CIBERCRIMINALIDADE: CRIMES CONTRA A HONRA NA INTERNET E AS MEDIDAS REGULADORAS DA LEGISLAÇÃO BRASILEIRA

CYBERCRIMINALITY: CRIMES AGAINST THE HONOR ON THE INTERNET AND THE REGULATORY MEASURES OF THE BRAZILIAN LEGISLATION

Ana Cássia Lima de Miranda[1]

Ivy de Souza Abreu[2]

RESUMO: O seguinte artigo científico busca analisar a legislação brasileira que regula a cibercriminalidade, especialmente no contexto dos crimes contra a honra cometidos na internet. Os crimes de honra tipificados no Código Penal Brasileiro são a calúnia, a injúria e a difamação. Com o avanço das tecnologias virtuais e melhores condições de acesso a essas tecnologias para a população, o número de usuários da internet continua aumentando no Brasil. Por consequência, os crimes cometidos em ambiente virtual também crescem, incluindo os crimes de honra. Não existe no Brasil uma legislação específica que regule os crimes de honra quando ocorrem na internet, eles então são julgados de acordo com o que está escrito no Código Penal. Porém, sem uma legislação que trate exclusivamente sobre o tema, nuances e variáveis presentes somente no ambiente virtual podem talvez não ser levadas em consideração no julgamento de casos dessa categoria, podendo acarretar, por exemplo, em dificuldades para se definir uma sentença.

Palavras-chave: cibercriminalidade; legislação; crimes contra a honra; internet.

[1] Graduanda em Direito pela Faculdade Multivix de Cachoeiro de Itapemirim;[2] Doutora em Direitos e Garantias Fundamentais pela FDV. Mestre em Direitos e Garantias Fundamentais pela FDV. Especialista em Direito Público. MBA em Gestão Ambiental. Coordenadora do Grupo de Pesquisa "Biodireito e Direitos Fundamentais". Avaliadora da Revista Opinión Jurídica do Chile (qualis A2). Avaliadora da Revista Brasileira de Políticas Públicas (qualis B1). Avaliadora da Revista Brasileira de Direito (qualis A1). Advogada. Bióloga. Professora Universitária.

ABSTRACT: The following scientific article sought to analyze the Brazilian legislation which regulates the cybercriminality, specially in the context of the crimes against the honor committed on the internet. The crimes of honor typified on the Brazilian Penal Code are the calumny, the injury and the defamation. With the advance of virtual technology and better conditions of access of said technology for the population, the number of internet users on Brazil grew. Consequently, the crimes committed on the virtual environment also grew, including crimes of honor. Brazil doesn't have a specific legislation which regulates crimes of honor when they happen on the internet, so they are judged in accord with what is written on the Penal Code about the subject. However, without a legislation which deals exclusively about this theme, nuances and variables present only on the virtual environment could maybe not be taken in consideration on the judgment of such cases, creating, for example, difficulties for the definition of a sentence.

Keywords: cybercriminality; legislation; crimes against the honor; internet.

1. INTRODUÇÃO

O termo "cibercrime" foi utilizado pela primeira vez em reunião do chamado grupo G-8 no fim da década de 1990, para designar atividades criminosas praticadas na internet. Um dos tópicos discutidos na ocasião foi o crescimento da atividade criminosa na rede mundial de computadores, e possíveis formas de punir, prevenir e combater quaisquer práticas ilícitas no âmbito digital. Um crime cibernético se caracteriza pela utilização de um sistema de informática que processa, armazena e transmite dados, em um ato que causa prejuízo a um bem ou direito protegido por lei.

Em relação ao que pode ser descrito como honra, existem dois tipos de: a honra objetiva, que se refere à maneira com a qual o indivíduo é visto em seu meio social, sua boa reputação na sociedade; e a honra subjetiva, que está relacionada com a forma com que o indivíduo percebe sua própria dignidade, sua percepção de si mesmo. Crimes de honra são aqueles que causam prejuízo à honra objetiva ou subjetiva de uma pessoa. Existem três tipos de crime contra a honra tipificados no

Código Penal Brasileiro de 1940: A calúnia e a difamação, que atentam contra a honra objetiva; e a injúria, que agride a honra subjetiva.

