidade e gera uma nova sociedade que debate o que está sendo posto na Rede. Dessa forma, há grandes chances de as pessoas melhorarem suas relações no trabalho, família, educação e de interagir com o mundo (SANTOS, 2001, p. 27).

Entretanto, da mesma forma que se ampliam os usos benéficos da internet (principalmente econômico e social), também, começaram-se a criar meios deturpados de seu uso. Vale dizer que o mundo cibernético não é permeado apenas de benesses, vez que existem inúmeros fatores negativos que merecem destaque. Nesse sentido, pondera Antônio Jeová:

> Durante o apogeu da televisão, foi cunhado o vocábulo "videota" para bem adjetivar aquele que ama a televisão. Atualmente, o "digeota", vem a ser aquele que não consegue viver sem a internet, sem navegar durante horas diariamente em busca das mais variadas sensações. (JEOVÁ, 2015, p.45)

Pode-se falar que há altos riscos de as pessoas se tornarem viciadas em internet ao ponto de passarem horas vislumbrando o mundo digital, de tal maneira que acabam por esquecer a realidade que os cercam, entrando em verdadeira paranóia se forem privados do direito ao acesso à internet. Isso causa isolamento, estresse e ansiedade nas pessoas que vivem em sociedade (SANTOS, 2001).

Além disso, existe a proliferação dos chamados crimes cibernéticos, como: pornografia infantil, da prática do racismo e de fraudes em contratos eletrônicos, crimes contra a honra, furtos de informações bancárias através de hackers. Jeová faz a seguinte reflexão:

> Que o excesso de excesso de dados não nos faça perder a informação. Que o excesso de informação não nos faça perder os conhecimentos. Que o conhecimento não nos impeça de ser sábios e que a ausência de sabedoria não nos faça perder o bom viver. (JEOVÁ, 2015, p.45)

Como se vê, é necessária inteligência e sabedoria na navegação online, vez que ela nos permite ínfimas possibilidades, sejam elas boas ou más. Portanto, ninguém pode ficar indiferente à internet, sendo dever de todos saber utilizá-la de maneira correta a fim de usufruir todas as suas vantagens e evitar que os crimes virtuais sejam proliferados.

A Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD, na sigla em inglês) realizou pesquisa onde o Brasil aparece como o quarto lugar no ranking mundial de usuários da rede mundial de computadores com 120 milhões de pessoas conectadas, perdendo apenas para os Estados Unidos (242 milhões), Índia (333 milhões) e China (705 milhões) (AGÊNCIA BRASIL, 2017).

De acordo com o Instituto Brasileiro de Geografia e Estatística (IBGE) os celulares foram os grandes responsáveis pela expansão do acesso à internet nos domicílios brasileiros. Pela pesquisa, o celular foi o equipamento utilizado por 94,6% das pessoas que acessaram a rede em 2016. O acesso móvel está acima de 90% em todas as grandes regiões. Apesar de o celular ser predominante, outras formas de acesso à rede são via microcomputador (63,7%), tablet (16,4%) e televisão (11,3%) (IDGNOW, 2018).

Interessante ressaltar que a internet está em constante modificação estrutural, sempre visando a máxima experiência em conexão para o usuário. Hoje, a imaterialidade da internet propícia a ausência de limites espaciais e temporais, são características marcantes. A internet pelo seu uso generalizado e pelo amplo acesso, alavanca riscos oriundos da vulnerabilidade do meio digital, sendo assim, quanto maior a utilização da internet nas interações humanas, mais se potencializa a tendência de surgimento de problemas legais, inclusive, o nascimento de novos tipos de crimes.

Os crimes realizados no meio virtual são denominados de crimes virtuais, digitais, informáticos, telemáticos, de alta tecnologia, crimes por computador, fraude informática, delitos cibernéticos, crimes transnacionais, dentre outras nomenclaturas. Estes se dividem em puros (ou próprios) sendo aqueles praticados por meio eletrônico em sentido amplo, onde a informática é o objeto jurídico tutelado, enquanto os impuros (ou impróprios) são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço real, ameaçando ou lesando outros bens diversos da informática (ALBUQUERQUE, 2006, p. 40 e 41).

