Conjecturas

DOI: 10.53660/CONJ-952-L10

Cibercriminalidade: Um Novo Desafio Para o Sistema Global de Proteção aos Direitos Humanos

Cybercrime: A New Challenge for the Global Human Rights System

Julio Cesar de Souza Ferreira[1]*, Carolina Yukari Veludo Watanabe[1]

RESUMO

Este trabalho apresenta a cibercriminalidade como uma violação aos direitos humanos, discutindo as dificuldades para o engajamento das nações em seu combate efetivo. Como metodologia, foi conceituada a cibercriminalidade e sua relação com os direitos humanos, e realizada uma tipologia de cibercrimes, buscando analisar cada tipo de conduta com normativas internacionais e a legislação internacional brasileira. Como resultado, verificou-se que o sistema global de proteção aos direitos humanos das Nações Unidas é eficaz na proteção normativa contra violações físicas (genocídio, tortura, xenofobia, escravidão etc.). A comunidade internacional, por outro lado, avança em normatização e tratativas para enfrentamento aos delitos transnacionais mais conhecidos. No entanto, quanto aos cibercrimes, há uma "desorganização" das nações frente ao dano já causado às economias e aos indivíduos de todo o globo por essas ações criminosas. Por meio do levantamento bibliográfico e da relação da tipologia dos crimes com as normativas, fica evidenciada a falta de leis mais específicas e a necessidade de melhor convergência de políticas e esforços de toda a comunidade internacional para enfrentamento dessa espécie delitiva.

Palavras-chave: Ciberviolência; Cibercriminalidade; Direitos Humanos; Tipologia de cibercrimes; Legislação de cibercrime.

ABSTRACT

This work presents cybercrime as a violation of human rights, discussing the difficulties for the engagement of nations in its effective fight. As a methodology, cybercrime and its relationship with human rights were conceptualized. A typology of cybercrimes was conducted to analyze each type of conduct with international regulations and Brazilian international legislation. As a result, the United Nations' global system of human rights protection was effective in normative protection against physical violations (genocide, torture, xenophobia, slavery, etc.). The international community is making progress in standardizing and dealing with the most well known transnational crimes. On the other hand, the cybercrime field presents a "disorganization" face of the damage already caused to economies and individuals across the globe by these criminal actions. Through the bibliographic survey and the relationship between the typology of crimes and the regulations, the lack of more specific laws and the need for a better convergence of policies and efforts of the entire international community to face this type of crime are evident.

Keywords: Cyber violence; Cybercrime; Human rights; Cybercrime typology; Cybercrime legislation.

[1] Universidade Federal de Rondônia
*E-mail: julio.cesar.opo@gmail.com

INTRODUÇÃO

O ataque à privacidade é uma das formas de violação mais frequentes e danosas da modernidade (FERRAZ JÚNIOR,1993), se considerado que a individualidade e a formação de subjetividade passam necessariamente pela garantia da intimidade. O desenvolvimento psíquico saudável exige interações sociais saudáveis (ARAUJO et al., 2010), e a violação de intimidade e exposição públicas (tão comuns em crimes cibernéticos) afetam sobremaneira o modo de vida de suas vítimas.

Um dos fatores para o aumento da incidência desse delito é o barateamento e a popularização da tecnologia e internet em todo o mundo, também resultante da revolução tecnológica, que, apesar de melhorar a qualidade e o modo de vida das pessoas, facilita ações criminosas dessa espécie, na medida em que se aumenta a quantidade de terminais conectados à rede.

Os delitos cibernéticos são uma nova modalidade de crime que pode abalar a própria essência e concepção de personalidade dos indivíduos que são vítimas, notadamente nos casos de vingança digital (em inglês conhecido também como porn revenge) ou cyberbullying (intimidação moral ou humilhação pública praticada via internet), por exemplo.

A internet possibilita que a nova criminalidade (cibernética) não possua quaisquer limites territoriais, tal como os demais crimes transnacionais, com a agravante da desnecessidade de deslocamento do criminoso para prática de quaisquer condutas. Em linhas gerais, uma pessoa pode praticar inúmeras condutas lesivas sem sair de sua residência, prejudicando, contudo, pessoas residentes do outro lado do planeta. É a ciberviolência.

O impacto da tecnologia na vida das pessoas se dá especialmente em suas relações sociais, no modo como se comunicam umas com as outras. O volume de transações realizados por intermédio da rede é o maior já visto (MOURA et. al, 2018) e isso facilita sobremaneira a ação de grupos criminosos nos mais variados tipos de crime cibernético.