Com o crescimento da adesão de usuários às redes sociais, cresceu também o número de casos de crimes contra a honra cometidos em ambiente virtual. Estimulados pela possibilidade de postar uma mensagem a qualquer momento através de vários dispositivos (computador, celular), e principalmente pelo senso de anonimato que uma rede social oferece, criminosos tecem comentários caluniosos, injuriosos e difamatórios contra terceiros, com uma enganosa noção de impunibilidade.

Como os crimes de honra já estão tipificados no Código Penal Brasileiro de 1940, não foi elaborada legislação específica para situações nas quais eles são cometidos por meios digitais. Em tais casos, a Lei considera a internet simplesmente como o instrumento pelo qual o infrator cometeu o delito.

A pesquisa tem como temática a forma com a qual a legislação brasileira é aplicada em casos de crimes contra a honra cometidos na Internet, e se as atuais medidas punitivas são efetivas no combate a esses tipos de crimes. Diferentes Leis são aplicadas para punir o indivíduo infrator de acordo com o delito digital cometido. No caso de crimes contra a honra o criminoso é enquadrado no Código Penal Brasileiro de 1940, sofrendo as penas ali descritas caso seja condenado, mesmo que o crime tenha sido cometido em ambiente virtual.

A pesquisa tem por objetivo analisar a eficácia da legislação brasileira para combater crimes cibernéticos contra a honra, avaliando como a atual legislação é aplicada nesse tipo de delito, em quais Leis o infrator é enquadrado, as condenações disponíveis de acordo com o crime cometido e os agravantes, e se a atuação da justiça consegue coibir a atuação desses criminosos. Sobre os objetivos específicos desta pesquisa, eles incluem descrever os conceitos de crimes contra a honra, conceituar a cibercriminalidade, pesquisar a legislação brasileira sobre crimes cibernéticos e avaliar se são necessárias mudanças na legislação.

A metodologia que será utilizada para a elaboração do artigo científico será a pesquisa bibliográfica. A pesquisa bibliográfica utiliza como fontes de conhecimento sobre o tema pesquisado publicações cientificamente verificadas, como livros, documentos, artigos científicos, dentre outros. No caso desta pesquisa foram utilizados principalmente livros e artigos científicos, que tratam da legislação brasileira sobre crimes virtuais e uma possível necessidade de atualizar algumas das Leis ou mesmo criar outras que sejam específicas sobre esse tipo de crime.

As legislações brasileiras que versam sobre crimes cometidos no meio digital ainda são relativamente recentes. As ferramentas reguladoras disponíveis para a justiça controlar crimes cometidos contra a honra por meios virtuais são eficazes? Quais são as condenações cabíveis para infratores que cometem tais delitos em redes sociais?

Como já especificado, indivíduos que cometem crimes de honra são enquadrados no Código Penal de 1940, que versa sobre a caracterização de tais crimes e as condenações cabíveis. Já outros crimes virtuais, como o roubo de dados e senhas, são regulados pela Lei dos Crimes Cibernéticos, instituída no ano de 2012. Ao invés de punir crimes digitais com leis diferentes, é possível que uma única legislação que englobasse todos esses delitos em uma única regulação tornasse o processo punitivo mais claro, abrangente e específico, contribuindo para inibir essa categoria de crime cada vez mais comum.

2. CRIMES CONTRA A HONRA NO ORDENAMENTO JURÍDICO PENAL BRASILEIRO

A importância da honra para a legislação brasileira é destacada já na Constituição Federal de 1988, no art. 5, inciso X, que diz “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação” (BRASIL, 1988). A honra é, portanto, considerada direito fundamental do indivíduo perante a Lei.

