Novos Cadernos NAEA

v. 20, n. 2, p. 127-148, maio-ago 2017, ISSN 1516-6481 / 2179-7536

A violência na prática de crimes no ciberespaço

The violence in cybercrimes

Beatriz Silveira Brasil - Delegada da Polícia Civil do Estado do Pará. Foi Diretora da Delegacia de Repressão a Crimes Tecnológicos da Polícia Civil do Estado do Pará (2009-2015). Atualmente é Assessora de Inteligência e Segurança Corporativa da Secretaria de Estado de Meio Ambiente e Sustentabilidade do Estado do Pará (SEMAS). Mestre em Defesa Social e Mediação de Conflitos, UFPA. E-mail: bosilveira@yahoo.com.br.

Edson Marcos Leal Soares Ramos - Professor Doutor da Universidade Federal do Pará. Coordenador do Programa de Pós-graduação em Segurança Pública. E-mail: ramosedson@gmail.com.

Silvia dos Santos Almeida - Professora Doutora da Universidade Federal do Pará. Atua no Programa de Pós-graduação em Segurança Pública. E-mail: salmeidaufpa@gmail.com.

Marcos Miléo Brasil - Delegado da Polícia Civil do Estado do Pará, mestre em Segurança Pública, UFPA. Atua no enfrentamento a fraudes, crimes ambientais e lavagem de dinheiro. E-mail: marcosmileo@gmail.com.

Resumo

Visa identificar a exteriorização da violência na prática de crimes na sociedade digital, onde há a redefinição ou extinção de fronteiras e supervalorização da informação, que agora possui alcance global e instantâneo. A metodologia adotada foi pesquisa bibliográfica e documental. Discutiu-se se os cibercrimes apresentam algum teor de violência e quais as suas formas de exteriorização. Observou-se que a cibercriminalidade também se adaptou a essa nova realidade social, consolidando a violência psicológica, moral e patrimonial, cujas práticas delitivas possibilitam maiores resultados danosos com menores riscos. Dessa forma, urge que os órgãos de justiça criminal busquem conhecer esses novos enfoques de atuação delitiva e se qualifiquem para o respectivo enfrentamento, especialmente com atuação cooperativa entre si e com a sociedade.

Palavras-chave

Digital. Sociedade. Informação. Tecnologia. Global. Delito.

Abstract

This paper aims to identify the externalization of violence in crime in the digital society, where there is resetting or extinction of borders and overvaluation of information, which now has global reach and in real time. The methodology adopted was bibliographic and documentary research. It was discussed cybercrimes have some level of violence and what its forms. It was observed that cybercrime has also adapted to this new social reality, consolidating the psychological, moral and patrimonial violence, whose criminal practices enable greater harmful results with less risk. Thus, it is urgent that criminal justice agencies seek to know these new approaches to delinquency and qualify for the respective confrontation, especially with cooperative action between themselves and with society.

Keywords

Society. Information. Technology. Global. Crime.

INTRODUÇÃO

Atualmente, o mundo vivencia uma nova forma de organização social, onde a tecnologia da informação tem papel fundamental, uma vez que remove fronteiras e atinge milhões de pessoas em tempo real.

Nesse contexto, surge a "sociedade da informação" ou "sociedade do conhecimento", que se caracteriza, conforme Lisboa (2006), pela preponderância da informação sobre os meios de produção, bem como pela nova forma de distribuição dos bens na sociedade, que se estabeleceu a partir da popularização das programações de dados utilizadas nos meios de comunicação existentes e nos elementos referentes a pessoas e/ou objetos, visando a realização de atos e negócios jurídicos.

Para Angeluci e Santos (2007), a comunicação e a informação em tempo real, em que as relações empresariais e pessoais são facilitadas pelo livre e irrestrito acesso à internet, fez com que muitos dos costumes e valores da sociedade fossem substituídos, passando a preponderar o egocentrismo, a superexposição e as informações em massa, favorecendo, inclusive, a prática de crimes no ciberespaço.

A nova ordem social, que ilustra a expressão popular "informação é poder", formou o que se denomina de ciberespaço, o qual, ao propiciar a intensificação das relações humanas, trouxe inúmeros benefícios, especialmente relacionados à democratização do acesso à informação, à cultura, à política, aproximando pessoas e reduzindo o tempo gasto em atividades rotineiras.

Deibert e Rohozinski (2010) conceituam o ciberespaço como domínio, mas destacam que, ao contrário do mar, da terra, do ar e do espaço, aquele é inteiramente criado, sustentado e transformado pela interação humana em curso e fruto de intensa competição. Destacam que a proteção do ciberespaço se tornou uma das principais preocupações políticas globais do século XXI, pois apesar de haver uma crescente literatura afirmando a segurança nesse ambiente relacional, muito pouco se refere acerca de toda a gama de riscos e respostas ou às implicações políticas em torno dele.

Santos e Fonseca (2010) entendem que um dos principais desafios do momento é a regulação do espaço cibernético, garantindo os direitos fundamentais no ambiente da *web*, pois além de diminuir o custo social, visa assegurar o exercício da cidadania em meios digitais, os direitos humanos, a pluralidade, a diversidade, a abertura, a livre iniciativa, a livre concorrência, a colaboração e normatização do desenvolvimento da rede mundial na sociedade da informação, como instrumento de transformação social.

Em 2011, na Islândia, os cidadãos utilizaram redes sociais e o site oficial do conselho criado para fazer a redação de uma nova constituição, para opinar sobre assuntos diversos, que iriam compor a sua futura norma constitucional, gerando a primeira legislação colaborativa, apresentando-se em um contexto favorável, haja vista a penetração de quase 95% de internet, um povo desiludido com a política e no limite por causa da crise de 2008 (BERGMANN, 2013).

Ressalta Bergmann (2013) que a web é uma nova ferramenta para a participação cidadã nos governos democratas, mas onde não se cria um novo modelo de democracia, e sim um aperfeiçoamento dela, visando um nível mais avançado do sistema político, onde a participação é o caminho para chegar lá.

É válido destacar que, conforme Bonavides (2008), o direito à democracia, à informação e ao pluralismo são direitos constitucionais de 4ª geração, que são a marca da era pós-industrial, trazendo também novos desafios ao Estado, acerca da regulação das novas relações geradas, bem como da discussão do próprio papel e existência do ente estatal.

Para Castells (2003), o Estado não desaparece, sendo apenas redimensionado na Era da Informação, passando a se proliferar sob a forma de governos locais e regionais, os quais se espalham pelo mundo com seus projetos, formam eleitorados e negociam com outros governos nacionais, empresas multinacionais e órgãos internacionais.

