juris rationis
REVISTA CIENTÍFICA DA ESCOLA DE DIREITO
Universidade Potiguar

A CRIMINALIDADE ALIADA A TECNOLOGIA: UMA ABORDAGEM ACERCA DOS MEIOS INSUFICIENTES PARA PREVENÇÃO E REPRESSÃO NO CIBERESPAÇO

ERICA MÁXIMO
Graduanda em Direito. Universidade Potiguar. E-mail: ericamaximo12@gmail.com

LILIANA BASTOS PEREIRA SANTO DE AZEVEDO RODRIGUES
Mestre em Ciências Jurídico-Empresariais. Instituto Jurídico Portucalense (IJP), Portugal. Professora da Faculdade Natalense de Ensino e Cultura (FANEC)/Universidade Paulista (UNIP). E-mail: lisanto@hotmail.com

Envio em: Março de 2016
Aceite em: Março de 2016

Resumo
É evidente que a criminalidade venha se tornando descomunal no Brasil. Do mesmo modo ou ainda pior, é a criminalidade no ciberespaço. Desta feita, a criminalidade ganhou um nupérrimo modo de se camuflar, o que já não é novidade usar a internet para a prática de meios ilícitos e danosos por muitos criminosos hoje em dia. Um grande aliado para o imenso número de cibercrimes é a tecnologia, que não para de avançar e inovar, dentre essas novidades e avanços, encontra-se a internet – rede mundial de comunicabilidade entre dispositivos eletrônicos e pessoas. O presente artigo foi desenvolvido tendo como base pesquisas bibliográficas, consultas em sites jurídicos e legislações vigentes no ordenamento jurídico brasileiro. Além disso, versa apresentar as dificuldades encontradas no trabalho investigativo na tentativa de reduzir a limites mais estritos a cibercriminalidade evidenciando a realidade do tema no Brasil e finalmente patenteando as formas de resolução e os meios adequados para prevenção e repressão.

Palavras-chave: Criminalidade. Crimes Cibernéticos. Tecnologia. Danos Psicológicos. Direito Penal.

CRIME ALLIED TECHNOLOGY: AN APPROACH ABOUT THE INSUFFICIENT MEANS FOR PREVENTION AND REPRESSION IN CYBERSPACE

Abstract
it is evident that criminality is becoming extraordinary in Brazil. On the same way or even worst it is the criminality in the cyberspace. This time, the criminality won these days a way to camouflage itself, what is not novelty to use the internet to practice illegal means and harmful for many criminals, nowadays. A great ally for the huge number of cybercrimes it is technology that does not stop to advance and renew. Among these innovations and advances is the internet - worldwide network of communicability between electronic devices and people. This article was developed based on literature searches, queries on legal sites and existing legislation in the Brazilian Laws. Besides, it reports the difficulties founded in the investigative work in an attempt to reduce to stricter limits the cybercriminality, showing the reality of the theme in the Brazil and finally manifesting the forms of resolution most appropriate means for the prevention and repression.

Keywords: Criminality. Cybercrimes. Technology. Psychological Damages. Criminal Law.

1 INTRODUÇÃO

Todos sabem que, há tempos observam-se avanços significativos mundialmente no que tange à evolução e o uso da tecnologia, porém, apesar do avanço da tecnologia da informação ser essencial para comunicação e informação, muito se tem visto um alarmante dado de vítimas de crimes cibernéticos avultarem.

Pode-se afirmar que o Brasil está entre os cincos países com maiores vítimas de crimes no ambiente virtual, com base numa pesquisa realizada pelo Comércio e Desenvolvimento divulgada pela Organização das Nações Unidas – ONU no ano passado (2015), o Brasil aparece atrás dos Estados Unidos, do Reino Unido e da Índia com maior criminalidade no espaço virtual.

Ainda se tratando de dados, a ONG Safernet, uma entidade que reúne professores, cientistas da computação, pesquisadores e bacharéis em Direito com a grande e notável missão de tutelar os direitos humanos no espaço virtual, mostrou dados do ano passado (2015), que em 2014 foi registrado o maior número de casos de vítimas que tiveram fotos e vídeos íntimos vazados, relacionando com os crimes mais praticados. Só no ano de 2014, a ONG recebeu denúncias de 224 casos do tipo em sentido oposto de 101 em 2013, considerando que os números são de esfera nacional.

Contudo, esse enorme e vultuoso problema não sobrevém somente em alguns países, como os já especificados, o meio da tecnologia como mecanismo é bem utilizada mundialmente para o uso de condutas criminosas, os crimes são diversos, e diante dessa multiplicidade é possível citar a discriminação e preconceito, ou mais conhecido como crime de ódio (racismo, homofobia, crimes contra o sentimento religioso, etc.), estelionato, bullying, fraudes diversas, apologia ao crime, pedofilia, calúnia, injuria e difamação (crimes contra a honra). Porém, os mais estimados são as fraudes diversas, pedofilia e crimes contra honra. É o que afirma também um delegado efetivo da Delegacia de Repressão aos Crimes de Informática (DCRI) do Rio de Janeiro, também investigador do caso de comentários racistas no Facebook da atriz Thaís Araújo, Alessandro Thiers afirma sobre os crimes mais praticados:

> Em primeiro lugar, com ampla vantagem, nós temos os crimes de vazamento de fotos e vídeos íntimos, com pessoas ofendidas na sua honra. Depois, temos a pedofilia, que as pessoas infelizmente botam bastante na internet. Em terceiro lugar, temos as fraudes financeiras, de uma forma geral. Em quarto lugar, nós temos os crimes de apologia: a atos criminosos, homofobia, racismo, intolerância religiosa", lista o Delegado Alessandro, sem propalar os números de vítimas que fizeram registro na delegacia em que é atuante (BOECKEL; COELHO, 2016).