A honra pode ser descrita como um bem imaterial, podendo ser atribuída às pessoas físicas e jurídicas. A honra engloba um conjunto de qualidades e características do

indivíduo pelos quais ele é avaliado pela comunidade onde vive. Se tal avaliação é positiva, o indivíduo passa a gozar de prestígio social e profissional, e proporciona ainda uma sensação de bem estar consigo mesmo (SILVA, 2012).

A Legislação brasileira considera a honra um bem imaterial e digno de tutela penal, portanto, atividades que causem dano a ela são consideradas criminosas (NUCCI, 2017). O Código Penal brasileiro tipifica três tipos de crimes contra a honra: calúnia, difamação e injúria (BRASIL, 1940).

O primeiro crime de honra tipificado pelo Código Penal brasileiro é a calúnia, que em seu artigo 138 o descreve como “Caluniar alguém, imputando-lhe falsamente fato definido como crime” (BRASIL, 1940). O crime de calúnia é, portanto, o ato de atribuir a autoria de atividade criminosa a um indivíduo que não a cometeu, de forma que terceiros tomem conhecimento da falsa acusação (GRECO, 2013).

O crime de calúnia pode ser cometido de duas formas: explícita e implícita. Na forma explícita o infrator faz a afirmação falsa de forma categórica, imputando de forma clara um delito a terceiro sem que este o tenha cometido de fato. Já na forma implícita o agente criminoso pode, por exemplo, utilizar frases que não citem a pessoa acusada diretamente, mas implicitamente lhe atribui culpa por um crime pelo qual ele é inocente. O crime de calúnia se efetiva mesmo se o delito erroneamente atribuído a um indivíduo inocente não tiver ocorrido (NUCCI, 2017).

O artigo 139 do Código Penal de 1940 versa sobre o crime de difamação, caracterizando-o como “difamar alguém, imputando-lhe fato ofensivo à sua reputação” (BRASIL, 1940). Para que o crime de difamação seja consumado é necessário que um fato nocivo para a reputação de um indivíduo, verdadeiro ou não, lhe seja atribuído e comunicado para outras pessoas, prejudicando sua imagem na comunidade na qual a pessoa tem seu convívio (ARANHA, 2000).

Diferente da calúnia, a difamação acontece quando o fato atribuído à terceiro é considerado desonroso, mas não criminoso. No caso da difamação, para ser considerada crime é necessário que a imputação seja clara e específica, pois caso seja de natureza implícita, é possível que ela seja enquadrada no crime de injúria. A

difamação se caracteriza como um ataque à honra objetiva, que é um bem jurídico protegido por Lei, onde o infrator fere a dignidade do outro o prejudicando perante a sociedade (MIRABETE; FABRINI, 2014).

Por fim, o crime de injúria está tipificado no artigo 140 do Código Penal de 1940 que o define como “injuriar alguém, ofendendo lhe a dignidade e o decoro” (BRASIL, 1940). O crime de injúria acontece quando o agente criminoso utiliza características vexatórias e ofensivas para descrever ou se referir a terceiro, de forma que atente contra sua honra subjetiva, causando danos a sua dignidade interior e autoestima (ARANHA, 2000).

Para Bitencourt (2011) o crime de injúria se caracteriza como o ato de se manifestar sobre um indivíduo de maneira suficientemente desprezível e desrespeitosa, ofendendo sua honra internamente. No caso da injúria não ocorre a imputação de um fato à pessoa, mas sim a exposição de termos agressivos, atacando-a em um nível pessoal. Por fim, para ser consumado o crime de injúria a ofensa deve ser comunicada pelo agressor para a própria vítima ou para outrem.

3. CONCEITOS INTRODUTÓRIOS ACERCA DA CIBERCRIMINALIDADE

Segundo Silveira *et al* (2017) um dos primeiros cibercrimes registrados aconteceu no ano de 1982, onde um estudante do ensino médio criou um vírus digital que infectava computadores do tipo Apple2. O intuito do estudante não era malicioso, era apenas uma brincadeira entre amigos. Porém, esse foi o primeiro vírus de computador criado, abrindo caminho para incontáveis atividades criminosas que podem ser disseminadas pela rede mundial de computadores.