As redes sociais, por seu turno, se tornam novos espaços de convivência social, e o tráfego de informações pessoais (incluindo imagens) é constante na rede (DA SILVA CORREA et al., 2018), o que se traduz em sérios riscos à intimidade e privacidade de seus usuários, mormente pela captação ilegal desses dados. Aqui se identifica um dos pontos de potencial violação a direitos.

Por um lado, o sistema global de proteção aos direitos humanos, alicerçado na Declaração Universal de Direitos Humanos (DUDH) e nos pactos que lhe conferem força jurídica, tem inaugurado, desde 1948 uma era de monitoramento constante dos estados partes (international accountability) quanto ao cumprimento dos direitos que se pretendeu proteger. Esse sistema tem sido muito eficaz para a proteção de direitos civis, políticos e até mesmo sociais, reforçando a malha protetora já existente pela positivação de direitos nos ordenamentos jurídicos dos estados-partes.

Por outro lado, dentro desse contexto, surge, então, um questionamento: mesmo pretendendo lidar com as mais diversas violações aos direitos fundamentais, a comunidade internacional e nacional está preparada juridicamente para lidar com as novas ameaças, aquelas que são fruto da revolução tecnológica do século XXI?

A fim de responder a esta pergunta, o objetivo deste artigo é verificar se há a necessidade de novos e efetivos mecanismos jurídicos e de cooperação jurídica mútua para fazer frente a esse novo formato de criminalidade. Como objetivos específicos, tem-se: (i) relacionar a ciberviolência como violação aos direitos humanos; (ii) identificar os tipos de cibercrimes existentes; e (iii) identificar os mecanismos específicos para proteção contra violações praticadas no ciberespaço, considerando o sistema global de proteção aos direitos humanos.

Como metodologia de pesquisa, foi adotada a revisão bibliográfica e pesquisa documental acerca da ciberviolência e dos cibercrimes, buscando-se também as referências sobre direitos humanos e o sistema de proteção global, além da coleta de dados em fontes abertas quanto ao uso de tecnologia e danos causados pelos crimes cibernéticos.

Para atingir os objetivos propostos, na primeira seção foi apresentada a estrutura do sistema global de proteção aos direitos humanos, demonstrando a inexistência de mecanismo específico para proteção contra violações praticadas no ciberespaço.

Na segunda seção, por seu turno, é trazido o conceito de crime cibernético com base na bibliografia revisada e os impactos desse tipo de crime na vida das pessoas, notadamente os danos causados em todas as vertentes.

A terceira seção é destinada a uma análise entre o arcabouço normativo sobre a matéria (ciberviolência), no qual se apresenta quais condutas são tratadas pela legislação pátria, tanto na esfera cível quanto na esfera criminal, e ainda quais os tratados internacionais existentes sobre cada tipo de violação cibernética.

Por fim, a última seção é voltada a uma análise sobre o tema proposto, demonstrando que os crimes cibernéticos, pelos prejuízos causados à população de todo o globo, merecem atenção especial dos estados e organismos internacionais, o que hoje não ocorre a contento.

DIREITOS HUMANOS, CONCEITO E ESTRUTURA NORMATIVA DO SISTEMA GLOBAL DE PROTEÇÃO

A compreensão de direitos humanos perpassa essencialmente pela historicidade desses direitos e pela ordem em que foram positivados tanto na esfera global como nos estados liberais. Em verdade, há uma dificuldade em se definir um conceito de direitos humanos por razões filosóficas e políticas. Logo, o que importa é definir quais são os direitos humanos, com base em seus fundamentos lógicos.

Nessa esteira, Robert Alexy em seu trabalho *Derecho, moral y la existencia de los derechos humano*s, critica o fato de se imaginar como fundamento de direitos humanos apenas a igualdade e a liberdade:

> As ideias de liberdade e igualdade são a base dos direitos humanos. Reconhecer outro indivíduo como livre e igual é reconhecê-lo como autônomo; isso implica reconhecê-lo como pessoa; por sua vez, isso significa atribuir sua dignidade. Atribuir dignidade a alguém é reconhecer seus direitos humanos. Com isso, pode-se pensar que uma fundação de direitos humanos foi alcançada. [TRADUÇÃO NOSSA](ALEXY, 2013, p.166)

De acordo com esse catedrático, as ideias de igualdade e liberdade não seriam as únicas bases dos direitos humanos, mas apenas as primeiras premissas que levam ao necessário reconhecimento da autonomia do indivíduo e de sua dignidade enquanto ser humano. É evidente que a teoria de Alexy (que é muito mais extensa) funda-se no discurso e sua lógica jurídica, não abordando necessariamente quais seriam as bases todas dos direitos humanos. Contudo, a primeira conceituação (dignidade) que propõe já seria parâmetro mínimo para definição desses direitos.