À vista disso, pode-se apontar o preconceito similarmente nos crimes mais praticados, porém, com menos grau do que os dois primeiros mencionados.

O presente artigo tem por um de seus objetivos expor os diversos crimes práticos no espaço virtual explicando de forma sucinta alguns deles, visando que, será destacado os crimes mais praticados. Além disto, com maior propósito, tem como escopo abordar de forma crítica os problemas encontrados nas formas de coibir tais crimes relacionado com o insuficiente trabalho investigativo dos policiais no Brasil relacionando, sem dúvidas como a maior parcela de culpa para os imensos números de vítimas no ciberespaço.

O 2º (segundo) capítulo expõe à questão da utilização da internet para a prática de condutas criminosas destacando os crimes mais praticados, e em seguida especifica os diferentes tipos de expressão de crimes cibernéticos diferenciando os cometidos de forma pública e os de forma privada.

No tópico 2.1, demonstra os múltiplos bens passiveis de ser lesados e os danos psicológicos sofridos pelas vítimas decorrente desses bens desrespeitados, fazendo um contraponto apresentando casos reais de vítimas no Brasil para melhor referir-se.

O tópico 2.2, destaca de forma íntegra três bens fundamentais, que seja: a questão da honra e intimidade versus a liberdade de expressão aduzindo os limites para manifestação de expressividade, opiniões,

ideias e pensamento.

O 3º (terceiro) capítulo demonstra a legislação brasileira referente a crimes informatizados tendo como um dos grandes problemas do tema em questão, evidenciando tal problema com as novas roupagens para a criminalidade no espaço virtual e que não para de modernizar.

No 4º (quarto) capítulo será feito uma análise sobre os meios de prevenção e repressão de crimes virtuais, mostrando como se dá o trabalho investigativo de forma adequada concernente com o meio mais importante e eficaz para a redução de vítimas.

No tópico 4.1, fala do aplicativo "*Whatsapp*", um breve prelúdio das utilidades do aplicativo e em seguida dando foco maior para crimes praticados com o uso deste aplicativo, observando as garantias do Marco Civil da Internet como meio garantidor dos bens passiveis de ser lesados na internet e nos diferentes aplicativos atuais como o whatsapp.

2 O CIBERESPAÇO E SEU LADO NEGATIVO

Considerando que "*Ciberespaço*" significa espaço virtual ou irreal para comunicação tendo como meio a internet, pode-se patentear mais compreensão. Conquanto, nos dias de hoje não é mais novidade que a internet se faça como uma enorme aliada para práticas de condutas delituosas mundialmente, por ser um mecanismo de acessível uso e de fácil disseminação a internet pode e está sendo o grande meio de utilização para a criminalidade, onde o sujeito do crime não se faz necessário ir às ruas ou até mesmo se expor para cometer crimes, os facínoras estão praticando crimes sentados, na frente de uma tela de computador ou pelo próprio celular. Crimes com a utilização da internet tornam-se a cada ano mais comum, diversos e inovantes.

Em se tratando dos crimes mais cometidos, e é o que mais será elucidado e focado no presente artigo, é conveniente falar que no ato de crimes contra honra, o intento do sujeito do crime é denegrir a reputação da vítima, os valores éticos e morais, os crimes de racismo seria a expressão de preconceito, os chamados também "crimes de ódio" que engloba os crimes de intolerância religiosa e homofobia (preconceito contra homossexuais e Lésbicas), já nas fraudes diversas, os criminosos utilizam a tecnologia para obter dinheiro fácil, o que é bem comum, por exemplo, receber e-mails de remetente que nunca viu estimulando a clicar num link de site fraudulento, parece, mas muita gente cai nesse tipo de fraude, outro exemplo de fraude são compras de produto por sites falsos, de compras feitas que nunca fosse obtidas, um exemplo bem costumeiro.

No entanto, muitas expressões foram criadas com o propósito de gerar tipicidade as ilicitudes cometidas na internet, dentre elas, crimes virtuais, crimes cibernéticos (como mais conhecido), crimes digitais, crimes de alta tecnologia, delitos informatizados, dentre outros. É de conhecimento geral manifestar também a diferença entre os crimes praticados de forma pública na internet, e os cometidos de maneira privada, muitos têm estorvo em fazer essa diferença, ou nem sabem que existe distinção.

Ao fazer uma análise profunda do assunto é possível diferenciar que, os crimes praticados de forma pública na web são chamados de Crimes Cibernéticos ou informatizados, ou seja, são aqueles crimes praticados, por exemplo, nas redes sociais menos irrestritas, de forma pública (sites, blogger, web, fanpage, etc.) o que irá ser exemplificado em um tópico especifico mais na frente. Já os praticados de forma privada são aqueles na qual é ímprobo e complexo de caracterizar o crime, que seja, os crimes contra a honra praticado em aplicativo de cunho "privado" como o Whatsapp, pode-se ter como exemplar.

2.1 MULTIPLOS BENS JURÍDICOS E DANOS PSICOLÓGICOS

Diante de tantos e valiosos bens jurídicos protegidos pela nossa Constituição Federal e até por outras legislações referente à violação de direitos no ambiente digital, é de fundamental importância falar de alguns desses

bens lesados e das reações geradas nas vítimas decorrente desses bens que foram desrespeitados.