Já para Jesus e Milagre (2016) a doutrina não consegue determinar qual incidente em específico pode ser considerado o primeiro cibercrime da história. Dois incidentes chamam a atenção nesse caso, nos anos de 1964 e 1978, estudantes de universidades americanas invadiram os sistemas eletrônicos de suas respectivas instituições.

O cibercrime ou delito informático pode ser definido como uma atividade ilícita, que pode ser caracterizada como crime ou mesmo contravenção, sendo cometida de forma dolosa ou culposa, por ação ou omissão, por pessoa física ou jurídica, em ambiente virtual ou usando ferramentas digitais, atingindo alvos virtuais ou reais (NUCCI, 2017).

Segundo Rossini (2004) os cibercrimes são classificados em duas categorias: próprios (ou puros) e impróprios (ou impuros). Os crimes virtuais próprios se caracterizam por atingir bens jurídicos de natureza digital, como sistemas ou dados. Já os crimes impróprios são aqueles que podem ser cometidos em ambos os ambientes, real e virtual, porém com o infrator utilizando a sistemas digitais para atingir a vítima.

Já Castro (2003) define o cibercrime próprio como crimes que só podem ser praticados dentro do ambiente virtual, através da informática. A existência desses crimes se deve exclusivamente à existência das ferramentas digitais, sendo impossível praticá-los fora desse ambiente. Já os cibercrimes impróprios são aqueles cometidos através de um dispositivo digital, mas que não dependem exclusivamente do ambiente virtual para serem efetuados. Portanto, crimes contra a honra que acontecem na internet podem ser considerados cibercrimes impróprios.

A gama de crimes passíveis de serem cometidos virtualmente é extensa, incluindo: acessar de forma ilegal sistemas e dados protegidos; interceptar comunicações sigilosas; modificar dados sem autorização; infringir direitos autorais através de pirataria; proferir discurso de ódio e discriminação; promover escárnio contra qualquer religião; distribuir ou armazenar pornografia infantil; atividades terroristas, dentre outros (ROZA, 2016).

Com o avanço em ritmo frenético das tecnologias que permitem acesso ao ambiente virtual, combater crimes desta natureza se torna uma tarefa cada vez mais complexa, pois as atividades criminosas se atualizam tão rapidamente quanto os sistemas que são utilizados para a realização dos delitos. Com o uso popularizado da internet, indivíduos com conhecimento privilegiado em criptografia, por exemplo, passaram a usar suas habilidades para praticar roubo de informações

criptografadas, tanto para lucro como simplesmente por diversão (JESUS; MILAGRE, 2016).

4. A LEGISLAÇÃO BRASILEIRA SOBRE CRIMES VIRTUAIS E OS CRIMES CONTRA A HONRA EM MEIO ELETRÔNICO

A internet em poucas décadas se popularizou de tal maneira que o ambiente cibernético se tornou uma verdadeira realidade virtual. Tanto que a internet possui canais próprios de comunicação e linguagens específicas utilizadas por seus usuários nessa nova realidade. A facilidade de expressão e anonimato fez com que infratores violassem direitos básicos da Constituição Federal, como a igualdade, a privacidade e a dignidade. Esses criminosos virtuais se sentiam relativamente seguros pois em um primeiro momento a legislação simplesmente não os alcançava (ROCHA, 2017).

Com o crescimento do uso de ferramentas digitais, existe uma necessidade praticamente constante do consumo de informação. Essa necessidade exige uma atualização frequente da tecnologia, facilitando o acesso dos usuários ao conteúdo virtual. A ocorrência de crimes cibernéticos se expande com a mesma rapidez, porém, a legislação brasileira não acompanha esse ritmo. Os atuais dispositivos legais ficaram ultrapassados em se tratando de crimes virtuais, com nítida urgência para a elaboração de Leis que sejam capazes de amparar e proteger usuários da internet no Brasil (ZAPAROLI, 2013).