Nesta esteira, aduz Augusto Rossini:

> [...] o conceito de "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)

Assim, os "delitos informáticos", segundo Rossini, contemplam crimes e contravenções penais, alcançando toda e qualquer conduta em que haja relação com sistemas informáticos, abrangendo, inclusive, delitos em que o computador seria uma mera ferramenta, sem a necessidade de conexão à Rede Mundial de Computadores, ou a qualquer outro ambiente telemático (ROSSINI, 2004)

Importante salientar o conceito de "crime de informática", delineado pela Organização para a Cooperação Econômica e Desenvolvimento da ONU: "O crime de informática é qualquer conduta ilegal não ética, ou não autorizada, que envolva processamento de dados e/ou transmissão de dados" (ROSSINI, 2004, p. 109). Em outras palavras, o crime virtual perante as suas varias denominações, é qualquer ação típica, antijurídica e culpável praticado por pessoa física ou jurídica, com o uso criminoso envolvendo processamento de dados e/ou transmissão de dados, sem a necessidade de conexão à internet.

Dessa forma, é responsabilidade do Estado, através de seu papel regulador e fiscalizador, encontrar formas de prevenção e combate às ilicitudes realizadas no meio virtual. Assim, o Direito, possui a necessidade de evolução e adaptação para acompanhar as transformações da sociedade. Entretanto, essa modificação é gradual e, muitas das vezes, tarda a encontrar soluções jurídicas, principalmente para os aspectos envolvendo as novas tecnologias e a internet.

3 O DIREITO DIGITAL NO ÂMBITO CRIMINAL

O Direito é uma área do conhecimento humano que trata de normas e princípios que disciplinam os atos praticados por pessoas de uma sociedade, buscando manter a paz social, resolver conflitos e até mesmo a punição de cidadãos que estão em desacordo com as leis. Assim, o Direito precisa se adequar aos fenômenos sociais, vez que há mudanças constantes no seio social, não devendo se tornar em um sistema de regramentos e valores de concretização impossível.

Nesse sentido, alude Reale:

> O Direito é, por conseguinte, um *fato* ou *fenômeno social*; não existe senão na sociedade e não pode ser concebido fora dela. Uma das características da realidade jurídica é, como se vê, a sua *socialidade*, a sua qualidade de ser social. (REALE, 2010, p.2)

O Direito Digital surge com o estabelecimento da internet e todas as suas situações sociais, políticas, econômicas e jurídicas. Essa disciplina consiste na evolução do próprio Direito, abrangendo todos os princípios fundamentais e institutos do Direito que estão vigentes e são aplicados até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as áreas (PINHEIRO, 2010, p. 71).

A jurista Peck aponta algumas situações que são tratadas pelo Direito Digital:

> A possibilidade de visibilidade do mundo atual traz também riscos inerentes à acessibilidade, tais como segurança da informação, concorrência desleal, plágio, sabotagem por hacker, entre outros. Assim na mesma velocidade da evolução da rede, em virtude do relativo anonimato proporcionado pela internet, crescem os crimes, as reclamações devido a infrações ao Código de Defesa do Consumidor, as infrações à propriedade intelectual, marcas e patentes, entre outras. (PINHEIRO, 2009, p.76)

Assim, a ausência de normas específicas para as situações no âmbito da internet é um fator que fomenta a impunidade, pois devido às peculiaridades dos ilícitos, várias condutas continuam sem tipicidade, e, assim, sem penalização. Algumas medidas em caráter de emergência e calamidade vêm sendo tomadas através da criação de normas que geram a tipificação de alguns atos criminosos que ocorrem via internet. Exemplos são as leis número 12.735 (Lei Azeredo) e 12.737 (Lei Carolina Dieckmann), as duas sancionadas em 30 de novembro de 2012.