Observa-se que todo o poder conferido aos indivíduos pelas declarações de direitos humanos passa a se materializar no ciberespaço, onde cada um pode fazer o que quiser, desde conectar-se com outras pessoas, até decidir os rumos do seu país, diariamente, a exemplo do que vem ocorrendo no Brasil, onde as manifestações populares começam pelas redes sociais, urgindo a regulação das relações sociais no ciberespaço, definindo os limites entre os direitos e deveres dos cidadãos do mundo globalizado.

O limiar entre o que é moral ou imoral ou lícito ou ilícito no ambiente globalizado é muito tênue, ante a carência de legislação específica, gerando sérios questionamentos acerca de até onde um indivíduo pode exercer sua liberdade de expressão, seu poderio econômico ou sua propaganda política, por exemplo, sem ferir os direitos dos outros.

Na análise da relação entre segurança e ciberespaço, Deibert e Rohozinski (2010) constataram a existência de duas dimensões, apontadas como "riscos": "riscos para o ciberespaço", que são riscos para o aspecto físico do computador e tecnologias da comunicação, como as invasões e envio de programas maliciosos; "riscos através do ciberespaço", que seriam os riscos que surgem do ciberespaço e são facilitados ou gerados especificamente por suas tecnologias, mas não

atingem diretamente as suas infraestruturas, por si sós, como as fraudes bancárias praticadas pela internet.

Independentemente de qualquer classificação, os riscos na rede vão desde a identificação de vulnerabilidades em sistemas informatizados à prática de crimes, simples ou complexos, de menor ou grande potencial ofensivo.

É válido destacar que o crescimento dos crimes praticados no ambiente virtual é acompanhado do aumento do acesso à internet, da ausência de regulamentação específica e pelas facilidades que o ciberespaço proporciona, entre elas o suposto anonimato, tornando de extrema relevância o estudo científico do presente tema, especificamente quando à violência no ciberespaço.

Ressalte-se que no ano de 2001, foi elaborada pelo Conselho da Europa a Convenção de Budapeste, ou Convenção sobre o Cibercrime, a qual é um tratado internacional que visa a unificação do tratamento dos crimes cibernéticos e a respectiva persecução penal, englobando mais de 20 países (HUNGRIA, 2001).

Em seu preâmbulo, a convenção confere caráter prioritário a uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, mais especificamente, a partir da adoção de legislação adequada e da melhoria da cooperação internacional (HUNGRIA, 2001).

O referido tratado traz elementos importantes para o combate à criminalidade cibernética, pois não só cria crimes específicos, como define provas, mecanismos de cooperação e de investigação penal (HUNGRIA, 2001).

Infelizmente, segundo Erdelyi (2008), o Brasil não participou das discussões que levaram à criação da Convenção de Budapeste nem aderiu a esta, pairando no país grande incerteza legislativa e social quanto aos cibercrimes, sua investigação, processamento e julgamento, haja vista as peculiaridades, especialmente quanto à plurilocalidade e o suposto anonimato.

Segundo o Ibope (2013), o total de pessoas com acesso à internet no Brasil no primeiro trimestre de 2013 chegou a 102,3 milhões, apresentando crescimento de 9% sobre os 94,2 milhões divulgados pelo instituto, no terceiro trimestre de 2012.

Observa-se que com o aumento e popularização do uso da rede mundial de computadores e outras tecnologias da informação e comunicação, há também o incremento no número de pessoas expostas aos riscos do ambiente virtual, podendo ser vítimas de crimes cibernéticos.

Há no país carência de legislação específica, tanto processual quanto material no campo do Direito Penal, transformando, em fonte do direito digital criminal, a atuação cotidiana do operador do direito e da segurança pública, estando aí a grande relevância da realização de estudos aprofundados sobre o tema.

Especificamente no que se refere à criminalidade cibernética mundial e brasileira, tem-se observado a intensificação da sua atuação, constituindo verdadeiras organizações criminosas, que passam a financiar a atividade de outros grupos delitivos, como traficantes de drogas, de armas, de humanos, homicidas etc.

A migração da criminalidade para o ambiente virtual provavelmente ocorre, especialmente, pelos menores riscos envolvendo a atuação criminosa, dificuldades de investigação por parte das polícias (falta de conhecimento técnico e carência estrutural) e penas brandas, em virtude da inexistência de legislação específica.

> Porque o crime organizado é uma atividade lucrativa, que atua especialmente na área do mercado ilícito (de drogas, de armas, de carros roubados etc.). Se dificuldades aparecem num determinado lugar, migra-se o crime para outros lugares, onde não existam tantos obstáculos, seja em razão da deficiência policial, seja porque poucas medidas preventivas foram adotadas, seja, enfim, pela pouca mobilização comunitária para desenvolver programas situacionais de impedimento do delito (GOMES, 2012, p.71).

Verifica-se, ainda, que os crimes tecnológicos são cíclicos, ocorrendo, precipuamente com base em falhas de segurança, seja dos *softwares* ou dos usuários, que uma vez identificadas e corrigidas, levam os criminosos a buscar outras formas de agir. Por exemplo, criminosos que controlam um site podem aproveitar a vulnerabilidade de um navegador da *web* para introduzir um cavalo de Troia no computador da vítima (NORTON SYMANTEC, 2014).

Um fator de grande relevância, que favorece a proliferação de delitos na web é a falta de informação dos usuários, que navegam na rede sem conhecer os verdadeiros riscos do ambiente virtual.

Como afirmam Cardoso et al. (2011), a popularidade das redes sociais e o crescimento a cada dia de acessos nesse ambiente, associados à ausência de noções de segurança por parte dos usuários, os quais divulgam, compartilham, e expressam a curiosidade de verem informações e se relacionarem com pessoas desconhecidas pela rede, têm estimulado cada vez mais o interesse e a migração de criminosos do mundo real para o mundo virtual, uma vez que o ciberespaço é um ótimo meio de esconderijo para esse tipo de criminoso que age valendo-se do anonimato.

A falta de informação também atinge os gestores de sociedades empresariais, pois conforme pesquisa realizada pela Internet Security System (ISS), a qual se destinava a verificar a porcentagem de empresas brasileiras que possuíam software para detectar invasores online, constatou-se que, das 100

empresas brasileiras pesquisadas, apenas 2,75% delas possuíam software para detectar invasores online (DAOUN, 1999).

