UNIVERSIDADE FEDERAL DO PARÁ
INSTITUTO DE FILOSOFIA E CIÊNCIAS HUMANAS
PROGRAMA DE PÓS- GRADUAÇÃO EM SEGURANÇA PÚBLICA

A Violência na Prática de Crimes no Ciberespaço

Beatriz de Oliveira da Silveira

Belém-PA

2015

Beatriz de Oliveira da Silveira

A Violência na Prática de Crimes no Ciberespaço

Dissertação apresentada ao Programa de Pós-Graduação em Segurança Pública – PPGSP, da Universidade Federal do Pará, como requisito parcial para obtenção do título de Mestre em Segurança Pública.

Área de Concentração: Segurança Pública.

Linha de Pesquisa: Conflitos, criminalidade e Tecnologia da Informação.

Orientador: Prof. Edson Marcos Leal Soares Ramos, *Dr*.

Coorientadora: Profa. Silvia dos Santos de Almeida, *Dra*.

Belém-PA

2015

A Violência na Prática de Crimes no Ciberespaço

Beatriz de Oliveira da Silveira

Esta Dissertação foi julgada e aprovada, para a obtenção do grau de Mestre em Segurança Pública, no Programa de Pós-graduação em Segurança Pública, da Universidade Federal do Pará.

.

_____

Prof. Edson Marcos Leal Soares Ramos, *Dr*.
(Coordenador do Programa de Pós-graduação em Segurança Pública)

Banca Examinadora

_____

Prof. Dr. Edson Marcos Leal Soares Ramos
Universidade Federal do Pará
Orientador

_____

Profa. Dra. Silvia dos Santos de Almeida
Universidade Federal do Pará
Coorientadora

_____

Profa. M.Sc. Adrilayne dos Reis Araújo
Universidade Federal do Pará
Avaliadora

_____

Profa. Dra. Maély Ferreira Holanda Ramos
Universidade Federal do Pará
Avaliadora

_____

Prof. Dr. Wilson José Barp
Universidade Federal do Pará
Avaliador

Dedicatória

Aos meus pais, Tereza e Antonio, por terem inspirado em mim valores fundamentais, como honestidade, perseverança e dedicação, mostrando-me que a educação é a melhor herança que podemos deixar aos nossos filhos.

Ao meu marido, Marcos, meu companheiro de todos os momentos, bons e ruins, que divide comigo os sonhos e a realidade.

Às minhas filhinhas tão amadas, por quem eu procuro sempre me superar, especialmente como mãe, para a formação de mulheres seguras, honestas, boas e batalhadoras.

Agradecimentos

Ao Marcos, pelo apoio constante. À Carolina, que muitas vezes foi às aulas comigo, mesmo tão bebezinha, para que eu não desistisse do presente projeto; à Sophia e à Luiza, que compreenderam a minha ausência nesses momentos.

Ao meu Orientador, Prof. Dr. Edson Ramos, pelo apoio incondicional, paciência e exemplo acadêmico.

À Profa. Dra. Silvia Almeida, minha coorientadora, pela ajuda de grande valia.

Ao Dr. Luiz Fernandes Rocha, então Secretário de Segurança Pública, por possibilitar a realização do presente curso, visando a qualificação dos profissionais da segurança pública do Estado do Pará.

À Polícia Civil do Estado do Pará, instituição da qual faço parte e que me proporcionou essa vivência acadêmica.

Aos meus colegas de mestrado, pela oportunidade de convivência engrandecedora.

À UFPA e aos professores do curso de mestrado, por terem alargado meus horizontes teóricos e práticos, no que se refere à Segurança Pública.

(…) Ainda que eu ande pelo vale da sombra da morte, não temerei mal algum, pois tu estás comigo; a tua vara e o teu cajado me protegem (Salmo 23, Davi).

RESUMO

SILVEIRA, Beatriz de Oliveira da. A Violência na Prática de Crimes no Ciberespaço. 2015. Dissertação (Mestrado em Segurança Pública) PPGSP, UFPA, Belém, Pará, 2015.