Inicialmente, é egrégio expressar o que seja "bem" para Francisco de Assis Toledo (1994, p. 15):

> Bem em um sentido mais amplo, é tudo aquilo que nos apresenta como digno, útil, necessário valioso [...] Os bens são, pois, coisas reais, ou objeto ideal dotado de "valor", isto é, coisas materiais e objetos imateriais que além de ser o que são, valem.

Seguindo a definição de "bem" de Toledo, é possível dizer que o bem ou o valor desrespeitado no que se trata de crimes cibernéticos é a violação da intimidade, da honra, da vida privada, dentre outros bens que será melhor expressado no tópico seguinte.

Em consequência da violação desses bens aludidos, surge, pois, os danos psicológicos nas vítimas, que muitas vezes se tornam irreparáveis. Os danos são diversos, o que acaba tirando, sem dúvida a paz e o convívio social da vítima, é possível citar alguns danos como: suicídio, depressão, cogitação de suicídio, privação social, perda de peso, tensão muscular, alto mutilação, dentre tantos outros.

Ao analisar alguns casos de vítimas é importante citar como exemplo um caso que ocorreu em 2014 e que é interessante observar a especialidade utilizada para disseminação. O caso sucedeu na maior metrópole do Brasil, uma estudante de Engenharia da Universidade Presbiteriana Mackenzie de São Paulo teve algumas de suas fotos de rede social do aplicativo Facebook usadas para produzir fotomontagens em posições pornográficas, as fotos colocavam o rosto da jovem em diversas posições obscenas, as imagens montadas foram propagadas falsamente em dois grupos do aplicativo Whatsapp, o que levou a jovem de 21 anos a apresentar sinais de depressão e a cogitar suicídio. A mãe da vítima que é advogada relatou que além das fotomontagens divulgadas a sua filha passou a receber telefonemas de homens desconhecidos marcando encontros sexuais.

Diante dessa circunstância pode-se observar o quanto a criminalidade no meio virtual vem se tornando habilidoso e maligno. Gerar enormes danos falsamente, ser capaz de idealizar, produzir e propalar fotos obscenas que nunca existiram, é realmente lamentável e ultrajante.

Sem escrúpulos, cabe a concordância que a situação de ter a imagem e toda sua reputação exposta para um público numeroso é razão de terríveis efeitos tanto na saúde psicologia e física, como no próprio convívio social.

A psicossocial do Safernet Juliana Cunha também concorda que ter a intimidade exposta é razão para inúmeros danos: "*Geralmente as vítimas sofrem com muitos transtornos, mentais, físicos e psicológicos*", afirma Juliana.

De acordo com a psiquiatra Carmita Abdo, da Associação Brasileira de Psiquiatria (ABP), a situação de ter a intimidade desrespeitada pode causar danos graves às mulheres, e alerta que as mulheres precisam estar atentas aos sinais de abusos:

"A gente tem que passar desconfiar a partir do momento que documentar a intimidade passa a ser uma insistência. Ele começa a querer fazer alguma coisa diferente, com o discurso de que deseja algo mais excitante. Principalmente em situações de crise no relacionamento", atenta a psiquiatra (BOECKEL; COELHO, 2016).

Em paralelo, é de grande importância citar outro caso que diferente do caso já mencionado acabou de forma bem drástica. Uma adolescente de 16 anos teve fotos intimas espalhadas na internet por um rapaz que ela conversava em redes sociais, o fato levou a adolescente a se suicidar.

Ulteriormente, tempos depois do ocorrido, o autor da divulgação das fotos bastante arrependido lamentou externando em uma entrevista feita por um repórter da RBS para o Profissão Repórter: "Uma bobeira. Foi o maior erro da minha vida. Me coloco no lugar dos pais dela. Sei que isso é difícil, uma tragédia. Eu não sei o que fazer". O fato ocorreu em um interior do Rio Grande do Sul, e sem dúvida um acontecimento marcado negativamente nessa cidade e uma história que jamais será esquecida nem pelos residentes do interior do RS nem para seus familiares. De modo infeliz essa adolescente é apenas

uma de muitas vítimas de crimes no espaço virtual.

Em face a essa realidade, de dados em tal grau gigantesco de vítimas, e que não para de aumentar, e, além disso tudo, dos inúmeros e terríveis danos causados, torna-se preocupante e caótico o estado das vítimas e das próprias autoridades sem ferramentas e sem preparo para resguardar e coibir crimes desse tipo, os criminosos a cada dia se apropriam da tecnologia como aliada, e leva consigo a sensação de "impunidade", o que lhes causa conforto e valência para executar o crime no ciberespaço.

A realidade é que o Brasil não está tão preparado para trabalhar contra a tecnologia e o seu lado negativo, a cada ano cresce o número de vítimas de crimes no ciberespaço, o que deixa perceptivo a falta de preparação.