Bossler e Holt (2011) realizaram pesquisa com oficiais de patrulha do Departamento de Polícia Charlotte-Mecklenburg (CMPD), em Charlotte, Carolina do Norte e o Departamento de Polícia Metropolitana Savannah-Chatham (SCMPD), em Savannah, Georgia, a fim de averiguar qual a percepção dos agentes da lei acerca da aplicação desta aos cibercrimes e estratégias de combate destes, tendo os entrevistados apontado o maior cuidado por parte dos cidadãos no ambiente virtual e melhorias para o sistema legal como melhores estratégias para lidar com tal modalidade delitiva.

Susan (2007) defende que sejam disciplinados os crimes de informática, uma vez que a tecnologia avança com rapidez no ambiente virtual, devendo haver também a capacitação dos operadores do Direito, os quais se encontram, em sua maioria, desatualizados, desinformados e despreparados para agir contra essa nova modalidade delituosa.

Vislumbra-se a necessidade de se definir quais são e como se consumam os crimes cibernéticos, uma vez que muitas vezes não passam de delitos comuns, apenas praticados por um novo meio, o tecnológico.

Colares (2012) alega, todavia, que há condutas onde o objeto da ação lesa direito relativo a bens ou dados de informática, que, em sua maioria, não encontram tipificação no ordenamento jurídico brasileiro, sendo chamados crimes informáticos, os quais podem ser perpetrados pelo meio eletrônico, que é o que rotineiramente ocorre.

Outra grande dificuldade observada no combate aos cibercrimes diz respeito à coleta e aos procedimentos legais das provas da materialidade delitiva, pois a internet, em razão de sua instantaneidade, consubstancia a possibilidade de serem eliminados, a qualquer momento, quaisquer vestígios necessários para a comprovação do delito. É como afirma Pinheiro (2000), pois independentemente do crime ser puro, misto ou comum, na maioria das vezes estes delitos ainda permanecem impunes, visto que continuam a ser novidades para os mecanismos coercitivos estatais.

O panorama dos delitos praticados em meio virtual está tão obscuro que, segundo pesquisas do Juiz Walter Fanganiello Maierovitch, apresentadas na convenção da ONU sobre crime organizado transnacional, em dezembro de 2000, na Itália, aproximadamente dois milhões de crianças foram cooptadas e escravizadas por redes internacionais criminosas para a pedofilia na internet, bem como o lucro anual da pedofilia na rede já chegava, à época, a cinco bilhões de dólares (BRAZACA et al., 2009).

Fenômeno que também se observa é a crescente prática de atos infracionais no meio virtual por adolescentes, especialmente às relacionadas ao *cyberbulling*. Para Yar (2005), entre as possíveis motivações dos adolescentes na prática de atividades delitivas pela internet, estão o tédio, conflitos familiares, resposta à sociedade, etc, ou seja, por escolha, bem como fatores psicológicos, sociais, biológicos, morais e familiares.

Ressalte-se, também, que as dificuldades das polícias no enfrentamento à cibercriminalidade não se restringem ao território brasileiro. Chan (2001) realizou pesquisas com forças policiais australianas e como a tecnologia da informação passou a influenciar nas práticas das policiais daquele país. Verificou que o surgimento de novas tecnologias da informação trouxe a reestruturação da sociedade e também das agências estatais, que tiveram que se adaptar àquela, inclusive alterando o cotidiano policial, com a automatização de processos, propiciando maior eficiência e eficácia da atuação estatal. Observou, todavia, forte resistência dos policiais a adaptar-se à nova realidade.

Além da falta de intimidade de grande parte das agências policiais com os meios tecnológicos, e a respectiva resistência a estes, observa-se que a situação é agravada pelos mesmos elementos apontados como benefícios do ciberespaço: encurtamento de fronteiras, instantaneidade, alcance global e suposto anonimato.

Quanto aos três primeiros fatores – encurtamento de fronteiras, instantaneidade e alcance global – verifica-se que foi criada uma nova modalidade criminosa, cuja atuação ou resultado é transfronteiriço ou plurilocal.

Button (2011) esclarece que as fraudes transnacionais se vulgarizaram, em razão, principalmente, do aumento de oportunidades para viajar, por vezes, com menos controle (como na União Europeia), combinado com modernos mecanismos de telecomunicações e internet, que são relativamente de baixo custo.

Kirby e Pena (2010) realizaram pesquisa com forças policiais da Inglaterra, onde foi detectado o aumento dos níveis de criminalidade móvel, o qual pressionou de modo considerável as estruturas práticas que sustentam os setores de inteligência estatal, além de desafiar a eficiência e eficácia operacionais, uma vez que apesar da atenção dada ao policiamento transnacional pela literatura que versa sobre o crime organizado, a carga de policiamento tanto sobre este, quanto ao crime oportunista, continua a recair sobre as forças policiais locais e não especializadas.

A falta de investimentos na estruturação das unidades policiais e na qualificação do efetivo, para a repressão aos crimes cibernéticos, pode ser explicada, entre outros motivos, segundo Hinduja e Patchin (2007), pelo fato

de que, comparados com crimes mais tradicionais, os delitos relacionados a computadores, muitas vezes não provocam a mesma reação do público e do sistema político – ambos influenciam fortemente a política de justiça criminal – o que resulta em apenas uma pequena quantidade de esforço e recursos alocados nessa área.

Colli e Lopes Junior (2009) sugerem às polícias, três possíveis rumos a serem seguidos para o combate eficaz dos cibercrimes, sendo eles a criação de divisões policiais especializadas, a cooperação policial (inter)nacional em conjunto com o armazenamento temporário de dados e a interpretação/aplicação adequada das normas já existentes.

Associadas aos obstáculos à investigação referentes aos delitos cibernéticos estão as dificuldades de realização da justiça criminal, sendo, conforme Magalhães e Azevedo (2003), um grande empecilho a ausência de regulamentação específica do ciberespaço, dificultando a definição de quais normas incidirão no processamento, inclusive quanto à competência para julgar.

Uma grande interrogação ocorre no momento de se verificar qual o juízo competente para analisar as representações dos órgãos investigativos por medidas cautelares, especialmente diante da plurilocalidade característica dos cibercrimes, em que, por vezes, o criminoso está em um local, a vítima em outro e o bem jurídico atingido em outro.

August (2002) afirma que os critérios de jurisdição baseados unicamente na territorialidade estão ultrapassados pelo advento da internet, devendo ser utilizados quaisquer dos nexos existentes, a fim de evitar lacunas ou injustiças e ressalta, quanto aos crimes transnacionais que para um órgão jurisdicional julgar criminosos e regulamentar sanções internacionais, deve haver alguma ligação ou nexo, entre a nação da regulação (do fórum) e o crime ou criminoso.