O presente estudo objetivou identificar e analisar a exteriorização da violência na prática de crimes no ciberespaço, entendido este como o ambiente virtual, propiciado pela internet e outras ferramentas tecnológicas, cujas peculiaridades englobam o tráfego intenso e instantâneo de informações, na atual Era da Informação. A metodologia adotada foi pesquisa em livros e artigos acerca do tema, além da análise de procedimentos policiais, a fim de contextualizar a sociedade digital, suas peculiaridades e definições. Ainda, adotou-se a técnica estatística descritiva, para a análise de dados estatísticos referentes a registros de boletins de ocorrência policial, sob a responsabilidade da Delegacia de Repressão a Crimes Tecnológicos da Polícia Civil do Estado do Pará, no ano de 2013. Dessa forma, verificou-se que os tipos penais com mais registros na unidade policial adotada como parâmetro, no ano elencado, totalizando 81% das ocorrências, trazem em si elementos indicativos da violência psicológica, moral e patrimonial, definidas em termos legais, cujas práticas, no mundo cibernético, possibilitam aos cibercriminosos maiores lucros com menores riscos.

Palavras-chave: Virtual. Cibercriminosos. Violência Moral. Violência Psicológica. Violência Patrimonial.

ABSTRACT

SILVEIRA, Beatriz de Oliveira da. The Violence in Cybercrimes. 2015. Dissertation (Master of Public Security) PPGSP, UFPA, Belém, Pará, 2015.

This study aimed to identify and analyze the manifestation of violence in crime in cyberspace, understood as the virtual environment, brought about by the Internet and other technological tools whose peculiarities include the intense and instant traffic information in the current Information Age. The methodology adopted was research in books and articles on the subject, as well as analysis of police procedures in order to contextualize the digital society, its peculiarities and definitions. Also adopted the descriptive statistical technique for the analysis of statistical data on records of police reports, under the responsibility of Enforcement Police Technological Crimes of the Pará State Civil Police, in 2013. Thus, it was found that the criminal types with more records in the police unit adopted as a parameter, in 2013, totaling 81% of cases, bring it self indicative information on the psychological, moral and equity, defined in legal terms, whose practices in the virtual world, enable cybercriminals to higher profits with less risk.

Keywords: Virtual. Cybercriminals. Moral violence. Psychological violence. Property violence.

SUMÁRIO

CAPÍTULO I

1.1. Introdução

Especialmente a partir da década de 1990, a internet e outras tecnologias da informação e conhecimento (TIC), como as comunicações por satélite e o bluetooth, passaram a integrar-se ao cotidiano de um grande número de indivíduos, fazendo surgir o ambiente virtual, onde é possível se relacionar com outras pessoas, trabalhar, fazer compras, vender bens, jogar, ouvir músicas, conhecer outras culturas, etc, despertando "nos novos ideólogos da modernização ou do capital, um interesse ímpar em se entender como as TIC contribuem para uma nova dinâmica na sociedade" (ALENCAR, 2014).

A nova sociedade, trazida pela chamada Era da Informação ou Era do Conhecimento, privilegia o fluxo intenso de informações em tempo cada vez menor, otimizando, assim processos, facilitando desde a atividades corriqueiras a processos tecnológicos complexos.

> A informática e seus deslindes afetam de maneira uniforme toda a sociedade global, uma vez que a tecnologia mostra-se imprescindível para o evoluir humano. Exceção feita a segmentos cada vez mais diminutos que a informática não atinge, todos estamos permeados pelos conceitos da tecnologia, que apresenta suas vantagens inquestionáveis (SYDOW, 2013).

Justamente em razão da facilidade de acesso à internet e outras tecnologias, passou-se a verificar a incidência de crimes no ambiente virtual, atingindo diversas pessoas, por vezes ao mesmo tempo, em diversas partes do globo terrestre.

Muito se discutiu acerca da existência dos crimes cibernéticos, mas hoje, em razão da consolidação da sociedade virtual, verifica-se que não só ocorrem, como trazem aspectos peculiares ao próprio meio onde se manifestam.

> Em que pesem inúmeros benefícios, esses mesmos recursos – hoje indispensáveis – apresentam diversos riscos, pois muitos deles podem proporcionar transtornos ou prejuízos para as vítimas. Nestas situações e existindo previsão penal, surgem os denominados crimes cibernéticos, que se caracterizam pela prática de delitos no ou por intermédio do ambiente cibernético, ou seja, da internet. Pode-se afirmar, mesmo que por uma análise empírica, que a ocorrência desses crimes apresenta um

> crescimento acentuado, seja pelo aumento do número de usuários, pelas vulnerabilidades existentes na rede ou pela falta de atenção do usuário (WENDT; JORGE, 2012).