Uma das soluções para redução desse quadro preocupante de crimes cibernéticos seria a educação, é preciso patentear de que numa circunstância de ter sua honra e intimidade divulgada a vítima não é culpada, e sim autor da divulgação. Uma escritora e ativista feminista Daniela Lima concorda e defende que esses dados gigantescos têm relação com a ausência de educação e falta de discussão sobre o assunto na sociedade:

> A mesma sociedade que não discute a cultura do estupro, mas a roupa que a mulher estava usando ou o lugar onde ela estava quando foi estuprada, tenta responsabilizar as mulheres que se deixaram filmar. Nos dois casos, deixamos de discutir atitudes criminosas dos homens para culpar as vítimas. É uma crueldade extrema. Temos que agir contra esses limites impostos sobre o comportamento das mulheres: o problema não está nas roupas, no lugar que se anda ou nos vídeos, mas no machismo, afirma a escritora (BOECKEL; COELHO, 2016).

A feminista afirmou, dando um exemplo para manifestar que esse problema da criminalidade no espaço irreal é uma questão de educação, de proferir com mais frequência dentre a sociedade que a culpa é do sujeito que expõe a intimidade da vítima e não da vítima.

Mudando o foco de crimes cometidos contra honra e intimidade é relevante citar o caso bastante famigerado (conhecido), que seja o caso da atriz Taís Araújo em que há pouco tempo atrás foi alvo de comentários racistas em sua página no Facebook por vários inconsequentes, a atriz registrou a ocorrência na Delegacia de Repressão a Crimes de Informática (DRCI) do Rio de Janeiro, a investigação teve início no dia 4 de Novembro de 2015 e houve investigação de cerca de 70 perfis com comentários racistas absurdos, o fato aconteceu em 31 de Outubro do ano supramencionado, um caso bem recente e que nos leva a refletir que ainda existe a expressão de racismo, e ademais, de forma covarde como bem fala a atriz quando desabafou na mesma rede social sobre os comentários racistas:

> É muito chato, em 2015, ainda ter que falar sobre isso, mas não podemos nos calar. Na última noite, recebi uma série de ataques racistas na minha página. Absolutamente tudo está registrado e será enviado à Polícia Federal. Eu não vou apagar nenhum desses comentários. Faço questão que todos sintam o mesmo que eu senti: a vergonha de ainda ter gente covarde e pequena neste país, além do sentimento de pena dessa gente tão pobre de espírito. Não vou me intimidar, tampouco abaixar a cabeça, escreveu (COELHO; ELIZARDO, 2016).

Talvez seja difícil dizer qual seja o pior crime no meio cibernético, e por que o número de vítimas não para de crescer, em meio a diversos casos e vítimas, e a uma nova roupagem para criminalidade, seria essencial voltar em grau maior os olhares para esse meio da tecnologia negativa onde propicia a prática da criminalidade.

2.2 O DIREITO A HONRA E INTIMIDADE E A LIBERDADE DE EXPRESSÃO NO MEIO CIBERNÉTICO

Não mudando muito de temática, e ainda falando sobre bens jurídicos lesados, é significativo elucidar a questão do direito a honra e intimidade e a liberdade de expressão com seus limites. Três bens fundamentais que estão explícitos e protegidos pela Lei Maior, pelo Código Penal – CP/40 e pelo Código Civil – CC/02.

A Constituição Federal prevê e protege de forma íntegra os bens passiveis de ser lesados, no seu capítulo

I, intitulada "Dos Direitos e Deveres Individuais e Coletivos", no Art. 5º, X: "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).

Sobre intimidade e vida privada Uadi Lammêgo Bulos explica (2015, p. 572) "*A vida privada* e a *intimidade* são os outros nomes do *direito de estar* só, porque salvaguardam a esfera de reserva do ser humano, insuscetível de intromissões externas (aquilo que os italianos chamam de *rizervatezza* e os americanos, *privacy*)."

De forma destacada em relação a "Honra" Bulos (2015, p. 153) expõe que "A honra é um bem imaterial de pessoas físicas e jurídicas protegida pela Carta de 1988. Traduz-se pelo sentimento de dignidade própria (honra interna ou subjetiva), pelo apreço social, reputação e boa fama (honra exterior ou objetiva)"

Sem dúvidas o bem jurídico desrespeitado é a liberdade individual, estando inserido no Código Penal Brasileiro, no capítulo onde trata sobre "Crimes Contra a Inviolabilidade de Segredos", nos artigos 153 a 154-B.

Por outro lado, a todos é garantido a liberdade de expressão, um direito também fundamental, e assegurado em grau igualitário aos bens jurídicos mencionados, porém com algumas privações e limites.

Para Bulos (2015, p. 580) "A liberdade de expressar o pensamento, pelo exercício de atividade intelectual, artística, científica ou de comunicação, é própria do Estado Democrático de Direito, não se sujeitando a qualquer tipo de censura ou licença prévia (CF, art. 5º, IX)."

Especifica ainda os limites da "Liberdade de Expressão":

"A liberdade de expressão intelectual, artística, científica e de comunicação não é um direito absoluto. Tanto é assim que o art. 5º, X, garante a inviolabilidade da vida privada, intimidade, honra e imagem das pessoas, cujo desrespeito acarreta indenização por danos matérias e morais." (BULOS, 2015, p. 181).

Porém, a liberdade de expressar seus pensamentos é precípuo, não se pode admitir em um Estado Democrático de Direito a privação de expressar suas idéias, opiniões e pensamentos. Contudo, assegurada constitucionalmente essa "liberdade de expressão" é preciso respeitar os bens passiveis de ser lesados, os valores morais e éticos, sociais, a dignidade da pessoa humana, respeitar as escolhas e opções, dentre outros bens. Não se pode emaranhar e confundir a liberdade de expressão com vulgarização, apesar de ser garantia constitucional deve-se resguardar e respeitar a honra e dignidade de outrem. Sem embargo, para especificar tais limites a nossa Carta Magna (Constituição Federal) apresenta os limites da liberdade de expressão quando garante: O direito a honra, a vida privada e a intimidade, a vedação do anonimato, o direito de resposta, e, além disso, a indenização por danos materiais, moral e à imagem.