A Lei n. 12.737/12, conhecida como “Lei Carolina Dieckmann” foi o primeiro esforço legislativo brasileiro para regular práticas criminosas em ambiente virtual. A comoção causada pelo roubo virtual de fotos íntimas da atriz e posterior divulgação culminou na elaboração da Lei, que versa sobre esse e outros delitos informáticos e suas penas (OLIVEIRA *et al*, 2017).

Finalmente através da Lei n. 12.737/12 o direito brasileiro tipificou criminalmente crimes digitais, viabilizando a punição penal para os infratores, tendo em vista que até aquele momento não havia no Código Penal de 1940 quaisquer artigos que regulassem práticas ilegais em ambiente virtual (PIOLI, 2015). A Lei acrescentou os

artigos 154-A e 154-B ao Código Penal, e alterou também os artigos 266 e 298. O artigo 154-A caracteriza o crime de invasão a dispositivo eletrônico, violando a segurança com o objetivo de roubar, adulterar ou danificar dados sem a permissão do proprietário (BRASIL, 2012).

O intuito dos artigos 154-A e 154-B é a proteção de dispositivos informáticos e seu conteúdo, incluindo computadores, *notebooks*, *smartphones*, *tablets*, dentre outros. Porém, outros cibercrimes continuam sem uma legislação específica, sendo enquadrados em leis já existentes (MENESES, 2019).

Já em 2014 foi publicada a Lei n. 12.965, conhecida como Lei do Marco Civil da Internet (BRASIL, 2014), que versa sobre os princípios, os deveres, os direitos e as garantias para o usuário da rede mundial de computadores no Brasil. A Lei busca garantir um espaço democrático no ambiente virtual, onde os brasileiros possam se expressar livremente, ao mesmo tempo em que impõe regras para uma boa convivência social, mesmo digitalmente (OLIVEIRA, 2014). Porém, A Lei do Marco Civil não tipifica nenhuma infração cibernética de fato, apenas estabelece determinadas sanções para quem não cumprir parte de suas determinações (ROCHA, 2017).

De acordo com a Lei n. 12.965/14 o uso da internet no Brasil é regido pelos seguintes princípios:

> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> IV - preservação e garantia da neutralidade de rede;
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei (BRASIL, 2014).

Na legislação brasileira existem leis que regulam o uso da internet no país, porém sem tipificar ou punir delitos graves que possam ocorrer por meio virtual. O judiciário

brasileiro legisla temerariamente, pois ao invés de determinar o que seria uma conduta incorreta e sua cabível punição, prefere estabelecer normas de conduta para a sociedade de forma geral. Principalmente quando considerados delitos de alto grau de gravidade, como o sequestro de informações digitais ou mesmo o roubo virtual (ROCHA, 2017).

Apesar da iniciativa louvável, a elaboração da Lei n. 12.737/12 só foi possível pela repercussão que o caso teve no país. Mesmo com o roubo de dados sendo uma prática comum, foi necessário um evento midiático para que providências fossem tomadas para punir criminosos que praticam esse tipo de delito. Essa inércia por parte dos legisladores faz com que as Leis brasileiras se tornem obsoletas, frente ao grande número de atividades ilícitas praticadas na rede mundial de computadores. A falta de legislação específica pode deixar “lacunas” que a atual legislação não cobre, dando a oportunidade para infratores saírem impunes dos crimes cometidos (CASSANTI, 2014).

Na própria Lei n. 12.737/12 existem lacunas legais que não foram preenchidas. O crime conhecido como “pornografia de vingança”, no qual o infrator divulga imagens íntimas da vítima com o intuito de constrangê-la e se “vingar” não está tipificado na Lei Carolina Dieckmann (TORRES JÚNIOR, 2016).

Mesmo quando considerada a Lei n. 12.965/14, ao tentar garantir a liberdade de expressão do cidadão no ambiente de rede, a Lei pode ter propiciado aos infratores um argumento que pode legitimar discursos de ódio contra terceiros. A linha entre liberdade de expressão e se manifestar de forma criminosa pode ser tênue, portanto, é necessário que a legislação seja específica em relação aos pontos dúbios (OLIVEIRA, 2014).