A busca pela realização da dignidade seria um parâmetro para se categorizar as pretensões que antecedem o próprio direito positivado, e assim denominar essa categoria especial de “direitos humanos”.

Na órbita internacional, os direitos humanos são construídos e garantidos em pelo menos duas vertentes (RAMOS, 2011, p.12), a saber: na esfera legislativa, por meio das

normas internacionais, e na vertente dita judicial ou quase judicial, em que tais normas são aplicadas por cortes internacionais em casos de violação de direitos humanos.

Tratados internacionais tradicionais visam estabelecer equilíbrio de interesses entre os Estados signatários. Os tratados e convenções internacionais que versam sobre direitos humanos, de outro bordo, objetivam garantir o exercício de direitos e liberdades fundamentais aos indivíduos.

Os principais tratados e convenções de direitos humanos estão listados no quadro 1, em ordem cronológica dos principais tratados e convenções internacionais ratificados pelo estado brasileiro (PIOVESAN, 2013).

Quadro 1 – Tratados internacionais de direitos humanos ratificados pelo Brasil

Instrumento Internacional	**Data de adoção na comunidade internacional**	**Data da ratificação pela república federativa do Brasil**
Carta das Nações Unidas	26/05/1945	21/09/1945
Declaração Universal dos Direitos Humanos	10/12/48	10/12/1948
Convenção sobre a Eliminação de Todas as Formas de Discriminação Racial	21/12/1965	27/03/1968
Pacto Internacional dos direitos Civis e Políticos	16/12/1966	24/01/1992
Pacto Internacional dos Direitos Econômicos, Sociais e Culturais	16/12/1966	24/01/1992
Convenção sobre a Eliminação de Todas as formas de Discriminação contra a Mulher	18/12/1979	01/02/1984
Convenção contra a Tortura e outros Tratamentos ou Penas Cruéis, Desumanos ou Degradantes	10/12/1984	28/09/1989
Convenção sobre os Direitos da Criança	20/11/1989	24/09/1990

Fonte: Elaborado pelos autores a partir de Piovesan (2013).

Ocorre que os direitos humanos decorrem da necessidade da sociedade em se proteger fortemente bens jurídicos que lhe sejam mais caros, e por isso mesmo tais direitos tem estrutura variada, podendo ser “direito-pretensão, direito-liberdade, direito-poder e, finalmente, direito-imunidade, que acarretam obrigações do Estado ou de particulares revestidas, respectivamente, na forma de: (i) dever, (ii) ausência de direito, (iii) sujeição e (iv) incompetência” (RAMOS, 2017, p. 21).

De acordo com a espécie de obrigação gerada, é possível elencar na ótica interna e internacional os direitos humanos mais basilares, e, assim, aproximar-se de uma definição. Poderiam ser citados, como exemplos de direitos já reconhecidos, os seguintes: vida, liberdade, não ser escravizado, não ser torturado, privacidade (direitos-liberdade), segurança pessoal, propriedade, educação básica, lazer, (direitos-pretensão)

personalidade, honra, nacionalidade, direitos políticos (direitos-poder/imunidade). Todos citados são reconhecidos na DUDH.

O rol de direitos humanos não é exaustivo ou *numerus clausus*, mas sim aberto às novas necessidades da espécie humana para promoção da dignidade de cada indivíduo. Assim, o direito à intimidade, por exemplo, traria a obrigação ao Estado e aos particulares na forma de "ausência de direito", pois não seria lícita a invasão da vida privada de um indivíduo nem por autoridade pública e nem por outros indivíduos, exceto nos casos específicos determinados (reserva de jurisdição), ao passo que o direito à propriedade seria uma espécie de sujeição de particulares e do Estado ao indivíduo proprietário.

Esses direitos, contudo, estão protegidos pelas normas internacionais de direitos humanos que foram relacionadas no quadro 1, contudo, sem relação com a sua violação em um ambiente virtual. Não foi encontrada norma específica para o tratamento das violações de direitos humanos mencionados por meio da rede de conexão global (internet).

É necessário demonstrar o funcionamento do sistema global de proteção aos direitos humanos para, em um segundo momento, as normas internacionais que protegem esses direitos, esclarecer sobre a inexistência de norma específica no âmbito da comunidade internacional.

A seguir é apresentado o sistema global de proteção aos direitos humanos, também conhecido como Sistema ONU (Organização das Nações Unidas), assim como seus principais instrumentos para garantia do cumprimento das normas internacionais de direitos humanos. Essa abordagem visa verificar se há, dentre as normativas, mecanismos voltados à proteção de pessoas contra violações perpetradas no ciberespaço.