Por esses aspectos, em relação aos limites da liberdade de expressão Bulos (2015, p. 181) conclui que "Se, por um lado, é proibida a censura e a licença prévia, por outro lado, cumpre o Estado zelar pela dignidade do povo e pelo mínimo de moralidade, proibindo a divulgação de notícias injuriosas, mentirosas e difamantes".

3 LEGISLAÇÃO

Embora o grande problema não esteja somente na legislação, à lei 12.737/12 que foi publicada para tipificar crimes na internet ainda é insuficiente para coibir as condutas criminosas no espaço cibernético, a lei que é apelidada de "Carolina Dieckmann" pelo caso da atriz global mencionada que teve fotos e vídeos íntimos roubados e divulgados por um técnico de manutenção de computador quando a atriz deixou o seu PC para concerto. O caso gerou repercussão mediática, levando um andamento acelerado nos projetos de lei onde iria tipificar os delitos na internet, pois, antes do caso da atriz não tinha existência de uma tipificação adequada para os crimes praticados virtualmente, os delitos desse caráter eram tipificados com base em crimes comuns do Código Penal – CP/40.

Além da lei 12.737/12, a nossa Constituição Federal de 1988 – CF/88 tutela de forma completa o bem jurídico que é privacidade, especificadamente no capítulo I "Dos

Direitos e Deveres Individuais e Coletivos", no artigo 5º, inciso X: "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".

Diante da diversidade de crimes no ambiente virtual, de aplicativos, e, além disso, do crescente número de vítimas, é de grande importância criar uma nova lei que permita caracterizar as condutas delituosas no ciberespaço. Os criminosos virtuais vêm se aperfeiçoando nas formas de delinquir, o que torna difícil e moroso decrescer o grande número de vítimas em crimes desse tipo.

Dentre inúmeros motivos que levam a criação de uma nova legislação, seria a variação de aplicativos existente, de novos aplicativos que não para de ser lançados, a uma certa "impunidade" de que atrás da tela de um computador lhe é garantido o anonimato, e consequentemente, leva os criminosos a usar inovações de aplicativos, aplicativos que, dificulta caracterizar o delito e o próprio trabalho de investigação das autoridades.

São inúmeros e diversos os bens jurídicos que podem ser lesados irreparavelmente por um curto tempo, a internet propicia isso. As inovações trazidas pela era da tecnologia, e a magnitude do crescente número de vítimas de crimes no mundo digital, torna-se a cada dia preocupante, é evidente e inegável a necessidade de uma nova lei que coíba e que englobe todos os aplicativos e futuras inovações que propicia a condutas criminosas em face dessa realidade hostil.

Ao perceber as dificuldades da lei 12.73712, por ter uma certa necessidade de definição mais precisa, é de grande importância mostrar as pertinentes considerações de Ramos Júnior (2013, p. 115) sobre o assunto:

> A ausência de definição legal de muitos termos e expressões utilizadas na norma penal certamente será o primeiro grande desafio a ser enfrentado na aplicação da lei, por haver a necessidade de esclarecer o que se entende por dispositivo informático, mecanismo de segurança, autorização tácita, invasão, vulnerabilidades etc. Esses obstáculos serão superados com a jurisprudência. Enquanto isso não ocorre, para solucionar essas questões, pondera-se, em relação ao conceito de dispositivo informático para fins penais, que seja possível a sua abrangência aos dispositivos que funcionam por computação em nuvem; no que tange ao mecanismo de segurança, considera-se que o seu conceito não pode ser restrito a apenas algumas formas de proteção, devendo englobar todo mecanismo computacional, desde uma senha ou um anti-vírus até a tecnologia mais moderna de detecção de intrusões, invasões e ataques cibernéticos.

4 EXPANSÃO DAS MEDIDAS DE PREVENÇÃO E REPRESSÃO PENAL E SUA (IN) EFICIÊNCIA

Partindo de uma análise entre a anelação que o homem tem em praticar condutas criminosas no ambiente virtual, torna-se gritante que os meios de resguardar e coibir a cyber criminalidade é bem insuficiente. Atualmente, é importante observar no Brasil a falta de delegacias especializadas em crimes virtuais. Não existem delegacias especializadas em boa parte da federação, enquanto que é de enorme mister e importância uma delegacia especializada em cada Estado, o uso de ferramentas apropriadas e de agentes policias preparados para adstringir esse imenso problema.

Ao realizar um estudo acerca das deficiências nas medidas de prevenir e reprimir as atitudes delituosas no ciberespaço é possível elencar algumas como grande primordialidade. Ao partir do presente estudo a primeira medida de prevenção seria a falta de legislação especifica, não que essa necessidade seja o grande problema em questão, mas, não há como omitir que a legislação vigente referente a crimes cibernéticos não tem exatidão nos termos do texto, passando esses problemas para serem resolvidos pela jurisprudência. Não há como prevenir atos ilícitos cometidos no ciberespaço sem que exista uma lei específica para os atos.