Sobre a questão da liberdade de expressão, e até que ponto ela pode ser considerada uma livre manifestação do pensamento, Lenza (2012, p. 981) diz o seguinte:

> A constituição assegurou a liberdade de manifestação do pensamento, vedando o anonimato. Caso durante a manifestação do pensamento se

> cause dano material, moral ou à imagem, assegura-se o direito de resposta, proporcional ao agravo, além da indenização.

A Carta Magna, portanto, apesar de garantir que o cidadão tenha a liberdade de expressão, não permite que esta seja exercida em anonimato, justamente para que haja direito de resposta para terceiros, caso estes se sintam lesados pelo que foi dito. Este é o direito do contraditório. A Constituição Federal versa sobre a livre manifestação do pensamento ou liberdade de expressão no seu art. 5º, inciso IV da seguinte maneira:

> Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> (...)
>
> IV - é livre a manifestação do pensamento, sendo vedado o Anonimato (BRASIL, 1988).

A vedação no inciso IV se faz necessária para garantir um equilíbrio entre ser livre para se expressar, e ser responsável por aquilo que se diz. Qualquer tipo de dano a outrem gerado por algo que foi dito por determinado indivíduo acarreta em direito de resposta, sendo cabível até uma indenização de acordo com a gravidade da ocorrência. O veto ao anonimato busca assegurar que a responsabilidade caia sobre o emissor (LENZA, 2012).

Por outro lado, crimes como a invasão de computadores desprotegidos ou a divulgação de imagens e vídeos sem a devida autorização continuam sem uma regulação legal, sendo julgado através de analogia com outros delitos, deixando em aberto a possibilidade dos criminosos não sofrerem punições devido as diferentes nuances e variáveis que o um cibercrime possui (TORRES JÚNIOR, 2016).

Um caso específico ocorrido no Brasil no ano de 2016 foram os ataques de cunho racista contra a jornalista Maria Julia Coutinho, que na época apresentava a previsão do tempo em um telejornal da rede de televisão TV Globo. Cometidos através da página oficial da emissora no Facebook, o crime gerou grande comoção na época,

inclusive com pressões vindas da própria Rede Globo para que os infratores fossem punidos (ROCHA, 2017).

Os criminosos foram de fato identificados e enquadrados pelos crimes de racismo, injúria, falsidade ideológica, corrupção de menores e formação de associação criminosa pela internet, Esta última categoria de crime está tipificada no Código Penal art. 288, que trata de associações criminosas. O enquadramento nestes tipos de delitos se deu principalmente pela falta de Leis específicas sobre esse tipo de crime quando cometido na internet (SOARES, 2016).

Então todos os infratores envolvidos no caso da jornalista, e tantos outros que cometem esse tipo de crime diariamente são enquadrados em tipos genéricos, não específicos. Em se tratando de legislação sobre crimes virtuais, no Brasil a história deste tipo de lei é bem recente e atrasada. Nos Estados Unidos, por exemplo, a lei mais antiga sobre crimes cibernéticos data de 30 anos atrás (ROCHA, 2017).

Fatores como a falta de denúncias, a dificuldade de se obter evidências, e até mesmo a limitação da tecnologia disponível para os agentes legais faz com que o número de casos que de fato vão a julgamento seja baixo, quando comparado com o número de delitos sendo cometidos por meios digitais. Tais problemas acabam dificultando o desenvolvimento de jurisprudências, que poderiam auxiliar na interpretação de crimes virtuais por parte dos tribunais (CORRÊA, 2010).

Para Torres Júnior (2016), novos dispositivos legais precisam ser criados de forma a proteger os bens jurídicos dos cidadãos das ameaças vindas da internet. Reformulação das atuais Leis, o desenvolvimento de novas legislações ou mesmo a criação Delegacias especializadas em crimes virtuais poderiam ser soluções para minimizar o problema da legislação obsoleta em se tratando de crimes digitais.