Muitos dos criminosos que outrora atuavam no mundo real, estão atualmente praticando crimes no ciberespaço, valendo-se, sobretudo da sensação de anonimato e impunidade, especialmente em razão das penas dos crimes serem geralmente mais brandas.

Somam-se a isso os lucros maiores das empreitadas criminosas, em razão de no ambiente cibernético haver a possibilidade de se atingir mais vítimas, inclusive à distância, o que também diminui os riscos de serem os delinquentes presos em flagrante delito.

Castells (2003) define a nova criminalidade como "(…) cibercrime - a prática de roubo na internet para lucro pessoal - o velho hábito do "crime do colarinho branco" executado mediante novos meios tecnológicos".

É possível, por exemplo, ofender pessoas em redes sociais, fazendo com que aquela ofensa se perpetue na vida do ofendido, uma vez que outros indivíduos acabam por ter acesso, compartilhar e comentar aquela postagem. Também é possível, por exemplo, invadir centenas de contas bancárias pela internet, subtraindo dinheiro daquelas, sem autorização do respectivo titular.

Cada cibercrime perpetrado, significa uma vítima lesada, além de um abalo à ordem social. No entanto, em razão de a conduta utilizar o meio virtual para ser configurada, observa-se uma cultura nos órgãos de justiça criminal de que cibercriminosos não são perigosos, pois não há a violência física.

Não haver violência física, em tese, nos crimes cibernéticos, não quer dizer não haver violência. É como diz Zaluar (2004): "É a percepção do limite e da perturbação (e do sofrimento causado), que vai caracterizar um ato como violento, percepção que varia cultural e historicamente".

Definir violência não é elementar, e mesmo que se esgotasse toda a literatura acerca do tema, dificilmente haveria um conceito uníssono, motivo pelo qual, neste trabalho, adotar-se-á, utilizando-se da técnica da interpretação analógica, o conceito legal das formas de violência previstas na Lei Nº. 11.340/2006.

Assim, contextualizando-se a ocorrência de crimes cibernéticos, visa-se verificar quais as formas de violência neles manifestas, as quais merecem atenção não só de estudiosos, como do próprio Estado.

1.2. Justificativa

Os usuários da internet e outras tecnologias da informação estão expostos a diversos riscos no ciberespaço, inclusive de virem a ser vítimas de crimes. Entretanto, em razão da recenticidade do tema, verifica-se a deficiência no tratamento deste, não só pela própria sociedade, onde muitas pessoas utilizam a internet sem observar requisitos mínimos de segurança, tais como a utilização de programas de proteção, por exemplo, como também pelo Estado, que despende pouca atenção à discussão do assunto, por não chamar atenção em razão da violência física, como os roubos a banco e homicídios, por exemplo.

Dessa forma, é imprescindível estudar as novas formas de violência potencializadas pelos atributos da sociedade digital, nos crimes praticados por meios tecnológicos, como forma de entender o fenômeno que ora se mostra e, assim, realizar a prevenção e enfrentamento adequados.

1.3. Problema

Como compreender as formas de violência incidentes nos crimes tecnológicos mais registrados na unidade policial especializada no Pará, no ano de 2013?

1.4. Hipótese

Os crimes tecnológicos marcam a sociedade virtual, atingindo, diuturnamente, pessoas de todos os níveis sociais, trazendo, instrinsecamente, novas formas de violência, uma vez que, visando obter êxito, o criminoso atinge a moral, o emocional e o psicológico de suas vítimas.

1.5. Objetivos

1.5.1. Geral

Identificar quais as formas de violência são traduzidas nos crimes praticados por meios tecnológicos, que tanto afetam a sociedade digital.

1.5.2. Específicos

i) Mostrar quais são as características da sociedade digital;
iii) Estudar as formas de violência detectadas na análise dos crimes tecnológicos mais incidentes.

1.6. A Manifestação da Violência no Cibercrime

Foi realizada a pesquisa em livros e artigos, bem como a leitura de procedimentos policiais lavrados na DRCT, a fim de contextualizar o presente trabalho, descrevendo os principais atributos da Sociedade da Informação e dos cibercimes, seus modos de execução e ocorrência.