Sistema global de proteção aos direitos humanos e os seus instrumentos internacionais

O processo de universalização dos direitos humanos obrigou os Estados a aceitarem que a comunidade internacional tutelasse matérias que, até então, lhes eram exclusivas (PIOVESAN, 2013, p.239), mitigando sua soberania. Esse controle busca, em última análise, a garantia de efetivação e respeito aos direitos humanos elencados nas declarações e tratados.

Nesse contexto, optou-se por uma metodologia internacional para monitoramento e controle da efetivação dos direitos humanos, a chamada *international accountability*. A

criação de um sistema global de proteção aos direitos humanos, bem como os sistemas regionais, são consequências desse esforço da comunidade internacional.

Vale mencionar que a Declaração Universal dos Direitos Humanos de 1948 lista uma série de direitos e políticas que devem ser adotadas pelos Estados, mas não possui qualquer força cogente enquanto norma jurídica (SHAW, 2008, p.46). Daí a necessidade de juridicizar o conteúdo da declaração, cenário em que são assinados os pactos internacionais de direitos civis e políticos e direitos econômicos, sociais e culturais, ambos no ano de 1966. Esses novos tratados têm força normativa e vinculam aos seus signatários, o desdobramento com força jurídica convencional daquilo que se declarava dezoito anos antes (REZEK, 2011, p.256).

O sistema da ONU (sistema global) é composto por mecanismos (convencionais ou extra-convencionais) e organismos. Os mecanismos se baseiam nas convenções de direitos humanos, as quais obrigam os Estados contratantes ao cumprimento estrito de seu texto. Cada convenção traz a criação de comitês específicos para monitoramento de seu cumprimento. Os mecanismos extra-convencionais, por outro lado, são fundados na própria carta da ONU e, portanto, obrigam a todos os membros daquela Organização, sendo os relatórios e os grupos de trabalho seus principais instrumentos.

Os organismos, por seu turno, são vários. Dentre eles, merecem destaque: o Conselho de Direitos Humanos da ONU, a Assembleia Geral e o Conselho de Segurança. Há ainda a Corte Internacional de Justiça, órgão jurisdicional, mas não voltado especificamente à proteção dos Direitos Humanos, cuja legitimidade ativa atende apenas aos Estados membros da ONU.

Conforme Piovesan (2013, p.263), como mecanismo de proteção dos direitos enunciados nos pactos e nas convenções internacionais de direitos humanos, via de regra adota-se a sistemática de relatórios a serem elaborados pelos Estados-partes. Eventualmente também se estabelecem o sistema de comunicações interestatais e o sistema de petição ou comunicação individual, em cláusulas ou protocolos facultativos.

Cada uma delas também prevê a instituição de determinado órgão, denominado "Comitê", responsável pelo monitoramento dos direitos constantes na convenção, ao qual compete a apreciação dos relatórios encaminhados pelos Estados-partes e, eventualmente, receber e considerar as comunicações interestatais e as petições individuais.

Como pode ser observado, os mecanismos convencionais estão atrelados à respectiva convenção, ou seja, o tratado de proteção a um direito define também o

mecanismo de monitoramento. Assim, há comitês para a proteção de direitos humanos como eliminação de discriminação, tortura, racismo, entre outros.

De outro bordo, os organismos existentes atualmente não estão engajados na luta pela proteção da intimidade e às novas formas de violação a esse direito, como o cibercrime. Não há um mecanismo convencional buscando o combate a esse crime, já que a única convenção sobre o tema, como se verá adiante, não foi assinada por iniciativa da ONU e sim do Conselho da Europa e não compõe, nesses termos, o sistema global.

CIBERCRIMINALIDADE: UMA VIOLAÇÃO AOS DIREITOS HUMANOS

Conceituar o cibercrime ou crime informático não é tarefa das mais simples, já que é espécie do gênero crimes tecnológicos. A literatura tem classificado o crime cibernético como aquele em que se utiliza a rede mundial de computadores como instrumento ou meio para sua prática (BARRETO, 2016.p. 16). Esses crimes, embora praticados no meio virtual, trazem consequências no mundo real.

As recomendações da *Organization for Economic Cooperation and Development* (OECD), de 1986, de acordo com Damásio de Jesus, conceituam crime eletrônico da seguinte maneira:

> "qualquer comportamento ilegal, aético ou não autorizado envolvendo processamento automático de dados e, transmissão de dados, podendo implicar a manipulação de dados ou informações, a falsificação de programas, o acesso e/ou o uso não autorizado de computadores e redes" (JESUS, 2016, p.49)

No entanto, o crime eletrônico em regra é um crime meio, ou seja, utiliza o meio virtual para a prática de condutas já tipificadas como o estelionato, a extorsão, a falsidade ideológica, as fraudes, entre outros. Assim, a conduta pode ser virtual, mas o crime não.