Segundo Corrêa (2010) existe uma carência legislativa em se tratando de crimes cibernéticos. Mesmo quando o culpado é identificado e o caso chega a julgamento, de acordo com o crime ele deverá ser julgado por analogia, devido à falta de regulação legal específica. Essa adaptação pode gerar penas moderadas, pois o Direito Penal não pode lesar o réu por um enquadramento de caso equivocado, o

que acarreta em prudência na hora de definir a sentença. Por outro lado, o enquadramento pode levar a uma pena branda, insuficiente para punir o criminoso à altura dos danos causados por suas atividades ilícitas na internet.

Diversos projetos de Lei relacionados a crimes cibernéticos tramitam na Câmara dos Deputados. As propostas legislativas abordam a “pornografia de vingança”, proteção da dignidade da mulher no ambiente virtual, agravamento da pena por crime cibernético, a identificação da fonte de anúncios veiculados na rede mundial de computadores, dentre outras. (MENESES, 2019)

5. CONSIDERAÇÕES FINAIS

O número de usuários de redes sociais e fóruns cresce a cada dia, aumentando as interações pessoais em ambientes virtuais, inclusive as interações criminosas. O falso senso de anonimato proporcionado pela Internet fomenta crimes como a calúnia, a difamação, e a injúria. O indivíduo tem a noção de que pode fazer afirmações não verdadeiras sobre terceiros sem ser punido, por estar utilizando um perfil sem seu nome verdadeiro. Apesar de essa ser uma noção equivocada e qualquer pessoa poder ser rastreada pelas autoridades competentes, esse tipo de crime continua a ocorrer diariamente.

Averiguar a efetividade da legislação no combate a um tipo de crime de ocorrência tão rotineira é fundamental, pois somente a constatação da eficácia ou não das leis que regulam tais crimes pode levar a tomada de providências, caso seja necessário, para tornar a legislação brasileira uma ferramenta que além de punir, seja capaz de inibir crimes de honra cometidos por meios digitais.

Quando considerado que muitos destes crimes virtuais são julgados por analogia com leis que punem crimes semelhantes, mas cometidos âmbito físico de fato, alguns problemas podem ocorrer. Por exemplo, determinar com exatidão a severidade da pena que deve ser aplicada ao infrator. Crimes virtuais possuem variantes únicas, que podem se tornar agravantes que não existem em um crime “físico”. Julgar estes agravantes sem uma lei específica que verse sobre o tema

pode ser tarefa complexa, de forma que pode acabar gerando tanto uma sentença muito branda, quanto uma sentença por demais severa.

Existe ainda a complexa questão sobre o limite entre a liberdade de expressão e cometer um crime de honra contra alguém. A Lei do Marco Civil da Internet garante a liberdade de expressão para seus usuários, enquanto o Código Penal caracteriza os crimes contra honra. Em uma situação de conflito entre ambas as legislações, um criminoso poderia se valer do direito de se expressar como uma justificativa para escapar de um crime contra a honra cometido. Leis que dissertem sobre o tema podem aclarar estes limites, fechar possíveis lacunas na legislação e aplicar a pena correta no infrator.

Portanto, novas legislações que tratem de crimes cibernéticos podem ser de grande auxílio para inibir e punir este tipo de ocorrência, além de atualizar a legislação brasileira sobre o tema. O ambiente virtual evolui com extrema rapidez, e novas ferramentas para navegar neste mundo são desenvolvidas a cada dia, aumentando também a gama de crimes possíveis de ser cometidos com elas, o que torna novas legislações sobre o cibercriminalidade essenciais para o presente e o futuro jurídico do Brasil.

4. REFERÊNCIAS

ARANHA, Adalberto José Q. T. de Camargo. **Crimes contra a honra**. São Paulo: Saraiva, 2000.

BITENCOURT, Cezar Roberto. **Tratado de direito penal**: parte geral. 20 ed. São Paulo: Saraiva, 2014.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 21 de maio de 2020.

BRASIL. Decreto-lei n. 2.848, de 07 de dezembro de 1940. **Diário Oficial da República Federativa do Brasil**. Brasília, 07 de dez. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 22 de maio de 2020.