Em seguida, foi solicitada autorização ao Delegado Geral da Polícia Civil, para que a Diretoria de Informática, Manutenção e Estatística (DIME) fornecesse o recorte do banco de dados da unidade 487, da Delegacia de Repressão a Crimes Tecnológicos (DRCT), no Sistema Integrado em Segurança Pública (SISP), referente ao ano de 2013.

Através do SISP são registradas todas as ocorrências e procedimentos policiais no Estado do Pará, sendo que os registros tramitam automaticamente para a unidade policial mais

próxima ao local do fato criminoso, podendo também permanecer na unidade, ou ainda, tramitado para uma delegacia especializada, como é o caso da DRCT.

Dessa forma, passou-se a analisar o recorte do banco de dados da DRCT, do ano de 2013, tomando-se como parâmetro apenas as ocorrências que permaneceram sob a responsabilidade da unidade 487, ou seja, ou que foram registradas já na DRCT e não tramitaram para outras unidades ou que foram tramitadas de outras unidades para a DRCT.

Foram identificados 245 boletins de ocorrência na unidade 487, dos quais foi procedida a leitura, a fim de verificar se a capitulação penal provisória aposta, correspondia ao descrito no texto do registro.

Utilizando-se a técnica estatística descritiva, foram confeccionadas tabelas e gráficos, podendo-se constatar que as fraudes constituem a grande maioria dos registros recebidos pela unidade policial especializada, com mais de 71% das ocorrências, manifestando-se como 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, sendo eles a injúria, difamação e calúnia representaram 8% dos registros, e, as ameaças, 2%.

Utilizando-se a técnica jurídica da interpretação analógica, foram cotejados os tipos penais identificados nos registros de BOPs analisados com a definição legal de formas violência trazida na Lei Maria da Penha, conforme o quadro abaixo.

Quadro 1. Principais tipos penais sob a responsabilidade da DRCT em 2013, relacionados com as formas de violência incidentes

Registros mais mais incidentes na DRCT, 2013			Violência Psicológica	Violência Patrimonial	Violência Moral
Artigos	Tipo Penal	Descrição	qualque conduta que cause dano emocional e diminuição da auto-estima ou que prejudique e perturbe o pleno desenvolvimento ou que vise degradar ou controlar 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 cause prejuízo à saúde psicológica e à autodeterminação.	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.	qualquer conduta que configure calúnia, difamação ou injúria.
171	Estelionato	Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento	■	■	
155, par. 4o., inc. II	Furto mediante fraude	Subtrair, para si ou para outrem, coisa alheia móvel, mediante fraude	■	■	
307	Falsa identidade	Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem	■		
299	Falsidade Ideológica	Omitir, em documento público ou particular, declaração que dele devia constar, ou nele inserir ou fazer inserir declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante	■		
298	Falsificação de documento particular	Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro	■		
297	Falsificação de documento público	Falsificar, no todo ou em parte, documento público, ou alterar documento público verdadeiro	■		
304	Uso de documento falso	Fazer uso de qualquer dos papéis falsificados ou alterados, públicos ou particulares	■		
140	Injúria	Injuriar alguém, ofendendo-lhe a dignidade ou o	■		■

		decoro			
139	Difamação	Difamar alguém, imputando-lhe fato ofensivo à sua reputação			
138	Calúnia	Caluniar alguém, imputando-lhe falsamente fato definido como crime			
147	Ameaça	Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave			

Fontes: SISP. C.P.B. Lei n. 11.340/2006.

Observa-se que, nos tipos penais constantes no Código Penal referentes às fraudes, há a manifestação da violência psicológica e patrimonial e, no que tange às ameaças e crimes contra a honra, há intrínseca a violência psicológica e moral, sendo que a soma dos registros onde tais formas de violência se apresentam representaram mais de 81% dos registros computados na DRCT, no período analisado, percentual bastante expressivo.

Assim, verifica-se ser fundamental a atenção da sociedade e do Estado no que se refere à prevenção e enfrentamento aos cibercrimes, seja por meio do conhecimento dos riscos oferecidos pelo ciberespaço, seja a partir de políticas criminais adequadas à nova ordem social vivenciada.