Muito tem se discutido, com o fulcro de sistematizar regras para a fixação da competência jurisdicional – que também é interligada com a atribuição policial para a investigação, sendo estas imprescindíveis para permitir o processamento dos cibercriminosos, com o consequente julgamento, a fim de se evitar que a impunidade impere no ciberespaço e no mundo real.

Uma vez definida a atribuição–competência para o processamento dos crimes tecnológicos, surge outra relevantíssima questão, que é a da verificação da periculosidade do agente.

Anteriormente, a violência que chocava a sociedade era apenas a física, ou a grave ameaça, com o uso da arma de fogo, por exemplo. No entanto, hoje se verifica a possibilidade de sofrimento intenso de vítimas no ambiente virtual, intensificada pelas características do ciberespaço.

Quando, por exemplo, um indivíduo exige o pagamento de certa quantia em dinheiro, sob a ameaça de que, na negativa, irá divulgar um vídeo em que a vítima aparece em cenas íntimas, poderá causar um sofrimento intenso e grave, e vir a caracterizar o crime de extorsão.

Outro exemplo corriqueiro é o de pessoas que têm poucas informações acerca dos perigos virtuais e, ao clicar em anexos de e-mails, acabam por instalar softwares maliciosos em seus computadores, possibilitando que sua conta bancária seja invadida e seus valores pecuniários subtraídos. Ao procurarem a delegacia, acabam por manifestar sofrimento e vergonha, por terem sido enganadas.

Aliam-se às características do ciberespaço, os riscos menores aos criminosos cibernéticos (já que, por vezes, sequer estão perto das vítimas), os lucros maiores e as penas previstas aos delitos, que são geralmente mais brandas.

Outro fator relevante é o de que muitos dos delinquentes que atuam em crimes tecnológicos acabam por serem presos por várias vezes, sempre com o mesmo modus operandi, não demonstrando receio de serem submetidos à ação da justiça criminal.

Desta forma, e diante da atualidade e complexidade do tema, o presente estudo objetiva analisar a manifestação da violência virtual, especialmente sob o ponto de vista legal, referente a condutas que caracterizam crime de acordo com a lei penal brasileira e que são praticadas por meio do ciberespaço.

1 A VIOLÊNCIA NOS CRIMES CIBERNÉTICOS

Os crimes tecnológicos são os cometidos utilizando-se meios eletrônicos complexos, tendo como subespécie os crimes virtuais, que são os praticados apenas pela internet. Assim, a clonagem de cartões bancários mediante o uso de um card skimming (aparelho conhecido como "chupa-cabra", que copia informações da tarja magnética de cartões) é exemplo de crime tecnológico, ao passo que o furto de dinheiro mediante a invasão de contas bancárias pela internet é um exemplo de crime virtual.

Muito se discute em virtude da pouca existência de tipos penais específicos, com afirmações de que se estaria realizando uma analogia em prejuízo aos indiciados (o que é vedado no Brasil) ao aplicar-lhes o Código Penal existente, que data de 1940, todavia já está pacificado na jurisprudência brasileira que o crime eletrônico é apenas de meio, ou seja, o efeito no mundo real é o mesmo, apenas a forma em que foi executado o delito que é mediante o uso de tecnologia.

O Supremo Tribunal Federal (STF) assim disciplina:

> Não se trata de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreende na decisão típica da conduta criminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da lei penal: a invenção da pólvora não reclamou a redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo (BRASIL STF, 1998.

Com isso, se, por exemplo, uma mulher é ofendida por seu companheiro, por meio da internet, tem-se um crime virtual, onde se aplica o Código Penal brasileiro, no que se refere ao delito contra a honra, bem como as medidas protetivas previstas na Lei Maria da Penha, ocorrendo o atendimento, em regra, na Delegacia Especializada em Atendimento à Mulher (DEAM), em razão da especificidade da matéria.

Brito (2013), ao realizar abordagem criminológica acerca dos cibercrimes, alega que a internet passa a ser sistema facilitador de crimes, comparando-a com a arma de fogo em ambiente físico, em termos de potencialidade lesiva, uma vez que é capaz de eliminar distâncias, facilitar o anonimato, diminuir os riscos pessoais e os esforços do criminoso, assim como a recompensa no final é animadora.

Consolidada a existência fática e jurídica dos crimes cibernéticos, verifica-se a ausência de legislação processual específica, que pudesse disciplinar os meios de investigação, processamento e julgamento, bem como a carência de aparatos técnicos e de qualificação dos órgãos de repressão, seja a Polícia, o Ministério Público e o Judiciário, tornando o processo penal lento e muitas vezes ineficaz.

É como afirma Pinheiro (2010):

> O maior estímulo aos crimes virtuais é dado pela crença de que o meio digital é um ambiente marginal, um submundo em que a ilegalidade impera. Essa postura existe porque a sociedade não sente que o meio é suficientemente vigiado, que os seus crimes são adequadamente punidos. O conjunto norma-sanção é tão necessário no mundo digital quanto no real. (PINHEIRO, 2010, p. 24)

Fiorillo e Conte (2013) afirmam que o crescimento da criminalidade informática, aliado ao seu rápido desenvolvimento ao longo dos últimos anos, tornou-se uma preocupação mundial, a ensejar a adoção de providências por parte de muitos países, seja por meio da subscrição a documentos internacionais de cooperação, seja por meio da promulgação de leis específicas para abarcar as novas condutas criminosas ou adaptação da legislação existente.

Destaque-se que diuturnamente são identificados pelos criminosos cibernéticos novos meios de ataque, e, uma vez realizada a repressão específica,

os suspeitos buscam novas ferramentas para consumar seus crimes, perpetuando suas práticas delitivas e causando insegurança no ciberespaço, sendo de grande importância o investimento e o aperfeiçoamento da computação forense (ELEUTÉRIO; MACHADO, 2010).

Com isso, verifica-se a intensificação dos cibercrimes, os quais trazem em si formas diferentes de exteriorização da violência, substituindo a violência física, pela violência moral, psicológica e patrimonial, as quais, em razão da ausência de definição legal específica no que se refere à sua ocorrência no ciberespaço, são definidas de forma analógica.

Visando definir violência para fins estritamente legais, pode-se adotar, genericamente, o conceito previsto no Estatuto do Idoso, que, em seu Artigo 19, § 1º, esclarece que se considera violência "qualquer ação ou omissão praticada em local público ou privado que lhe cause morte, dano ou sofrimento físico ou psicológico" (BRASIL, 2003).