Há diversidade de crimes virtuais são imensas e a cada avanço da tecnologia com a criação de novos aplicativos torna-se notório a importância de uma lei que tipifique todos os crimes praticados no espaço virtual. Além disso, outro revés e um dos mais importantes é a escassez de ferramentas apropriadas pelas autoridades

na regalia de gerar resposta rápida as ilicitudes cometidas na internet, e sem dúvidas, o último e não menos importante é policiais preparados para atender e está instruído para receber dos mais diversos casos.

Contudo, todos sabem que no Brasil, há tempos observa-se um estorvo na ocasião ausente de ferramentas adequadas e do despreparo policial em crimes virtuais, o que torna patente é os dados descomunais de vítimas em crimes cibernéticos, como bem releva um delegado atuante do Rio Grande do Sul de uma Delegacia de Repressão aos Crimes de Informática (DRCI). O delegado Emerson Wendt, expos respondendo algumas indagações feitas pelo G1 (Portal de Notícias da Globo) a respeito das dificuldades encontradas na prática do trabalho de investigação nesse cenário factual de crimes com a utilização da internet:

> Acho que a Polícia precisa de mais treinamento e agentes policiais em investigação, além de equipamentos e ferramentas adequadas. Sentimos, também, falta de mais peritos formados na área, justamente para que possam comparecer e realizar o que chamamos de perícia online. Acredito que para 2011 - se o planejamento dependesse só de mim - o ideal seria termos ao menos uma Delegacia de Polícia em cada Estado, interagindo e trabalhando em conjunto no combate aos crimes praticados no ambiente virtual (ROHR, 2011).

Apesar dos problemas expostos pelo delegado não ter sido recente é possível verificar que esses impasses são os mesmos atualmente, problemas que as autoridades estão vivenciando nos dias de hoje. É realidade que o veraz obstáculo do crescente número de vítimas no tema em espeque é a falta de preparação policial e muitas vezes da inexistência de ferramentas adequadas.

Entretanto, tendo como base um manual de investigação de crimes cibernéticos é possível explicar de forma consentânea (apropriada) como se dá a forma de repressão e investigação em crimes na internet com a utilização de ferramentas propícias. Inicialmente, para chegar ao autor do crime é necessário que o URLs (Endereço que digitamos ao fazer determinadas buscas) sejam traduzidos para um endereço numérico,chamado "Endereço IP", a abreviação "IP" significa *Internet Protocol*, explicando com mais exatidão pode-se afirmar que, cada página ou site em que fazemos buscas e acessamos está instalado em um computador ligado à rede, o que chamamos de servidor, onde é identificado somente pelo endereço de IP, cada endereço de IP é único e é graças ao endereço numérico que pode-se chegar ao criminoso, pois, o IP é o número que determinado computador ou roteador recebe ao se conectar com a internet existindo de forma exclusiva cada número – O *Internet Protocol* (IP), como já mencionado.

A identificação do IP é o primeiro passo e mais importante para a investigação de um crime cibernético e consequentemente chegar-se ao autor do delito. Em conformidade com um manual de investigação do Ministério Público Federal (MPF) de crimes cibernéticos é essencial mostrar como funcionar a partir do momento que se recebe a denúncia:

"Quando recebemos a notícia de um crime cibernético, a primeira providência a tomar é a identificação do meio usado: trata-se de a) um website?; b) um e-mail?; c) programas de troca de arquivos eletrônicos (do tipo Kazaa)?; d) arquivos ou mensagens ofensivas trocados em programas de mensagem instantânea (do tipo MSN Messenger ou ICQ)?; e) arquivos ou mensagens ofensivas trocados em salas de bate-papo (chats)?; f) grupos de discussão (como yahoo groups)?; ou g) comunidades virtuais como o Orkut? As características de cada um desses meios são diferentes e, por isso, as medidas a serem tomadas são igualmente distintas" (SUIAMA, 2006).

Ainda tendo como base o referido manual de investigação Suiama (2006), relata que é possível tornar claro as características do crime:

> a) possuem formato complexo (arquivos, fotos, dados digitalizados etc.);
> b) são voláteis, i.e., podem ser apagadas, alteradas ou perdidas facilmente;
> c) costumam estar misturadas a uma grande quantidade de dados legítimos, demandando, por isso, uma análise apurada pelos técnicos e peritos que participam da persecução penal.

Diante dos meios investigativos propícios para responsabilizar o sujeito do crime e caracterizar o crime, não é bem isso que sucede atualmente no Brasil e desde um bom tempo atrás. Ao explorar o tema em espeque é possível comprovar que o problema está exatamente na inexistência da investigação e do preparo policial, é pertinente destacar também que em boa parte da federação não existe delegacias especializadas em crimes cibernéticos, e acaba que sendo encargo da Policia Federal e Policia Civil, o que só torna árduo e difícil os números vultuosos da cibercriminalidade diminuírem.

4.1 WHATSAPP: SUAS UTILIDADES E PERIGOS OCULTOS

O aplicativo *Whatsapp Messenger* é um aplicativo de mensagens e chamadas de voz instantâneas e, além de trocar mensagens com amigos os usuários podem enviar imagens, vídeos e mensagens de áudio, e também fazer ligação gratuita para amigos que usem o Whatsapp, todas essas utilidades necessitam do uso da internet. O aplicativo foi criado no ano de 2009 por Brian Acton e Jan Koum, o Whatsapp foi vendido para o Facebook por US$16 bilhões, portanto o aplicativo Whatsapp pertence ao Facebook desde ano de 2014 e está sediada na Califórnia.