CAPÍTULO II - ARTIGO CIENTÍFICO

A VIOLÊNCIA NA PRÁTICA DE CRIMES NO CIBERESPAÇO[1]

SILVEIRA, Beatriz de Oliveira da[2]
Mestranda em Segurança Pública, UFPA
RAMOS, Edson Marcos Leal Soares[3]
Professor Doutor, UFPA
ALMEIDA, Sílvia dos Santos[4]
Professora Doutora, UFPA

RESUMO

Este trabalho visa apresentar a exteriorização da violência na prática de crimes na sociedade digital, onde há a redefinição ou extinção de fronteiras, supervalorização da informação, que agora possui alcance global e de forma instantânea. A metodologia adotada foi pesquisa bibliográfica e documental, bem como análise de dados estatísticos referentes a registros de boletins de ocorrência policial sob a responsabilidade da Delegacia de Repressão a Crimes Tecnológicos da Polícia Civil do Estado do Pará, no ano de 2013. Nesse contexto, observa-se que a criminalidade também se adaptou a essa ordem social crescente, onde os cibercrimes consolidam a violência psicológica, moral e patrimonial, cujas práticas possibilitam maiores lucros com menores riscos. Dessa forma, urge que os órgão de justiça criminal busquem conhecer esses novos enfoques de atuação delitiva e se qualifiquem para o respectivo enfrentamento, de forma cooperativa nacional e internacionalmente.

Palavras-chave: Digital. Sociedade. Cibercrimes. Informação.

---

1 Trabalho que integra a dissertação ora apresentada, submetido para avaliação da Revista Direito GV.
2 Mestranda em Segurança Pública, Universidade Federal do Pará.
3 Professor da Universidade Federal do Pará.
4 Professora da Universidade Federal do Pará.

ABSTRACT

This paper presents the manifestation of violence in crime in cyberspace, where there is resetting or extinction of borders, overvaluation of the information we now have global reach and instantly. The methodology adopted was bibliographical and documentary research and analysis of statistical data on the records of police reports under the responsibility of the Bureau of the Technological Crimes Suppression of the Civil Police of the state of Pará, in the year 2013. In this context, it is observed that the crime has also adapted to this growing social order, consolidating the psychological, moral and property, whose practices allow higher profits with less risk. Thus, it is urgent that the criminal justice agency to seek new approaches to meet these criminal performance and qualify for their confrontation, nationally and internationally cooperatively.

Keywords: Digital. Society. Cybercrime. Information. Technology.

1. 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 à realização de atos e negócios jurídicos.

Para Angeluci e Santos (2007), a comunicação e a informação em tempo real, onde as relações empresariais e pessoais são facilitadas pelo livre e irrestrito acesso a 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.

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 ai 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).

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 Tróia no computador da vítima (NORTON SYMANTEC, 2014).

Um fator de grande relevância, que favorece à 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, tem 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 Sistem – 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 grande 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 (2002), 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 ainda 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 atividade 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, tendo pesquisas realizadas no exterior apontado as mesmas conclusões, sempre ligadas à baixa qualificação do pessoal, carência de estrutura técnica e pouca atenção do estado.

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 à adaptar-se à nova realidade.

Rosenbaum et al. (2011) analisaram uma amostra de polícias municipais, a fim de avaliar a utilização de sites pelas agências estatais como forma de repassar e obter informações. A pesquisa demonstrou que a utilização da internet como ferramenta de interação entre as polícias municipais norte-americanas e a população está atrofiada, resumindo-se muito mais em "empurrar" informações, do que democratizar a atuação policial. Há a necessidade de as agências explorarem plenamente o potencial desta ferramenta para a aproximação da polícia e a comunidade, visando a obtenção de uma resposta sobre o desempenho da polícia, favorecendo a resolução de conflitos na circunscrição, além de reforçar a confiança do público.

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, suposto anonimato.

Quanto aos três primeiros fatores – encurtamento de fronteiras, instantaneidade, 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 policias, 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 referente aos delitos cibernéticos estão as dificuldades de realização da justiça criminal, pois como afirmam Magalhães e Azevedo (2003), uma das grandes dificuldades enfrentadas pelo Judiciário 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 policiais por medidas cautelares, especialmente diante da plurilocalidade característica dos cibercrimes, onde, 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 exteriorização de outras formas de violência, intensificadas pelas características do ciberespaço, como a moral e a psicológica, capazes sim, de trazer sérias consequências às vítimas, já que, por exemplo, quando 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 tem poucas informações acerca dos perigos virtuais e, ao clicar em anexos de emails, 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.