A lei 12.735/2012 (conhecida como Lei Azeredo) estabelece a obrigatoriedade de interrupção imediata de mensagens com conteúdo racista além de retirá-las de qualquer meio de comunicação e a criação das delegacias virtuais. A Lei foi proposta à época pelo deputado federal Eduardo Azeredo (PSDB). O intuito da lei foi alterar o Código Penal, o Código Penal Militar e a lei contra o racismo (nº 7.716/89) visando à tipificação de "condutas realizadas mediante o uso de sistema eletrônico digital ou similares, que sejam praticadas contra sistemas informatizados e similares". A lei sancionada traz apenas dois pontos.

O artigo 4º da lei estipula "Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado", ou seja, a criação de setores de combate ao crime virtual nas delegacias comuns e delegacias especializadas em crimes eletrônicos.

Além disso, o artigo 5º da referida lei acrescentou no artigo 20 da lei 7.716/89 (Lei de Combate ao Racismo) o inciso II do §3º estipulando que: "a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio" de mensagens racistas. O texto original da norma envolvia questões polêmicas, como a tipificação de compartilhamento de arquivos e a obrigatoriedade dos provedores de guardar e fiscalizar o registro das atividades de usuários. Entretanto esses pontos foram vetados. A alternativa à Lei Azeredo foi à lei Carolina Dieckmann.

A Lei 12.737/12 introduziu no ordenamento jurídico 3 tipificações penais no Código Penal: o artigo 154- A que versa sobre a invasão de dispositivo informático alheio, o artigo 266, §1º e 2º que fala sobre a interrupção ou perturbação de serviço telefônico, telegráfico, informático, telemático ou de informação de utilidade pública, artigo 298,§ único, que tipifica falsificação de cartão de crédito ou débito.

A Lei 12.737/2012 surgiu em meio ao fato escandaloso que ocorreu com a famosa atriz brasileira, sendo a norma jurídica conhecida popularmente como a Lei Carolina Dieckmann. Antes da análise jurídica, cabe tomar conhecimento do caso. Em maio de 2012, fotos íntimas tiradas por Carolina, que se exibiu para o seu marido, foram indevidamente divulgadas em vários sítios eletrônicos da rede mundial de computadores. Segundo informações, após deixar um computador pessoal em um estabelecimento de assistência técnica especializada, violaram a sua conta de correio eletrônico, oportunidade em que o criminoso obteve acesso às imagens, passando a chantagear a atriz, sob pena de divulgar as imagens tidas como comprometedoras. O caso foi comunicado às autoridades policiais e ganhou relevância nacional, causando bastante constrangimento na vítima. Os agentes foram punidos pelos crimes de extorsão, difamação e furto, mas não pela invasão de computador, devido o vácuo legislativo da época (JEOVÁ, 2015).

Os especialistas que investigaram o caso afirmaram que ela foi vítima da engenharia social chamada de *pishing*, pois, as pessoas simplesmente acreditam em *spams* ou mensagens publicitárias que garantem um beneficio interessante e totalmente gratuito ao usuário da rede que acaba acreditando, mas tudo não passa de um meio de os *crackers* obterem informações detalhadas contidas em um *smarthphone*, *tablet* ou *notebook*. Diante disso, a mídia pressionou constantemente os parlamentares para que tomassem alguma providencia cabível a fim de combater esse tipo de violência digital que já é bastante comum nos dias atuais.