BRASIL. Lei n. 12.737, de 30 de novembro de 2012. **Diário Oficial da República Federativa do Brasil**. Brasília, 30 de Nov. 2012. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 02 de jun. de 2020.

BRASIL. Lei n. 12.965, de 23 de abril de 2014. **Diário Oficial da República Federativa do Brasil**. Brasília, 23 de abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 03 de jun. de 2020.

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais**. Rio de Janeiro: Brasport, 2014.

CASTRO, Carla Rodrigues Araújo de. **Crimes de informática**: e seus Aspectos Processuais. 2. ed. Rio de Janeiro: Lumem Júris, 2003.

CORRÊA, G. T. **Aspectos jurídicos da Internet**. 5 ed. São Paulo: Saraiva. 2010.

GRECO, Rogério. **Código penal comentado**. 7. ed. Niterói: Impetus, 2013.

JESUS, Damásio de. MILAGRE, José Antonio. **Manual de Crimes de Informáticos**. São Paulo: Saraiva, 2016.

LENZA, Pedro. **Direito Constitucional Esquematizado.** 16ª ed. São Paulo: Saraiva, 2012.

MENESES, Sâmia Pereira. **Crimes virtuais:** possibilidades e limites da sua regulamentação no Brasil. 2019. Monografia. (Bacharelado em Direito) – Centro universitário Fametro, Fortaleza, 2019. Disponível em: http://repositorio.unifametro.edu.br/bitstream/123456789/107/1/S%c3%82MYA%20PEREIRA%20MENESES.pdf. Acesso em: 03 de jun. de 2020.

MIRABETE, Julio Fabbrini; FABBRINI, Renato N. **Manual de direito penal**: parte especial. São Paulo: Atlas, 2014.

NUCCI, Guilherme de Souza. **Manual de direito penal**. 13 ed. Rio de Janeiro: Forense, 2017.

OLIVEIRA, Carlos Eduardo Elias de. **Aspectos principais da lei nº 12.965 de 2014, o marco civil da internet**: subsídios à comunidade jurídica. 2014. Disponível em: www.senado.leg.br/estudos. Acesso em 01 de jun. de 2020.

OLIVEIRA, et. al. Crimes Virtuais e a legislação brasileira. **Revista do Curso em Graduação em Direito do Instituto Cenecista de Ensino Superior de Santo Ângelo**. EDIESA, n. 13, p. 119 – 130, jan./jun. 2017.

ROCHA, Adriano Aparecido. **Cibercriminalidade:** os crimes cibernéticos e os limites da liberdade de expressão da internet. 2017. Monografia. (Bacharelado em Direito) – Faculdade de Ensino Superior e Formação Integral, Garça, 2017.

ROSSINI, Augusto Eduardo de Souza**. Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

ROZA, Anderson Figueira Da. **As redes sociais no mundo do crime**. 2016. Disponível em: canalcienciascriminais.com.br/as-redes-sociais-no-mundo-do-crime. Acesso em: 18 de maio de 2020.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. São Paulo: Malheiros, 2012.

SILVEIRA, Neil *et al*. **Crimes cibernéticos e invasão da privacidade à luz da lei Carolina Dieckmann**. 2017. Disponível em: https//jus.com.br/artigos/61235. Acesso em 16 de maio de 2020.

SOARES, Marcelo. **Maluf sofre sabotagem digital em e-mail.** Publicado em 2000. Disponível em http://www1.folha.uol.com.br/fsp/brasil/fc2410200025.htm. Acesso em 22 de out. de 2020.

TORRES JÚNIOR, Paulo Fernando Moreira. **O direito à privacidade e à intimidade na Internet**. 2016. Disponível em: https://openrit.grupotiradentes.com/xmlui/handle/set/1172. Acesso em 13 de maio de 2020.

ZAPAROLI, Rodrigo Alves. **Comentários à lei nº 12.737/12**. 2013. Disponível em: https://www.boletimjuridico.com.br/doutrina/artigo/3058/comentarios-lei-n-12-73712. Acesso em: 27 de maio de 2020.