2. 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 ATM 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).

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.

Nesse sentido Sydow (2013) elenca como características do direito informático criminal a interatividade, mobilidade, conversabilidade, conectividade, mundialização, fracionabilidade, divisibilidade, intangibilidade, disponibilidade, pluralidade, simultaneidade, anonimidade e a velocidade, podendo o ambiente virtual ser utilizado para atividades lícitas, mas também potencializando atividades ilícitas.

Interessante classificação de crimes cibernéticos é proposta por Norton Symantec (2014), dividindo-os em tipo I e tipo II, sendo que, no tipo I, há a atuação da vítima, que, por exemplo, baixa sem saber softwares de atividades ilegais, tais como programas de registro de digitação, vírus, rootkits ou Cavalos de Troia, que irão atacar falhas ou vulnerabilidades no software visado, como por exemplo, quando criminosos que controlam um site podem aproveitar a vulnerabilidade de um navegador da Web para introduzir um Cavalo de Tróia no computador da vítima. São exemplos: o phishing, o roubo ou a manipulação de dados ou serviços por meio de pirataria ou vírus, roubo de identidade e fraude no setor bancário ou de comércio eletrônico.

Já o tipo II inclui atividades como assédio e molestamento na Internet, violência contra crianças, extorsão, chantagem, manipulação do mercado de valores, espionagem empresarial complexa e planejamento ou execução de atividades terroristas, tendo como características uma série contínua de eventos envolvendo interações repetidas com a vítima, utilizando-se de programas que não estão incluídos na classificação de atividades ilegais, como por exemplo, as conversas podem acontecer usando clientes de IM (mensagens instantâneas) ou arquivos podem ser transferidos usando FTP (NORTON SYMANTEC, 2014).

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, Ministério Público e 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).

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).

Wendt e Jorge (2012) afirmam que além das vulnerabilidades existentes na rede, há o constante crescimento do número dos usuários, bem como a reiterada falta de atenção por parte destes. Verifica-se, assim, que os crimes cibernéticos têm grandes impactos na sociedade, pois o número de pessoas conectadas à rede só aumenta, o que não vem acompanhado da obtenção de informações e práticas de procedimentos seguros na internet e quanto mais indivíduos expostos, mais chances de virem a ser vítimas de cibercriminosos.

Os delinquentes, por sua vez, também se integraram ao ambiente virtual e passaram a praticar suas condutas delitivas consubstanciadas pelas facilidades da nova era: conseguem atingir mais vítimas, com menos custos, menos exposição ao risco (e penas mais suaves) e, consequentemente, maiores lucros.

Com isso, verifica-se a intensificação de formas de violência ínsitas aos crimes tecnológicos, substituindo a violência física, pela violência moral e psicológica. Entretanto, não há, no Brasil, diploma legal que discipline o que pode ser conceituado como violência no ciberespaço, sendo necessário defini-la, inclusive quanto às suas formas de manifestação.

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).

Excelente definição dos diversos tipos de violência se encontra na Lei Maria da Penha, que disciplina as formas de violência doméstica e familiar contra a mulher:

> 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 auto-estima 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 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, 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 das novas 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 através de 41.354 números IPs 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, 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 tem 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 (Tabela 1).

Tabela 1. Registros Por Tipo de Conteúdo em Páginas Distintas, no Brasil, de 2006 a 2014.

DESCRIÇÃO	N. PÁGINAS	PERCENTUAL %
Pornografia Infantil	4909	33,09
Racismo	4012	27,05
Apol. e Incit. a Crimes Contra a Vida	2416	16,29
Homofobia	870	5,86
Intolerância Religiosa	780	5,26
Xenofobia	583	3,93
Maus Tratos Contra Animais	493	3,32
Tráfico de Pessoas	346	2,33
Neonazismo	258	1,74
Não Classificado	167	1,13
TOTAL	14834	100,00

Fonte: Safernet Brasil, 2015.

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).

Verifica-se, assim, que os crimes cometidos por meios eletrônicos só tendem a crescer, especialmente porque também só aumenta a quantidade de pessoas conectadas à internet e que incorporaram a tecnologia em seu modo de vida.