Neste seguimento, surge á problemática da "legislação do pânico" no Brasil. A legislação do pânico ocorre quando o Poder Legislativo, repentinamente, elabora leis com o intuito de resolver um problema que gerou relevante comoção popular, mas ainda existe a omissão no ordenamento jurídico para tratar o assunto. Geralmente, busca-se o aumento de penalidades ou de tipificações penais para serem aplicadas aos infratores que praticam atos que aterrorizam o povo. Em relação aos crimes virtuais, há que se falar que ele já era um problema antigo no Brasil, mas só foi feito alguma medida depois que houve o escândalo nacional envolvendo a famosa atriz Carolina Dieckmann. Portanto, demonstra-se claramente o "**Direito Penal do Terror**", onde, não raras vezes, os parlamentares criam e aprovam leis por pura pressão da imprensa nacional (MASSON, 2012, p. 11).

Neste diapasão, foi então que o Congresso Nacional editou a referida lei em comento em 30 de novembro de 2012, sendo publicada no Diário Oficial da União em 03 de dezembro de 2012, e em vigor 120 (cento e vinte) dias após a sua publicação oficial. Vale dizer que dispõe sobre a tipificação criminal de delitos informáticos e altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal. Em seu artigo 2º, o legislador criou a seguinte norma penal incriminadora, que passa a integrar a Seção IV (Dos crimes contra a inviolabilidade dos segredos), do Capítulo VI ("Dos crimes contra a liberdade individual"), do Título I ("Dos crimes contra a pessoa"), do Código Penal.

Foi incluído o crime de invasão de dispositivos informáticos no Código Penal:

> **Art. 154-A**. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

O núcleo do tipo consiste em invadir dispositivos informáticos alheios, evidentemente sem sua autorização, pois se o objetivo for para consertar uma máquina por um técnico em informática contratado pelo dono do equipamento, não há que se falar em fato típico. Esse crime é formal porque a mera invasão em dispositivo informático alheio sem a devida autorização já o consuma, não sendo necessário que ocorra a obtenção de dados pessoais da vítima ou que haja a instalação do vírus. Se isto ocorrer, há a incidência do §3º do dispositivo em comento, conforme se nota abaixo:

> **§ 3o** Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: (Incluído pela Lei nº 12.737, de 2012) Vigência Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

Convém dizer que o bem jurídico tutelado é a liberdade individual das pessoas e também busca-se a inviolabilidade de segredos e que esse crime, para existir, deve ser praticado dolosamente. A tentativa é plenamente possível, vez que, por ser o crime de caráter plurissubsistente, é permitido o fracionamento do intercrimini, exemplo disso se dá quando o sujeito realiza manobras para devassar o computador alheio, visando a destruição de dados, mas não consegue fazê-lo porque a vítima, especialista em informática, adota medidas que impedem essa invasão.

A Lei Carolina Dieckmann teve vários elogios no meio jurídico porque veio para garantir mais dignidade aos usuários da internet, prezando pela tutela da honra, privacidade e intimidade das pessoas. Isso é inquestionável, vez que fortalece os Direitos Humanos no Brasil e no mundo. Por outro lado, também houve quem criticasse a mesma, pois inegável foi à grande demora para sua edição, sendo feita apenas quando uma pessoa de notória fama foi vítima da invasão de dispositivo informático. A sociedade, de certa forma, se sentiu inconformada com a situação, vez que em muitos casos ocorreram violações da segurança de dados alheios, mas, por omissão legal, o tratamento jurídico foi insatisfatório. Vale notar ainda, que as penas podem ser consideradas leves, já que há a detenção, havendo reclusão apenas na qualificação do crime.

Quanto às questões processuais, o artigo 154-B do Código Penal trouxe a definição da ação penal cabível, pois a ação penal é pública condicionada à representação. Trata-se de direito disponível, dependendo de provocação do ofendido. Em razão da disponibilidade do bem jurídico tutelado, o consentimento do ofendido exclui o direito de punir do Estado. No entanto, a ação penal será pública incondicionada se o crime for cometido contra dispositivos da administração pública.

Em relação à competência, em regra ela é da Justiça Estadual, não sendo observado se o crime foi cometido pela rede mundial de computadores, sendo da Justiça Federal apenas se houver preenchimento dos requisitos previstos no artigo 109, incisos IV e V, da Constituição Federal: (MASSO, 2014, p.317).