Apesar dos benéficos que o aplicativo oferece existe um lado negativo, que seja uma das novas roupagens para a criminalidade, muitos aplicativos como o Whatsapp são usados para cometer o que chamamos de "*crimes digitais*", como bem já foi explicado em um tópico anteriormente, tendo como exemplar é possível mencionar vários crimes praticados contra honra e intimidade no whatsapp. O aplicativo também tem a opção de criar grupos restritos onde só participa quem o administrador (criador do grupo) adicionar, e muitos desses grupos apresentam conteúdos pornográficos e difamatórios.

Com o uso do whatsapp para prática de crimes, não há como negar que a disseminação é enorme, uma vez que, de uma mensagem ou foto enviada para uma pessoa é repassada para um grupo desse grupo se propaga por inúmeros grupos e diversas pessoas em um curto tempo, o que incorre a dificuldade de encontrar onde deu inicio, isso tudo de forma "privada", até porque só irá ter acesso ao conteúdo ilícito a quem foi enviado ou a quem fizer parte de um estabelecido grupo em que foi enviado o conteúdo, o conteúdo difamatório não é posto, por exemplo, como determinado comentário racista ou atento contra honra e intimidade cometidos no aplicativo Facebook, blogger, dentre outros aplicativos públicos, apesar da propagação ser imensa é possível chegar-se ao principal autor de onde teve inicio sempre através do "IP" do computador se praticado com a utilização de um PC ou do roteador que libera internet para os *smartphones*, e aos que participam na divulgação do conteúdo também são responsabilizados.

Além disso, embora que diante de uma investigação de um crime digital como praticado no Whatsapp, se as informações forem "apagadas ou descartadas" é possível ainda sim recuperar, o criminoso não poderá ficar "impune" através das utilidades de um aplicativo "restrito". De acordo com o Marco Civil da Internet os provedores devem guardar as conversas dos usuários do aplicativo, mesmo que o App Whatsapp esteja sediado na Califórnia deve-se respeitar e cumprir a legislação brasileira, que dispõe no próprio Marco Civil, onde estabelece direitos, garantias e deveres relacionados à internet.

Na seção II do Marco Civil da Internet onde trata "Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas" garante no Artigo 10:

> A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas

6 CONCLUSÃO

Não há como falar da criminalidade no ciberespaço sem falar de globalização e a tecnologia que, com

isso, tornou-se perceptivo a proporção em tal grau que sucedeu, demonstrando que há uma nova forma de camuflagem para a criminalidade tornando manifesto que novas formas de resguardar e coibir a cibercriminalidade devem ser criadas e ajustadas para que o direito não ande em descompasso com as inovações da tecnologia.

Em se tratando de como surgiu os crimes cibernéticos é pertinente aludir o que seja "globalização" colocando, sem dúvidas como grande contribuição para o cenário atual referente a criminalidade no ciberespaço. De uma forma concisa Beck transparece alguns problemas encontrados com a globalização:

> Globalidade significa o desmanche da unidade do Estado e da sociedade nacional, novas relações de poder e de concorrência, novos conflitos e incompatibilidades entre atores e unidades do Estado nacional por um lado e, pelo outro, atores, identidades, espaços sociais e processos sociais transnacionais (p. 49).

Consentâneo com o cenário atual no Brasil, com o avanço da tecnologia e com a criação de novos aplicativos virtuais, é primordial a existência de uma legislação especifica, com melhor exatidão, e seguidamente um preparo mais adequado para atender os inúmeros e diversos casos de crimes cibernéticos, não há como resolver apenas um problema esquecendo que o trabalho investigativo poderá seguir sem uma lei especial para crimes cometidos no ciberespaço.

Sob essa perspectiva, da árdua tarefa de resguardar os bens desrespeitados com o uso da internet, e ademais, da criação de um novo mundo para criminalidade e que está sempre inovando a partir do avanço da tecnologia e da criação de novos aplicativos é factível analisar em grau de grande importância de meios eficazes e concretos a resolução desses delitos, observando constantemente os avanços na tentativa primeiramente de proteger tais bens visando sem dúvidas posteriormente à redução de vítimas.

REFERÊNCIAS

AMORIM, Maurício Oliveira; SOUSA, Monica Teresa Costa. O protagonismo judicial e as políticas públicas. **Direito, Estado e Sociedade**, [s.l.], v. 1, n. 46, p.268-290, maio 2015. Semestral.

ANDRADE, Allan Diego Mendes Melo de. **O direito à intimidade e à vida privada em face das novas tecnologias da informação.** 2013. 13 f. TCC (Graduação) - Curso de Direito, Universidade Federal de Piauí, Piauí, 2014. Cap. 7.

BECK, Ulrick. **O que é globalização**. São Paulo: Paz e Terra, 1999. 283 p. Tradução de: André Carone.

BOECKEL, Cristina; COELHO, Henrique. Vazamento de 'nudes' é crime virtual mais comum no Rio, diz delegado. **Portal G1**, 2016. Disponível em: <http://g1.globo.com/rio-de-janeiro/noticia/2015/11/vazamento-de-nudes-e-crime-virtual-mais-comum-no-rio-diz-delegado.html>. Acesso em: 12 jan. 2016.

BULOS, Uadi Lammêgo. **Curso de Direito Constitucional.** 9.ed. São Paulo: Saraiva, 2015.

BRASIL. Ulysses Guimarães. República Federativa do Brasil. **Preâmbulo.** 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 04 jan. 2016.