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 potencializam as 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 órgão 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, em razão da expressão da violência moral e psicológica, vislumbradas, a título de exemplificação, nos crimes contra a honra (calúnia, injúria e difamação), nas ameaças, nas fraudes e na pornografia infanto-juvenil, que vem se alastrando nas redes sociais.

Os crimes contra a honra são a calúnia, a difamação e a injúria, previstas nos Artigos 138, 139 e 140 do Código Penal Brasileiro (BRASIL, 1940).

A calúnia (Art. 138, do C.P.B) 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. A difamação (Art. 139, do C.P.B), 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. Já na injúria (Art. 140, do C.P.B), 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, 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 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 C.P.B) 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 C.P.B.) e no furto mediante fraude (Art. 155, parágrafo 4º, inciso II, do C.P.B.), 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.

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.

Destaque-se que a desorganização do Estado é atrativa aos criminosos eletrônicos, uma vez que o Brasil é carente de legislação específica, sobretudo quanto ao processamento dos crimes tecnológicos, desde a regulamentação da fase pré-processual ao julgamento, especialmente quanto aos critérios de atribuição e competência, bem como de coleta adequada e preservação de provas, que normalmente são voláteis.

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.

Além da carência legislativa brasileira específica, 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, institutos periciais, Ministério Público e 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 e a psicológica, pois poucos delinquentes tecnológicos ficam presos, já que a maioria dos julgadores acredita que aqueles não são perigosos, entendendo a periculosidade apenas como a de cometer a violência física ou a grave ameaça ao físico da vítima.

3. Análise dos Registros de Boletins de Ocorrência Policial cuja unidade responsável é a Delegacia de Repressão a Crimes Tecnológicos, no ano de 2013.

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. Isso significa que a citada unidade registrou ou recebeu os referidos BOPs, estes registrados em outras unidades da Polícia Civil do Estado do Pará, 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 BOPs da DRCT por crimes, no ano de 2013, por meio da técnica estatística descritiva, verifica-se que as fraudes constituem a grande maioria dos registros recebidos pela unidade policial especializada, com mais de 71% das ocorrências, manifestando-se como 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, sendo eles a injúria, difamação e calúnia representaram 8% dos registros, e, as ameaças, 2%. Verifica-se que os crimes em que são vislumbradas a violência psicológica e patrimonial como as fraudes, somados aos delitos que possuem intrínseca a violência moral, como as ameaças e crimes contra a honra representaram mais de 81% dos registros computados na DRCT, percentual bastante expressivo.

4. CONCLUSÃO

Atividades hoje corriqueiras na vida dos cidadãos podem trazer riscos ainda pouco conhecidos pelos usuários dos meios tecnológicos. Uma simples compra pela internet pode tornar alguém vítima de estelionato se, por exemplo, a mercadoria for inexistente e nunca for entregue. O furto mediante fraude pode acontecer quando há a subtração de dinheiro alheio por meio de invasão da conta corrente pela internet. Já os crimes contra a honra e as ameças, costumeiramente ocorrem quando se ofende alguém, por exemplo, em sites, emails ou redes sociais.

Observa-se que, com a incorporação dos meios tecnológicos ao cotidiano dos indivíduos, surgem também novos meios de praticar delitos já existentes, mas que são potencializados, por exemplo, pela internet, os quais dão relevância à uma nova forma de criminalidade bastante perigosa, pois pode atingir milhões de pessoas, instantaneamente e em nível mundial.

Nesse contexto, consolidam-se, ainda, a violência moral e a psicológica, em contrapartida à violência física – que só é possível de ocorrer no ambiente real – mas tão perniciosa como esta, pois são capazes de abalar profundamente a dignidade da pessoa humana.

Assim, urge o estudo aprofundado das novas formas de violência que afetam os cidadãos no mundo globalizado, bem como o aperfeiçoamento legislativo e a qualificação dos integrantes do sistema de justiça criminal (Polícias, Ministério Público, Judiciário, etc.) para a realização do adequado enfrentamento à criminalidade tecnológica, que se expande no Pará, no Brasil e no Mundo.

REFERÊNCIAS BIBLIOGRÁFICAS

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.

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. Decreto-lei Nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Rio de Janeiro, RJ, 1940.