> **Art. 109**. Aos juízes federais compete processar e julgar: IV - os crimes políticos e as infrações penais praticadas em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas, excluídas as contravenções e ressalvada a competência da Justiça Militar e da Justiça Eleitoral; V - os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente;

Ademais, a Lei 12.965/2014 elencou, garantias, princípios, direitos e deveres para a utilização da internet em território nacional, envolvendo provedores de conexão, de aplicação e usuários e

regulou o uso da rede no Brasil e aborda assuntos como direitos e garantias dos usuários, neutralidade de rede, proteção aos registros, a atuação do Poder Público na melhoria do uso da internet no Brasil e a responsabilidade dos provedores. Nesta perspectiva, o decreto nº 8.772/2016 regulamentou o marco civil da internet tratando, entre outras coisas, da guarda e proteção de dados por provedores de conexão e de aplicação, além de apontar medidas de transparência na requisição de dados cadastrais pela administração pública e parâmetros para a apuração e fiscalização de infrações.

Ressalta-se, que apesar de ainda não encontrar, no Brasil, lei específica de proteção de dados, há dois projetos de lei em tramitação (PL 5276/2016 – Câmara e PL 330/2013 – Senado), sem previsão para sua aprovação. Encontra-se, nos projetos a ideia da criação de um órgão específico para efetivar a proteção de dados virtuais, inclusive com poder fiscalizatório e de polícia.

É importante destacar acerca dos crimes contra a honra perpetuados na internet, que aumentaram significativamente nos últimos anos, tendo em vista o crescente número de usuários que utilizam a internet no seu dia a dia, e com o sentimento de impunidade dos usuários, pela falta de fiscalização do poder público. Sendo os crimes a honra aqueles que atingem a integridade ou incolumidade moral da pessoa humana, que se caracteriza pela dignidade da pessoa, o respeito que há entre cidadãos, a boa fama do nome e, inclusive, reputação de alguém (SILVA, 2011). São previstos os seguintes crimes contra honra no Código Penal: calunia (art. 138), difamação (art. 139) e injuria (art. 140).

Nesse contexto, é oportuno abordar sobre outros crimes comuns no âmbito virtual, ameaça (art. 147, CP); fraude bancárias por meio de Internet Banking ou clonagem de cartão Internet Banking (art. 155, § 4º, inciso II, CP); comentar, em chats, e-mails e outros, de forma negativa, sobre raças, religiões e etnias (preconceito ou discriminação art. 20 da Lei n. 7.716 /89); enviar, trocar fotos de crianças nuas (pedofilia art. 247 da Lei n. 8.069 /90, o Estatuto da Criança e do Adolescente - ECA); exploração sexual cibernética contra crianças e adolescentes (art. 241-A c/c art. 241-E, do Estatuto da Criança e do Adolescente- ECA); falsa identidade virtual (art. 307, CP) e a venda de medicamento pela Internet (art. 273, § 1º, CP) (STF, 2009).

Nesta lógica, a natureza jurídica desta disciplina, ora trata é de matéria de Direito Público quando, por exemplo, há a verificação e o combate de crimes informáticos, ora regula conteúdo de Direito Privado, ao englobar os contratos eletrônicos. O Direito Digital estabelece um relacionamento entre o Direito Codificado e o Direito Costumeiro, aplicando os elementos que cada

um tem de melhor para a solução das questões da sociedade Digital. O marco civil, o código penal, a Lei Carolina Dieckmann, o Código de Defesa do Consumidor e até o Código Civil são exemplo de legislações que regulamentam este ramo jurídico estudado, mas, devido ao caráter dinâmico da internet e de sua rápida evolução, é preciso se valer do Direito Costumeiro, praticado na arbitragem. (PINHEIRO, 2010, p. 71)