Para este trabalho, adotou-se, ainda, por sua clareza, os conceitos de violência psicológica, moral e patrimonial constantes na Lei Maria da Penha, que disciplinou as formas de violência doméstica e familiar contra a mulher, mas cujas definições podem ser usadas no ordenamento jurídico analogicamente:

> Art. 7º São formas de violência doméstica e familiar contra a mulher, entre outras:
>
> I - a violência física, entendida como qualquer conduta que ofenda sua integridade ou saúde corporal;
>
> II - a violência psicológica, entendida como qualquer conduta que lhe cause dano emocional e diminuição da autoestima ou que lhe prejudique e perturbe o pleno desenvolvimento ou que vise degradar ou controlar suas ações, comportamentos, crenças e decisões, mediante ameaça, constrangimento, humilhação, manipulação, isolamento, vigilância constante, perseguição contumaz, insulto, chantagem, ridicularização, exploração e limitação do direito de ir e vir ou qualquer outro meio que lhe cause prejuízo à saúde psicológica e à autodeterminação;
>
> III - a violência sexual, entendida como qualquer conduta que a constranja a presenciar, a manter ou a participar de relação sexual não desejada, mediante intimidação, ameaça, coação ou uso da força; que a induza a comercializar ou a utilizar, de qualquer modo, a sua sexualidade, que a impeça de usar qualquer método contraceptivo ou que a force ao matrimônio, à gravidez, ao aborto ou à prostituição, mediante coação, chantagem, suborno ou manipulação; ou que limite ou anule o exercício de seus direitos sexuais e reprodutivos;
>
> IV - a violência patrimonial, entendida como qualquer conduta que configure retenção, subtração, destruição parcial ou total de seus objetos,

> instrumentos de trabalho, documentos pessoais, bens, valores e direitos ou recursos econômicos, incluindo os destinados a satisfazer suas necessidades;
>
> V - a violência moral, entendida como qualquer conduta que configure calúnia, difamação ou injúria (BRASIL, 2006)

Verifica-se a preocupação do legislador brasileiro em conceituar as formas de violência referentes a grupos considerados vulneráveis, como mulheres e idosos, por exemplo, sendo tais definições muito úteis, também, para a aplicação quanto aos crimes cibernéticos, tão novos e tão atuais, no Brasil e no mundo, até porque muitos são os usuários de internet que se mostram em situação de vulnerabilidade quanto aos riscos do ciberespaço.

Mais especificamente, observa-se que no mundo globalizado as ameaças e os crimes contra a honra (injúria, calúnia e difamação) em redes sociais, incluindo o cyberbullying; a pornografia infanto-juvenil na internet; as extorsões; as fraudes em comércio eletrônico e bancárias etc., trazem em si além da violência patrimonial, a moral e psicológica, intensificadas em razão de as vítimas dificilmente verem seus agressores processados e, quando são submetidos a um processo penal e presos (nos crimes em que a prisão é cabível) muitas vezes acabam postos em liberdade logo em seguida pelo Poder Judiciário, em virtude de considerarem que o aquele criminoso não é "violento", logo não é "perigoso".

A abordagem acerca dessas formas de violência a que as vítimas de crimes tecnológicos são submetidas ganha ainda mais relevância quando se ressalta que, em 9 anos, a SaferNet Brasil (2015), organização não governamental especializada, recebeu e processou 3.606.419 denúncias anônimas envolvendo 585.778 páginas distintas escritas em 9 idiomas e hospedadas em 72.739 hosts (servidores) diferentes, conectados à internet por meio de 41.354 números de IP distintos, atribuídos para 96 países em 5 continentes, destacando-se que as denúncias foram registradas pela população por meio dos 7 hotlines (canais) brasileiros que integram a Central Nacional de Denúncias de Crimes Cibernéticos.

Em nível mundial, os hosts ou servidores que apresentaram mais denúncias à Safer Net Brasil, de 2006 a 2014, se referem a redes sociais, entre estas o orkut.com.br, com 200.221 registros; orkut.com, com 143.691; facebook.com 59.361; images.orkut.com, contando com 13.437, e twitter, com 11.962 denúncias (SAFERNET BRASIL, 2015).

Ainda de acordo com a Safernet Brasil (2015), o Brasil aparece em 2º lugar, se for colocado como parâmetro o IP (número atribuído pelo provedor ao usuário para acesso à internet), segundo a origem, no período de 2006 a 2014, contando com 4.532 registros, perdendo apenas para os Estados Unidos

da América, que possuem 24.392 denúncias. Isso significa que, das denúncias computadas pela instituição, o Brasil apresenta o segundo maior número de criminosos cibernéticos na escala mundial.

Vislumbra-se claramente a incidência da violência moral e psicológica, por ocasião da análise dos registros, por tipo de conteúdo, em páginas distintas, de 2006 a 2014 (SAFERNET BRASIL, 2015), haja vista que sequer os ofensores têm contato físico com os ofendidos, mas são capazes de realizar crimes terríveis, com graves consequências às vítimas, destacando-se, no caso, a pornografia infantil, com 4.909 registros e racismo pela internet, com 4012 páginas denunciadas.

Também são relevantes os dados divulgados pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br, 2015), demonstrando que houve, em 2014 um aumento de 297% no total de incidentes reportados, em comparação com o ano de 2013, sendo 1.047.031 e 352.925 registros, respectivamente. Desses incidentes reportados em 2014, 44,66% se referem a fraudes (CERT.BR, 2015).

No Pará, no ano de 2013, foram registrados no Sistema Integrado em Segurança Pública (SISP), 245 boletins de ocorrência policial (BOP), sob a responsabilidade da unidade 487, referente à Delegacia de Repressão a Crimes Tecnológicos (DRCT). Isto significa que a citada unidade registrou ou recebeu os referidos BOP, estes registrados em outras unidades policiais de qualquer parte do Estado, mas que os registradores entenderam ser de atribuição da DRCT, em razão de terem sido praticados utilizando-se ou com auxílio de meios tecnológicos, em tese, estes entendidos como dispositivos eletrônicos com capacidade de transmissão e recebimento de dados, especialmente pela internet.