A maior parte dos crimes cometidos na internet ocorrem também no mundo real. A internet facilita apenas a prática desses delitos especialmente pelo anonimato que proporciona aos criminosos. Nesse contexto, os conceitos são os mesmos do direito penal e processual penal comum. Algumas condutas, contudo, ainda merecem tipificação própria.

Desse modo, o crime cibernético pode ser próprio (puro) ou impróprio (impuro) (BARRETO, 2016, p. 17). Crimes cibernéticos próprios são aqueles em que o sistema operacional, banco de dados ou arquivos são os alvos do criminoso (dano, invasão de sistemas, inserção de dados, etc.), ao passo que crimes cibernéticos impróprios são aqueles em que o meio tecnológico é apenas instrumento para a prática de crimes já

tipificados e cometidos no mundo real (crimes contra honra, ameaça, furto, lavagem, etc.). O quadro 2 apresenta a descrição desses dois tipos de crimes cibernéticos.

Quadro 2 – Crimes Cibernéticos

CRIMES CIBERNÉTICOS	OS ATAQUES TEM COMO ALVO	EXEMPLOS
Próprios / Puros	As estruturas dos sistemas informatizados.	Invasão de dispositivos, danos aos sistemas informatizados, inserção de dados falsos em sistemas informatizados, etc.
Impróprios / Impuros	Bens jurídicos comuns, mas por meio cibernético	Extorsão, crimes contra honra praticados em redes sociais, furtos de valores em contas bancárias, lavagem de capitais, etc.

Fonte: Elaborado pelos autores a partir de Barreto (2016).

Segundo proposto por Robson Ferreira (PECK, 2013) em sua tese sobre crimes eletrônicos, uma classificação dos crimes por computador, tomando por base o uso do computador no ilícito, é:

> 1) quando o computador é o alvo — p. ex.: crime de invasão, contaminação por vírus, sabotagem do sistema, destruição ou modificação do conteúdo do banco de dados, furto de informação, furto de propriedade intelectual, vandalismo cibernético, acesso abusivo por funcionário, acesso abusivo por terceirizados, acesso abusivo de fora da empresa; 2) quando o computador é o instrumento para o crime — p. ex.: crime de fraude em conta corrente e/ou cartões de crédito, transferência de valores ou alterações de saldos e fraudes de telecomunicações, divulgação ou exploração de pornografia; 3) quando o computador é incidental para outro crime — ex.: crimes contra a honra, jogo ilegal, lavagem de dinheiro, fraudes contábeis, registro de atividades do crime organizado; 4) quando o crime está associado com o comutador — p. ex.: pirataria de software, falsificações de programas, divulgação, utilização ou reprodução ilícita de dados e programas, comércio ilegal de equipamentos e programas. (FERREIRA, in PECK,2013,p.164)

A convenção de Budapeste[2] define cibercrime como "atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta de desses sistemas, redes e dados".

Antes dessa convenção, contudo, já havia tentativas de conceituação dos crimes virtuais. Conforme explica Natário (2013), em 1989, 1998 e 2000 já se tentara definir os cibercrimes. Inicialmente se conceituava como sendo o crime em que se envolvia a tecnologia de computadores (1989), passando a ser conceituado como aquele que utiliza

[2] Disponível em:http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislação /legislacoes-pertinentes-do-brasil/docs_legislacao/ convencao_cibercrime.pdf. Acesso em 20 março de 2019.

a internet (1998) e por fim, no 10º Congresso da ONU, em 2000, definiu-se que crime cibernético seria no sentido estrito, qualquer comportamento ilegal, conduzido através de meios eletrônicos, cujo alvo fosse a segurança de sistemas de computadores e os dados neles alojados e, no sentido lato, qualquer comportamento ilegal cometido por meio de, ou relacionado com, sistemas ou redes de computadores, incluindo crimes como a posse ilegal e distribuição de informação através de sistemas ou redes de computadores.

Portanto, poderiam ser definidos como crimes cibernéticos (ou cibercrimes) como uma espécie do gênero de violações cibernéticas, cuja utilização de dispositivos informáticos e da rede mundial de computadores é preponderante para consecução dos objetivos criminosos, seja para prática de condutas que já estejam tipificadas e sejam perpetradas também no mundo real, seja para vulnerabilizar sistemas de informação e danificar estruturas tecnológicas.