_____. Hildo Rocha. ComissÃo de ConstituiÇÃo e JustiÇa e de Cidadania. **Projeto de Lei Nº 215, DE 2015 (Em apenso os PLs nºs 1.547 e 1.589, de 2015)**. 2015. Disponível em: <http://www2.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=1EB570EBF5BA7B1CFBF530AAE3799307.proposicoesWeb2?codteor=1367703&filename=Tramitacao-PL+215/2015>. Acesso em: 20 jan. 2016.

COELHO, Henrique; ELIZARDO, Marcelo.'Racismo é recorrente', diz delegado de combate a crimes virtuais no Rio. **Portal G1**, 2016. Disponível em: <http://g1.globo.com/rio-de-janeiro/noticia/2015/11/racismo-e-recorrente-diz-delegado-de-combate-crimes-virtuais-no-rio.html>. Acesso em: 08 jan. 2016.

COLLI, Maciel. **Cibercrimes**: limites e perspectivas para a investigação preliminar policial brasileira de crimes cibernéticos. 2009. 172 f. Dissertação (Mestrado) - Curso de Mestrado em Ciências Criminais, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2009. Cap. 4.

ELIEZER, Cristina Rezende; GARCIA, Tonyel de Pádua. O novo crime de invasão de dispositivo informático. **R. Curso Dir. Unifor,** Formiga, v. 5, n. 1, p.69-87, maio 2014. Semestral.

FREITAS, Ana Teresa Silva de. Protagonismo judicial no Brasil: em busca da concretização de direitos fundamentais sociais. **R. Pol. Públ**., São Luís, p.379-384, jul. 2014. Número especial.

FREITAS, Jessica Oniria Ferreira de. Sobre a tortura e sua configuração jurídica e fática no Brasil. **Revista do Caap**, [s. L.], p.161-187, fev. 2009. 1º semestre.

GARRIDO, Adriana Cristina Oliver. **FATORES SOCIAIS DE CRIMINALIDADE**. 2013. 18 f. TCC (Graduação) - Curso de Direito, Faculdade Atenas – Paracatu/mg, Minas Gerais, 2014. Cap. 2.

GODOY, Regina Maria Bueno de. **Bem Jurídico Penal**. 2010. 122 p. Dissertação (Mestrado em direito) – Pontifícia Universidade Católica de São Paulo, São Paulo, 2010.

GOERGEN, Pedro. Educação e valores no mundo contemporâneo. **Educ. Soc.**, Campinas, v. 26, n. 92, p.983-1011, ago. 2005. Semestral. Disponível em: <http://www.cedes.unicamp.br>. Acesso em: 20 dez. 2015.

MUELLER, Suzana Pinheiro Machado. O impacto das tecnologias de informação na geração do artigo científico: tópicos para estudo. **Ci. Inf.**, Brasília, v. 23, n. 3, p.309-317, nov. 1994. Trimestral.

PINHEIRO, Emeline Piva. **Crimes Virtuais:** uma análise da criminalidade informática e da resposta estatal. 2006. 34 f. TCC (Graduação) - Curso de Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2006. Cap. 5.

RAMOS JÚNIOR, H. S. **Invasão de dispositivo informático e a Lei 12.737/12**: comentários ao art. 154-A do Código Penal Brasileiro. Disponível em: <http://www.42jaiio.org.ar/proceedings/simposios/Trabajos/SID/09.pdf>. Acesso em: 24 abr. 2014.

RODRIGUES, Fillipe Azevedo. **Análise Econômica do Direito Penal**. Belo Horizonte: Del Rey, 2014.

ROHR, Altieres. Trabalho contra crimes virtuais ainda está longe do ideal, diz delegado. 2011. **Portal G1**. Disponível em: <http://g1.globo.com/tecnologia/noticia/2011/01/trabalho-contra-crimes-virtuais-ainda-esta-longe-do-ideal-diz-delegado.html>. Acesso em: 29 dez. 2015.

SCALCON, Raquel Lima. Apontamentos críticos acerca do funcionalismo penal de Claus Roxin. **Congresso internacional de Ciências Criminais**. II Ed. 2011. Disponível em: <http://ebooks.pucrs.br/edipucrs/anais/ciencias-criminais/edicao2/Raquel_Scalcon.pdf>. Acesso em: 02 jan. 2016.

SILVA, Ana Karolina Calado da. O estudo comparado dos crimes cibernéticos: uma abordagem instrumentalista-constitucional acerca da sua produção probatória em contraponto à jurisprudência contemporânea brasileira. **Âmbito Jurídico**, Rio Grande, XVI, n. 109, fev 2013. Disponível em: <http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=12778&revista_caderno=17>. Acesso em: 10 jan. 2016.

SUIAMA. Sergio Gardenghi. Ministério Público Federal. **Crimes cibernéticos**: manual prático de investigação. 2006. Disponível em: <http://www.mpce.mp.br/orgaos/CAOCRIM/pcriminal/ManualdeCrimesdeInformática-versaofinal.pdf>. Acesso em: 12 jan. 2016.

TOLEDO, Francisco de Assis. In: FRANCO, Alberto Silva. **Crimes Hediondos**. 5.ed.rev.,atual.e ampl. São Paulo: Editora Revista dos Tribunais, 2005. p. 126.

ZANATTA, Leonardo. **O direito digital e as implicações cíveis decorrentes das relações virtuais**. 2010. 37 f. TCC (Graduação) - Curso de Ciências Jurídicas e Sociais, Pontifícia Universidade Católica do Rio Grande do Sul, Rio Grande do Sul, 2010. Cap. 3.