Analisando-se o quantitativo de registros de BOP da DRCT por crimes, no ano mencionado, verificou-se que as fraudes – que manifestam a violência patrimonial e psicológica – constituíram a maioria dos registros recebidos pela unidade policial especializada, com mais de 71% das ocorrências (estelionato, 36%; furto mediante fraude, 25%; falsa identidade, 3%; falsidade ideológica, 2%; falsificação de documento particular, 2%; falsificação de documento público, 2%; uso de documento falso, 1%); os crimes contra a honra (injúria, difamação e calúnia) representaram 8% dos registros; já as ameaças, 2%, sendo que nestes dois últimos grupos vislumbra-se, claramente, a ocorrência de violência moral e psicológica.

Esse resultado se coaduna com o observado no restante do país (conforme os dados já expostos tanto da SaferNet Brasil, quanto do Cert.Br), demonstrando que os cibercrimes representam uma preocupação da atualidade, merecendo a atenção devida, não só quanto ao enfrentamento, mas também no que se refere à prevenção.

Nesse novo panorama, a periculosidade dos agentes que praticam delitos eletrônicos (ou *crackers*) acaba por ser *sui generis*, mas tão concreta quanto a de assaltantes do mundo real, até porque a rede mundial de computadores e outras tecnologias da informação e comunicação, são potencializadas condutas criminosas, havendo, por exemplo, centenas de vídeos ensinando a invadir páginas de instituições bancárias; a pescar senhas de usuários; a ludibriá-los; diversos fóruns de troca de materiais com conteúdo de pornografia infantil, racismo, homofobia e etc.

Aliados à facilidade em obter conteúdo técnico na rede para a prática dos meios diversos crimes tecnológicos, estão a possibilidade do anonimato; o pouco ou nenhum contato físico com as vítimas; os grandes lucros; a intensidade dos prejuízos que podem ser causados; a desorganização do Estado, seja pela pouca atuação legislativa, seja pelo baixo preparo específico dos órgãos de justiça criminal, de modo a atrair criminosos aos novos meios de praticar delitos.

A intensidade dos prejuízos que podem ser causados às vítimas também é preponderante no estímulo aos crimes tecnológicos, onde os cibercriminosos escolhem praticar os delitos pela internet, justamente em razão da "viralização" (quando centenas de pessoas passam a compartilhar conteúdos), permitindo maior humilhação e, consequentemente, intensos danos psicológicos e morais relativos ao seu alvo.

Neste sentido, é imperioso analisar, abstratamente, condutas tipificadas nas leis penais brasileiras como sendo crimes e que podem ser praticadas no ciberespaço, e a manifestação da violência virtual relativa a estas.

Nos crimes contra honra, por exemplo, sendo estes a calúnia (Art. 138, do CPB), que se caracteriza quando o agente atribui à vítima falsamente fato definido como crime, ou quando alguém, sabendo falsa a imputação, a propala ou divulga, inclusive por meios eletrônicos. Já a difamação (Art. 139, do CPB) incrimina a conduta de imputar fato ofensivo à reputação de alguém, expondo-o às críticas sociais, atingindo a honra objetiva da vítima, ou seja, o que a sociedade pensa dela. Na injúria (Art. 140, do CPB), o autor ofende a dignidade ou o decoro da vítima, ou seja, o que esta pensa sobre si, trazendo uma qualificadora que ocorre quando as ofensas consistem na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência (BRASIL, 1940).

Constata-se nesses crimes a violência moral e a psicológica, tal qual foram descritas pelo legislador brasileiro, no parâmetro legal ora utilizado por empréstimo, qual seja, a Lei Maria da Penha (BRASIL, 2006).

Outro exemplo de manifestação da violência psicológica e da moral é a conhecida como "vingança pornô", onde são divulgadas fotografias ou vídeos íntimos de adultos nas redes sociais e sites de pornografia e prostituição, sem a autorização da vítima (crime de difamação), normalmente por alguém com quem esta já teve algum tipo de relacionamento e com o intuito de trazer–lhe transtornos. Tais formas de violência atingem tão fortemente as vítimas, que já há casos no Brasil de mulheres que se suicidaram, após terem seus vídeos íntimos divulgados rede mundial de computadores. A violência virtual por parte de alguns ofensores é tão intensa, que por vezes chegam a associar os perfis reais das vítimas em redes sociais aos vídeos pornográficos, para que os demais internautas não tenham dúvidas quanto à identidade daquelas.

As ameaças (Art. 147, do CPB) também podem caracterizar a violência psicológica, em sua definição legal, haja vista que o criminoso, por e-mail, por exemplo, pode prometer à vítima a prática de mal injusto e grave (BRASIL, 1940).

As fraudes, por sua vez, caracterizam-se pela indução ou manutenção de alguém em erro, com o fim de obtenção de vantagens diversas, como ocorre no estelionato (Art.171, do CPB) e no furto mediante fraude (Art. 155, parágrafo 4º, inciso II, do CPB), cujos exemplos são vendas fraudulentas no comércio eletrônico e a transferência de valores de contas bancárias invadidas pela internet, respectivamente (BRASIL, 1940).

Nos casos acima, verifica-se, além da violência patrimonial, a psicológica, uma vez que o criminoso visa manipular e explorar a vítima, passando-lhe falsa percepção da realidade, trazendo-lhe humilhação e sofrimento, ao perceber ter sido enganada e despojada de seus bens e/ou valores, de forma ardilosa.

O tipo previsto no Art. 241-D, do Estatuto da Criança e do Adolescente (ECA), criminaliza as condutas de aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, inclusive a internet, criança, com o fim de com ela praticar ato libidinoso, bem como de facilitar ou induzir o acesso à criança de material contendo cena de sexo explícito ou pornográfica com o fim de com ela praticar ato libidinoso, e, ainda, induzir criança a se exibir de forma pornográfica ou sexualmente explícita (BRASIL, 1990).

A gravidade das condutas previstas na figura penal acima citada não deixa dúvidas quanto à manifestação da violência psicológica inerente, uma vez que o agente, para fins sexuais, ilude, chantageia, ameaça ou coage crianças, causando-lhes males irreparáveis.

Assim, quando uma vítima adulta tem um vídeo íntimo seu ou mesmo um xingamento contra si divulgado em redes sociais, caracteriza-se, no máximo, o crime de difamação, por exemplo, o que leva ao questionamento seguinte:

tem a mesma proporção xingar uma pessoa em uma sala contendo outros vinte indivíduos e o fazer em um ambiente virtual, onde milhões de internautas terão acesso àquele conteúdo difamatório? Carece o Brasil de uma alteração legislativa que inclua no Código Penal causa de aumento de pena para os casos em que os crimes sejam cometidos em ambientes que facilitem sua propagação e perpetuação ("viralização").