Impacto dos cibercrimes no mundo como violação aos direitos humanos

De acordo com o Relatório NORTON Symantec (Antivirus)[3] divulgado em 2015, quase dois terços da população adulta mundial já fora vítima de algum crime cibernético. O mesmo relatório indica que pelo menos 79% dessas pessoas não esperam que haja alguma punição aos criminosos. As principais espécies de cibercrimes praticadas em larga escala são a pedofilia, as fraudes de cartões de crédito ou bancárias e o estelionato, a subtração de valores e informações ou sua destruição (NORTON, 2015).

A título de comparação, a Norton informa que entrevistou cerca de 17 mil pessoas em 17 países. 85% dos entrevistados no Reino Unido, por exemplo, receiam ser vítimas de crimes online (NORTON,2015) 70% dos entrevistados no Canadá, por outro lado, preferem cancelar um jantar com o melhor amigo a cancelar seu cartão de crédito ou débito. No Brasil, considera-se que as crianças e os adolescentes são o grupo mais vulnerável online. O relatório de perdas financeiras decorrentes do crime cibernético é ainda mais assustador. Informa o relatório (2015) que o mundo teve perdas no montante de 150 bilhões de dólares naquele ano. No Brasil esse prejuízo foi de aproximadamente 45 bilhões de reais no mesmo período (NORTON, 2015).

Os crimes cibernéticos são, portanto, uma das formas de violação de direitos humanos mais básicos, como a propriedade e a intimidade. O pacto internacional dos

[3] Disponível em: http://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime _report/ Norton_Portuguese-Human%20Impact-A4_Aug18.pdf .Acesso em 20 ago. 2018.

direitos civis e políticos prevê em seu artigo 17 que “ninguém será objeto de intervenções ilegais ou arbitrárias em sua vida privada”, com a clara intenção de proteger a privacidade do indivíduo.

Nesse sentido, Mendes e Branco (2012, p.320), ao tratarem do direito à privacidade como um direito humano, trazem a lume a teoria de William Prosser, ao afirmar que existem quatro meios básicos de afrontar a privacidade, a saber: 1) intromissão da reclusão do indivíduo; 2) exposição pública de fatos privados; 3) exposição do indivíduo a uma falsa percepção do público (*false light*) e 4) apropriação do nome e da imagem da pessoa, sobretudo para fins comerciais. Fica claro, nesse átimo, que a cibercriminalidade tem o potencial em suas variadas vertentes de violar substancialmente o direito à privacidade.

Por outro viés, outro direito fundamental violado é o direito à propriedade pois o objetivo da maioria dos delinquentes virtuais é a obtenção de lucro às custas de subtrações e fraudes bancárias, bem como, lavagem dos valores obtidos de forma criminosa, especialmente com a conversão de valores em criptomoedas (moedas digitais) como o bitcoin. Calderon (2017, p.77-78) esclarece que se trata de uma espécie de “cambio do novo milênio” em que se troca a moeda real por uma moeda existente apenas no mundo virtual, tudo com vistas a lograr as autoridades estatais.

Por fim, para concluir as espécies de violação, podem ser citadas as ações criminosas em detrimento de crianças e adolescentes, a pedofilia e a exploração sexual de incapazes, com preponderante utilização do ciberespaço. A convenção sobre direitos da criança firmada em 1989 e seu protocolo facultativo referente à prostituição e pornografia infantil, de 2000 (ratificado pelo Brasil em 2004) tratam da matéria.

O Protocolo traz em seu preâmbulo que os Estados Partes “Preocupados com a crescente disponibilidade de pornografia infantil na Internet e em outras tecnologias modernas, e relembrando a Conferência Internacional sobre o Combate à Pornografia Infantil na Internet (Viena, 1999) e, em particular, sua conclusão, que demanda a criminalização em todo o mundo da produção, distribuição, exportação, transmissão, importação, posse intencional e propaganda de pornografia infantil, e enfatizando a importância de cooperação e parceria mais estreita entre governos e a indústria da Internet.” Fica claro, portanto, que é uma preocupação da comunidade internacional e do sistema ONU o combate à pedofilia e à pornografia infantil.

CIBERSEGURANÇA E MECANISMOS JURÍDICOS DE PROTEÇÃO

Ante esse plexo de ameaças que despontam no mundo informatizado, por meio do cibercrime, a segurança da informação (também denominada segurança cibernética ou *cyber security*, em inglês), ou cibersegurança, é o novo desafio da comunidade internacional. A cibersegurança não só é essencial à garantia dos direitos individuais fundamentais de todos que tem acesso à rede, como também é tida como função estratégica de Estado (MANDARINO JUNIOR; CANONGIA, 2010, p.25).

O conceito de cibersegurança engloba a abordagem e as ações associadas aos processos de gerenciamento de riscos de segurança, seguidas por organizações e estados, para proteger a confidencialidade, integridade e disponibilidade de dados e ativos usados no ciberespaço. Ainda inclui diretrizes, políticas e coleções de proteção, tecnologias, ferramentas e treinamento para fornecer a melhor proteção para o estado de ambiente cibernético e seus usuários (SCHATZ, BASHROUSH e WALL, 2017).