No Direito Costumeiro, os elementos que estão a amparar o Direito Digital são: a generalidade, a uniformidade, a continuidade, a durabilidade e a notoriedade. A generalidade significa que um determinado fato deva ser repetido com número relevante para que possa virar regra; uniformidade traz a idéia de vinculação à regra criada, vez que um caso concreto servirá de exemplo para outras situações idênticas; continuidade está relacionada com a obediência ao costume que virou regra, sendo a decisão sempre aplicada quando for necessário; durabilidade diz respeito á constância no tempo das decisões do Direito Costumeiro; notoriedade, por fim, diz respeito à publicidade das decisões. (PINHEIRO, 2010, p. 74)

A internet, portanto, é um novo caminho para a realização de delitos já praticados no mundo real, sendo necessário que as leis sejam adaptadas para os crimes eletrônicos. Essa é a nova missão da Justiça: adaptar os vários dispositivos do Código Penal no combate ao crime digital.

4 CONSIDERAÇÕES FINAIS

Como foi aludido, a internet trouxe inúmeros resultados positivos para sociedade, seja na área política, econômica, social ou cultural. Ocorre que várias mazelas foram trazidas com o seu surgimento como, por exemplo, a proliferação dos chamados crimes cibernéticos, como: pornografia infantil, da prática do racismo e de fraudes em contratos eletrônicos, crimes contra a honra, furtos de informações bancárias através de hackers, dentre outros crimes virtuais.

A partir dessa conjuntura é que surge o Direito Digital que consiste na evolução da própria ciência jurídica, abrangendo todos os princípios fundamentais e institutos do Direito vigente. Convêm ressaltar que, para combater os crimes virtuais, surgiram legislações a fim de impedir o crescimento acelerado das ilicitudes cometidas no ambiente digital, porém, um dos grandes empecilhos e, que no fim, acaba fomentando a impunidade é a falta, ainda, de normas específicas de regulamentação dos ilícitos na internet, em virtude de inúmeras condutas continuarem sem tipicidade, desta forma,

não podendo ser penalizadas. Ainda assim, é inegável que medidas estão sendo adotadas para tentar minorar essa realidade, este é o caso, da lei 12.737/2012 (Lei Carolina Dieckmann).

O fato é que a mera elaboração de uma norma ainda não é suficiente para combater a violência, pois o Estado precisa dar mais conscientização à população, implementando mais conteúdos que eduquem as crianças e adolescentes nas escolas para que possam evitar a prática de ilícitos por meio da rede. Foi feito uma análise da legislação brasileira, ficou constatado que no direito brasileiro algumas condutas conseguem ser abarcadas pela legislação atual, mas outras ainda carecem de projetos de lei, ou seja, o Direito deve acompanhar a evolução da sociedade para que as relações entre os indivíduos que utilizam meios eletrônicos no seu dia a dia, não sintam insegurança em suas relações com terceiros em ambientes virtuais.

Assim, a criminalidade virtual ainda crescerá bastante, vez que os avanços tecnológicos não param de trazer novidades. E a legislação, doutrina e jurisprudência brasileira, que surgirão no decorrer dos próximos anos, devem se adequar a essa realidade de maneira proporcional, sem aumentar em demasia as penalidades ou até criar um sistema de censura em relação às redes sociais e demais sítios eletrônicos que se encontram na rede mundial de computadores. O surgimento de uma lei que combata a violência digital só torna-se eficaz quando as autoridades públicas passam a ser qualificadas para lidar com o referido problema. Ou seja, delegacias de polícias precisam ser especializadas em crimes cibernéticos, os juízes devem se atualizarem nas jurisprudências e doutrinas que envolvem delitos informáticos e os advogados, públicos ou privados, devem acompanhar a evolução do Direito Digital para que possa haver uma melhora no funcionamento da Justiça no Brasil.