BRASIL. 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, DF, 1990.

BRASIL – STF (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.

BRASIL. Lei Nº 10741, de 01 de outubro de 2003. Dispõe sobre o Estatuto do Idoso e dá outras providências. **Lei Nº 10.741, de 1º de Outubro de 2003**. Brasília, DF, 03 out. 2003.

BRASIL. Lei Nº 11.340, de 07 de agosto de 2006. **Lei Nº 11.340, de 7 de Agosto de 2006.** Brasília, DF.

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.

DAOUN, A. J. Os novos crimes de informática. **Jus Navigandi**, Teresina, ano 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. 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?** 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, ano 5, n. 44, 1 ago. 2000. Disponível em: http://jus.com.br/artigos/1830. Acesso em: 14 set. 2013.

ROSENBAUM, D. P.; GRAZIANO, L. M.; STEPHENS, C. D.; SCHUCK, A. M. **Understanding Community Policing and Legitimacy-Seeking Behavior in Virtual Reality:** A National Study of Municipal Police Websites, 2011. Disponível em: <http://pqx.sagepub.com/content/14/1/25>. Acesso em: 20 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.

SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas.** São Paulo: Saraiva, 2013.

WENDT, E.; JORGE, H. V. N. **Crimes cibernéticos:** ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2012.

YAR, M.. Computer Hacking: Just Another Case of Juvenile Delinquency?. **The Howard Journal,** Canterbury, p. 387-399. 01 set. 2005.

CAPÍTULO III - CONCLUSÕES

A atual Era da Informação é marcada pela automação e otimização de processos, com base em tecnologias de informação e comunicação, possibilitando tornar mais fáceis e lucrativos desde procedimentos simples a atividades complexas, enriquecendo o cotidiano dos indivíduos.

Justamente as vantagens da sociedade digital acabam por expô-la a novos riscos, e, entre eles, os cibercrimes, que aliando engenharia social (manipulação de outrem, para a obtenção de informações sensíveis) à tecnologia, podem atingir milhões de pessoas, instantaneamente e em nível mundial.

Observou-se em 2014 um aumento de 297% no total de incidentes reportados ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT.br, 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).

Assim como em nível nacional, no Pará as fraudes despontaram, no período analisado, em mais de 71% das ocorrências analisadas neste estudo, seguidas pelos crimes contra a honra (8%) e ameaças (2%) em meio virtual.

Verifica-se, nesse panorama, que os crimes cibernéticos vêm se alastrando, consolidando a manifestação da violência psicológica, da violência moral e da violência patrimonial, em contrapartida à violência física – que só é possível de ocorrer no ambiente real. Destaque-se, todavia, que tais formas de violência (psicológica, moral e patrimonial) são tão perniciosas como a violência física, pois são capazes de abalar profundamente a dignidade humana.

Conclui-se, portanto que as formas de violência manifestadas no mundo globalizado são capazes de afetar não só os indivíduos, mas toda a sociedade, urgindo o aprofundamento do estudo do tema por parte das academias, bem como o aperfeiçoamento legislativo e a qualificação dos integrantes do sistema de justiça criminal (Polícias, Ministério Público, Judiciário, etc.) para a realização do adequado enfrentamento à criminalidade tecnológica, que se expande no Pará, no Brasil e no Mundo.

REFERÊNCIAS BIBLIOGRÁFICAS

ALENCAR, M. G. S. P. **A leitura e as tecnologias de informação e comunicação na atual configuração de sociabilidade capitalista:** era da informação ou da indeterminação? Informação & Sociedade: Estudos (I&S)**,** João Pessoa, *v.* 24, *n.* 2, *p.* 13-18, 2014.

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** – 2015. Disponível em: http://www.cert.br/stats/incidentes/. Acesso em: 24 maio 2015.

BRASIL. Lei Nº 11.340, de 07 de agosto de 2006. **Lei Nº 11.340, de 7 de Agosto de 2006.** Brasília, DF.

SYDOW, S. T. **Crimes informáticos e suas vítimas.** São Paulo: Saraiva, 2013.

ZALUAR, A. **Integração perversa:** pobreza e tráfico de drogas. Rio de Janeiro: FGV, 2004.

WENDT, E.; JORGE, H. V. N. **Crimes cibernéticos:** ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2012.