A manutenção de infraestruturas sensíveis à defesa nacional, como energia, telecomunicações, finanças e a própria informação estratégica, por exemplo, exigem uma política de cibersegurança consolidada e resistente aos constantes ataques de *hackers* e *crackers*, que agem de forma autônoma ou até mesmo prestando serviços a outros governos ou corporações. *Hackers* são pessoas que dominam as tecnologias de informação e comunicação (TIC) a ponto de encontrar vulnerabilidades nos sistemas operacionais e invadirem sistemas com objetivos diversos. *Crackers* são *hackers* que utilizam seus conhecimentos para prática de ilícitos (NUNES, 2018).

Para o cidadão comum que utiliza a internet para suas atividades do dia-a-dia, a segurança do terminal utilizado pode prevenir muitos golpes e ataques e se torna tão essencial quanto a segurança física proporcionada por muros, portões e fechaduras.

Nesse contexto, surgiu a convenção de Budapeste, marco normativo no âmbito internacional para o combate ao cibercrime, cunhada no âmbito do Conselho Europeu e já assinada por mais de 60 países na atualidade.

A convenção de Budapeste

A única referência atual acerca do tema da cibersegurança é a *Convention on Cybercrime*, conhecida em língua portuguesa como Convenção Internacional sobre Cibercrime, ou “Convenção de Budapeste” (CONVENÇÃO DE BUDAPESTE, 2001). Nesta convenção foi elaborado o primeiro tratado internacional que aborda o tema e busca

integrar os ordenamentos jurídicos dos estados signatários para melhor cooperação no enfrentamento dos crimes cibernéticos.

Na convenção são elencados os seguintes delitos: infração de *copyright* (violações de direito autoral), pornografia infantil, fraudes na Internet, violações de sistemas de segurança e os crimes de ódio. A convenção trata até mesmo de procedimentos e poderes das autoridades como rastreamento, busca e apreensão de computadores, e interceptação telemática.

A Convenção é acompanhada de uma Minuta do Relatório Explicativo, a qual foi adotada pelo Comitê de Ministros do Conselho da Europa em 08 de novembro de 2001 e aberta para assinatura de outros países em Budapeste no dia 23 de novembro do mesmo ano, entrando em vigor três anos após, no dia 01 de julho de 2004.

Atualmente, 61 países já assinaram e ratificaram a convenção e 4 países assinaram, mas não ratificaram, dentre os quais não se inclui o Brasil. No Brasil já se discute a necessidade do combate aos cibercrimes, mas ainda não houve adesão ao referido tratado (BARRETO, 2016).

No entanto, por ser firmada no âmbito do Conselho da Europa e não da ONU, a Convenção de Budapeste não faz parte do sistema global de proteção aos direitos humanos, portanto, não traz quaisquer mecanismos de proteção aos direitos ali protegidos, como a intimidade e a propriedade. Por outro lado, não há qualquer organismo da ONU atuando para monitorar essa nova ameaça, de modo que a ordem internacional se encontra inerte frente a esse tipo de crime.

Conforme se verificou, o sistema global de proteção aos Direitos Humanos ainda não conta com mecanismos ou órgãos voltados ao combate do cibercrime. A convenção de Budapeste, embora tenha tratado de inúmeros temas relativos ao auxílio mútuo entre os estados signatários, não trouxe em seu bojo mecanismos similares para monitoramento do seu cumprimento. É questionável, nesse ponto, se pode ser classificada como uma convenção de direitos humanos ou se apenas como um tratado de cooperação jurídica.

Taxonomia de cibercrimes

O primeiro passo para gerar políticas que visem combater o cibercrime e realizar a identificação dos tipos de cibercrime. Dentre o grande volume de crimes cibernéticos e a variedade de ataques cibernéticos da atualidade, é possível verificar uma mudança

comportamental dos atacantes dia-a-dia, com diferentes formatos de ataques e novas metodologias para busca de informações confidenciais.

A ação dos criminosos virtuais busca afetar os três princípios fundamentais da rede, quais sejam, a confidencialidade, a integridade e a disponibilidade (CID). Tais conceitos formam a chamada tríade CID, que incorpora os objetivos de segurança fundamentais para dados e informações, bem como para serviços de computação (STALLINGS; BROWN, 2014). A ação de *hackers* e *crackers* têm sofrido variações no decorrer dos anos, o que dificulta sobremaneira a defesa da segurança da rede pelos profissionais que atuam nessa atividade.