Conclui-se, que ainda inexiste legislação suficiente para combater a criminalidade digital, apesar de o Direito Digital ainda estar em crescente evolução. Em vista disso, a lei 12.737/2012 é uma evolução legislativa, na medida em que visou garantir a segurança e proteção do direito ao sigilo dos dados e informações dos indivíduos no âmbito digital, mas não podemos ignorar que a lei ainda precisa ser aprimorada, principalmente no sentido da clareza e da aplicabilidade de suas disposições.

REFERÊNCIAS

ALBUQUERQUE, Roberto Chacon de. **A Criminalidade Informática**. São Paulo: Editora Juarez de Oliveira, 2006.

AGÊNCIA BRASIL. **Relatório aponta Brasil como quarto país em número de usuários de internet**. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2017-10/relatorio-aponta-brasil-como-quarto-pais-em-numero-de-usuarios-de-internet/> Acesso em 30 março de 2018.

BRITO, Auriney. **Direito Penal Informático**. 1º Ed. São Paulo: Saraiva, 2012.

FIGUEREDO, Vitor. **Informática Básica para Concursos**. Brasília: Vestcon, 2012.

GRECO, Rogério. **Curso de Direito Penal:** parte geral. Rio de Janeiro: IMPETUS, 2006.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro**. 3. ed. rev. e atual. São Paulo: Saraiva, 2008. v. IV

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo Curso de Direito Civil**. 2. ed. rev., atual. eampl. São Paulo: Saraiva, 2004. v. 3.

IDGNOW. **Brasil tem 116 milhões de usuários Internet e comunicação é principal uso**. Disponível em: <http://idgnow.com.br/internet/2018/02/21/brasil-tem-116-milhoes-de-usuarios-internet-e-comunicacao-e-o-principal-uso/> Acesso em 30 março de 2018.

JEOVÁ. Antonio Santos. **Dano Moral Indenizável**. 5. ed. Salvador/BA: Juspodivm, 2015.

JESUS, Damásio Evangelista de. **Código Penal Anotado**. 17. ed. atual. São Paulo: Saraiva, 2006.

LIMA, Renato Brasileiro de. **Manual de Processo Penal**, vol. Único, 2. ed. Salvador, BA: Juspodivm, 2014.

MASSON, Cléber Rogério. **Direito Penal Esquematizado** – Parte Geral. v.1. 6.ed. Rio de Janeiro: Forense; São Paulo: Método, 2012.

MASSO, Fabiano Del. ABRUSIO, Juliana. FILHO, Marco Aurélio Florêncio Filho. **Marco Civil da Internet** – lei 12.965/2014. 1 ed. São Paulo: Revista dos Tribunais, 2014.

MACIEL, Kátia Regina Ferreira Lobo Andrade et al. **Curso de Direito da Criança e do Adolescente**. Aspectos Teóricos e Práticos. 7ª ed. São Paulo: Saraiva, 2014.

PINHEIRO, Patricia Peck. **Direito Digital**. 4ed. Ver., atual. eampl. São Paulo: Saraiva, 2011.

REALE, Miguel. **Lições Preliminares de Direito**. 27.ed São Paulo: Saraiva, 2006

ROSSINI, Augusto Eduardo de Souza. **Informática, Telemática e Direito Penal**. São Paulo: Memória Jurídica, 2004.

SANTOS, Antonio Jeová. **Dano Moral na Internet**. 1º Ed. São Paulo: Método, 2001.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 6ª ed., São Paulo: Revista dos Tribunais, 1990.

SUPREMO TRIBUNAL FEDERAL, **Justiça usa Código Penal para Combater Crime Virtual**. 2009. Dosponivel em: <http://stj.jusbrasil.com.br/noticias/234770/justica-usa-codigo-penal-para-combater-crime-virtual> Acesso em 30 de maio de 2018.)

TEIXEIRA, Tarcísio, **Direito Eletrônico**. 4º Ed. São Paulo: Joarez de Oliveira, 2007.