Além da carência legislativa brasileira específica, reitera-se que a realidade é a da pouca ou nenhuma qualificação dos diversos integrantes do sistema de justiça criminal para o enfrentamento aos crimes tecnológicos, desde as polícias, os institutos periciais, o Ministério Público e o Judiciário.

Muitos desses profissionais ao se depararem com situações de crimes que envolvem o uso de tecnologia não sabem como agir, por vezes apegados ainda ao excesso de formalismo e a conceitos ultrapassados, incompatíveis com a era digital.

Assim, urge que o sistema de justiça criminal se conscientize de que os crimes eletrônicos são uma realidade e passe a qualificar seus agentes, para que o enfrentamento se dê de forma eficaz, para, ao menos, começar a desestimular o exponencial aumento de crimes tecnológicos e a adesão de novos criminosos.

Importantíssimo é, ainda, que os operadores da segurança pública e do Direito compreendam as formas de violência manifestadas pelos criminosos digitais, quais sejam, a moral, psicológica e a patrimonial, pois poucos delinquentes tecnológicos são penalizados, já que a maioria dos julgadores acreditam que aqueles não são perigosos, entendendo a periculosidade apenas como a de cometer a violência física ou a grave ameaça ao físico da vítima.

CONCLUSÃO

Atividades hoje corriqueiras na vida virtual dos cidadãos podem trazer riscos ainda pouco conhecidos pelos usuários dos meios tecnológicos, os quais incorporaram a tecnologia em seu cotidiano, muitas vezes olvidando-se que os criminosos também o fizeram.

Neste sentido, é importante destacar que a preocupação com os efeitos dos ciberdelitos merece abordagem em nível mundial, uma vez que em 2016 houve um acréscimo de 10% no número de ataques virtuais no mundo em relação a 2015, sendo que, só no Brasil, 42,4 milhões de pessoas foram afetadas e tiveram um prejuízo total de 10,3 bilhões de dólares (CONVERGÊNCIA DIGITAL, 2016).

No que se refere aos sujeitos passivos dos delitos eletrônicos: "observa-se que qualquer pessoa pode acabar sendo vítima de crimes cibernéticos, uma vez que os criminosos utilizam técnicas cada vez mais apuradas de engenharia social, aliadas às novas tecnologias, atingindo, assim, muitas pessoas" (BARRETO; BRASIL, 2016, p. 32)

Os ciberdelinquentes aproveitam-se da vulnerabilidade de seus alvos, podendo esta ser técnica (pouca habilidade em se defender de ataques virtuais) como também emocional e/ou psicológica (crianças, adolescentes, idosos, pessoas que passaram por traumas emocionais, como separação ou viuvez), conseguindo, então garantir os proveitos de seu intento criminoso, seja por meio de prejuízos patrimoniais, morais e/ou psicológicos.

Esta realidade parece estar começando a ser percebida pelos usuários do mundo virtual, uma vez que 48% dos pais acreditam que seus filhos estão mais inclinados a sofrerem bullying online do que no ambiente real, sendo que, em 2015, apenas 23% dos genitores tinham essa mesma percepção (CONVERGÊNCIA DIGITAL, 2016).

Nesse contexto, ao serem praticados cibercrimes, estes entendidos como aqueles previstos na legislação penal brasileira comum e praticados por meio da internet e/ou outras tecnologias da comunicação e da informação, vislumbra-se a consolidação da violência virtual, que afeta a vítima não só em âmbito patrimonial, mas também moral e psicologicamente, contrapondo-se à violência física – que só é possível de ocorrer no ambiente real – mas tão perniciosa como esta, por ser capaz de abalar profundamente a dignidade humana, conforme exposto no decorrer deste trabalho.

A proteção dos direitos humanos na internet perpassa pela compreensão de que os crimes cometidos no ciberespaço trazem em si formas de violência graves, que, mesmo que não sejam capazes de abalar o corpo físico do indivíduo, atingem-lhe outros bens igualmente preciosos e que merecem proteção social e estatal.

Assim, urge a discussão aprofundada das formas de violência que afetam os cidadãos no mundo globalizado, bem como o aperfeiçoamento legislativo e a qualificação (e familiarização quanto às ferramentas eletrônicas) dos integrantes do sistema de justiça criminal (Polícias, Ministério Público, Judiciário, etc.) e da sociedade, para a realização do adequado e cooperativo enfrentamento e prevenção à criminalidade tecnológica, que se expande no Pará, no Brasil e no Mundo.

REFERÊNCIAS

ANGELUCI, R. A.; SANTOS, C. A. A. C. **Sociedade da Informação:** O mundo virtual *second life* e os crimes cibernéticos, 2007. Disponível em: <http://www.migalhas.com.br/dePeso/16,MI46552,101048-Sociedade+da+informacao+O+mundo+virtual+Second+Life+e+os+crimes>. Acesso em: 12 set. 2013.

AUGUST, R. International cyber-jurisdiction: a comparative analysis. **American Business Lawjournal,** Washington, p. 531-573, jun. 2002.

BARRETO, A. G.; BRASIL, B. S. **Manual de Investigação Cibernética:** à luz do Marco Civil da Internet. Rio de Janeiro: Brasport, 2016.

BERGMANN, E. **Constituição colaborativa da Islândia serve de exemplo ao Brasil.** Porto Alegre. 23 de maio de 2013. Portal Terra: Déborah Salves, 2013. Disponível em: http://tecnologia.terra.com.br/internet/constituicao-colaborativa-da-islandia-serve-de-exemplo-ao-Brasil,f9f3a0b2993de310VgnVCM3000009acceb0aRCRD.html. Acesso em: 07 jul. 2013.

BONAVIDES, P. **Curso de Direito Constitucional.** São Paulo: Malheiros, 2008.

BOSSLER, A. M.; HOLT, T. J. **Patrol officers perceived role in responding to cybercrime, 2011.** Disponível em: <www.emeraldinsight.com/1363-951X.htm>. Acesso em: 20 set. 2013.

BRASIL. Lei nº 11.340, de 07 de agosto de 2006. **Lei Maria da Penha**. Brasília, 07 ago de 2006.

_____. Lei nº 10741, de 01 de outubro de 2003. Dispõe sobre o Estatuto do Idoso e dá outras providências. **Estatuto do Idoso.** Brasília, 03 out. 2003.

_____. Supremo Tribunal Federal. **HC 76689/PB**. DJE 22 de setembro de 1998. Disponível em: http://stf.jusbrasil.com.br/jurisprudencia/740355/habeas-corpus-hc-76689-pb. Acesso em: 20 set. 2013.

_____. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. **Estatuto da Criança e do Adolescente**. Brasília, 1990.

_____. Decreto-lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Rio de Janeiro, 1940.

BRAZACA, A.; SANTOS, G. R. dos; WERKHÄUSER, S.; MARTINS, P. C. R. **Pedofilia e Internet:** A intervenção do estado e o poder econômico, 2009. Disponível em: http://www.upf.br/seer/index.php/rjd/article/view/2166/1398. Acesso em: 12 set. 2013.

BRITO, A. **Direito Penal Informático.** São Paulo: Saraiva, 2013.

BUTTON, M. **Cross-border fraud and the case for an "Interfraud", 2011.** Disponível em: <www.emeraldinsight.com/1363-951X.htm>. Acesso em: 20 set. 2013.

CARDOSO, N. M.; HASHIMOTO, Y. C.; SILVA, K. M. D.; MAIA, A. T. **Redes sociais a nova arma do crime cibernético:** o efeito do uso da engenharia social e da esteganografia, 2011. Disponível em: http://dx.doi.org/10.5769/C2011023. Acesso em: 12 set. 2013.

CASTELLS, M. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar, 2003.

CERT.BR - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Incidentes Reportados ao CERT.br 2014**. Disponível em: http://www.cert.br/stats/incidentes/. Acesso em: 16 mar. 2015.

CHAN, J. B. L. **The Technological Game:** How Information Technology is Transforming Police Practice, 2001. Disponível em: <http://crj.sagepub.com/content/1/2/139>. Acesso em: 20 set. 2013.

COLARES, R. G. **Cybercrimes: os crimes na era da informática. Revista Eletrônica InfoDireito**, 2012. Disponível em: http://www.infodireito.com.br/infodir/index.php?option=com_content&task=view&id=23&Itemid=42. Acesso em: 12 set. 2013.

COLLI, M.; LOPES JUNIOR, A. **Cibercrimes:** limites e perspectivas da investigação preliminar policial brasileira de crimes cibernéticos, 2009. Disponível em: http://tede.pucrs.br/tde_busca/arquivo.php?codArquivo=2477. Acesso em: 12 set. 2013.

CONVERGÊNCIA DIGITAL (Brasil). **Ataques hackers provocaram um prejuízo de R$ 30 bilhões no Brasil.** 2016. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=44019&sid=18>. Acesso em: 16 nov. 2016.

DAOUN, A. J. Os novos crimes de informática. **Jus Navigandi**, Teresina, v. 4, n. 37, 1 dez. 1999. Disponível em: http://jus.com.br/artigos/1827. Acesso em: 14 set. 2013.

DEIBERT, R. J.; ROHOZINSKI, R. Risking Security: Policies and Paradoxes of Cyberspace Security. **International Political Sociology**, Toronto, v. 4, n. 1, p. 15-32, mar. 2010.

ELEUTÉRIO, P. M. S.; MACHADO, M. P. **Desvendando a computação forense.** São Paulo: Novatec, 2010.

ERDELYI, M. F. **Itamaraty ainda estuda adesão à convenção de Budapeste.** Brasília, Consultor Jurídico, 2008. Disponível em: http://www.conjur.com.br/2008-mai-29/itamaraty_ainda_estuda_adesao_convencao_budapeste. Acesso em: 30 set. 2013.

FIORILLO, C. A. P.; CONTE, C. P. **Crimes no meio ambiente digital.** São Paulo: Saraiva, 2013.

GOMES, L. F. **Crime organizado:** migração e busca de lucro fácil. Disponível em: http://marioleitedebarrosfilho.blogspot.com.br/2012/07/crime-organizado-migracao-e-busca-de.html. Acesso em: 20 out. 2012.

HINDUJAA, S.; PATCHIN, J. W. Offline consequences of online victimization: School violence and delinquency. **Journal of School Violence***, v. 6, n.* 3, p. 89-112, 2007.

HUNGRIA. **Convenção sobre o cibercrime.** Budapeste, 2001.

IBOPE – Instituto Brasileiro de Opinião Pública e Estatística. **Número de pessoas com acesso à internet passa de 100 milhões**. 2013. Disponível em: http://www.ibope.com.br/pt-br/noticias/Paginas/Numero-de-pessoas-com-acesso-a-internet-passa-de-100-milhoes.aspx. Acesso em: 30 set. 2014.

KIRBY, S.; PENNA, S. **Policing mobile criminality:** implications for police forces in the UK, 2010. Disponível em: <www.emeraldinsight.com/1363-951X.htm>. Acesso em: 20 set. 2013.

LISBOA, R. S. **Direito na sociedade da informação.** São Paulo: Revista dos Tribunais, 2006.

MAGALHÃES, D. F.; AZEVEDO, L. H. B. **Estudo da eficiência jurisdicional no direito cibernético. Revista Eletrônica do Ministério Público do Estado de Goiás**, 2003. Disponível em: http://dialnet.unirioja.es/servlet/articulo?codigo=4061630. Acesso em: 12 set. 2013.

NORTON SYMANTEC. **O que é crime cibernético?** 2014. Disponível em: <http://br.norton.com/cybercrime-definition>. Acesso em: 20 dez. 2014.

PINHEIRO, P. P. **Direito Digital.** São Paulo: Saraiva, 2010.

PINHEIRO, R. C. Os cybercrimes na esfera jurídica brasileira. **Jus Navigandi**, Teresina, v. 5, n. 44, 1 ago. 2000. Disponível em: http://jus.com.br/artigos/1830. Acesso em: 14 set. 2013.

SAFERNET BRASIL (Brasil). **Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos**. 2015. Disponível em: <http://indicadores.safernet.org.br/index.html>. Acesso em: 02 abr. 2015.

SANTOS, C. A. A. C.; FONSECA, F. N. **Marco civil e as investigações no espaço cibernético. 2010.** Disponível em: http://www.icofcs.org/2010/ICoFCS2010-FULL.pdf#page=50. Acesso em: 12 set. 2013.

SUSAN, S. R. **Sanção e coação:** uma perspectiva para os crimes de internet. **Sistema Anhanguera de Revistas Eletrônicas**, 2007. Disponível em: http://www.sare.anhanguera.com/index.php/anuic/article/view/2001/887>. Acesso em: 12 set. 2013.

YAR, M. Computer hacking: just another case of juvenile delinquency? **The Howard Journal,** Canterbury, p. 387-399, 01 set. 2005.

Texto submetido à Revista em 13.03.2016
Aceito para publicação em 08.12.2016