O mundo hacker tem oferecido ferramentas gratuitas para ataques em serviços como compras online e aplicativos de redes sociais, o que traz para a atividade criminosa não só os especialistas em sistemas de informação, como também amadores (geralmente jovens) interessados em atacar as estruturas de segurança.

Nesse sentido, Brar e Kumar (2018, p. 5) propõem uma categorização de cibercrimes, o que denominam de *taxonomy of the cybercrime.* De acordo com esses autores, a violência criada no mundo real com a ajuda de um sistema de computador ou qualquer dispositivo (como celular) conectado à Internet é conhecida como ciberviolência.

Como formas de manifestação da ciberviolencia elencam: a guerra cibernética (*cyberwar*), o terrorismo cibernético (*cyberterrorism*), a perseguição virtual (*cyberstalking*) e a vingança digital (*cyberrevenge*) (BRAR; KUMAR, 2018 p.5). Também categorizam como o *Cyberpeddler* o que denominam atos de roubar dados confidenciais de alguém, cujas subcategorias se dividem em fraudes financeiras ou bancárias (*cyberfraud*) e o chamado cyberactivism, que seria basicamente a atividade de pichação moral em redes sociais, que no Brasil convencionou-se denominar popularmente como “fake news”.

Como categoria apartada de cibercrime, Brar e Kumar (2018, p.6) ainda propõem o *cybertrespass*, que é a violação não autorizada de um sistema confidencial, cujas espécies seriam o ciberroubo (*cybertheft*), a espionagem cibernética e a divulgação não autorizada de conteúdo sexual (*cyberpornography*). Por fim, os autores elencam como última categoria o denominado *cybersquatting*, que é basicamente o registro fraudulento de domínio de internet (ou roubo de perfis ou domínios) com objetivos financeiros ou depreciativos.

Combate ao cibercrime: tipologias e normativas jurídicas

No âmbito do sistema global, como bem exposto, a única convenção que trata do tema é a Convenção de Budapeste, não sendo encontrada qualquer outra que verse sobre crimes cibernéticos tanto no sistema global como nos sistemas regionais de proteção aos direitos humanos.

No Brasil a primeira tentativa de tipificação de crimes digitais foi o projeto de lei 84/99, que posteriormente foi aprovado (desfigurado) como lei 12.735/12. Essa lei ficou conhecida como "Lei Azeredo", em alusão ao deputado relator do projeto na Câmara Federal.

Ocorre que o texto aprovado no senado[4] foi desfigurado, e o texto aprovado na Câmara dos Deputados como redação final do projeto[5], já bem modesto em relação ao original, sofreu ainda vetos da presidência da república. Ao final, a lei apenas permitiu a retirada de conteúdo de cunho racista da internet.

Outra lei aprovada e publicada no mesmo dia foi a lei federal nº. 12.737/12, também apelidada de "lei Carolina Dieckman" (BRASIL, 2012), a qual faz referência a uma atriz brasileira que fora vítima de crime cibernético. Contudo, a lei supra apenas passou a tipificar a invasão de dispositivo informático e não as demais espécies de crimes cibernéticos.

Visando verificar se há normativas jurídicas de combate ao cibercrime no Brasil e no mundo, foi elaborado o quadro 3. Neste quadro são apresentados os crimes cibernéticos próprios e impróprios relacionados aos os tratados internacionais e à tipificação na lei penal brasileira, quando existentes. Os tipos de crimes foram definidos a partir das várias ações que se tem notícia recentemente e da já mencionada Convenção de Budapeste.

Quadro 3 – Tipos de crimes cibernéticos

CRIMES CIBERNÉTICOS PRÓPRIOS

[4] Disponível em < http://www.camara.gov.br/sileg/integras/588033.pdf>. Acesso em 22 de setembro de 2018.

[5] Disponívelem<http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1037657&filename=Tramitacao-PL+84/1999> Acesso em 22 de setembro de 2018.

TIPO DE CRIME	TRATADOS INTERNACIONAIS (CRIME CIBERNÉTICO)	TIPIFICAÇÃO NO BRASIL
Invasão de domínios e perfis	Não Há.	Não Há.
Interceptação ilegítima de dados telemáticos (violar privacidade)	Apenas Convenção de Budapeste (Art.3º). Nenhum tratado no sistema global de Direitos Humanos.	**Apenas na seara cível**, com o Marco Civil da Internet. Arts. 10 a 12 da Lei 12.965/14. Não há crime.
Falsidade e burla informática	Apenas Convenção de Budapeste (Art.7º e 8º). Nenhum tratado no sistema global de Direitos Humanos.	Art.154-A CPB, inserido pela lei 12.737/12 (Invadir dispositivo informático alheio).
Invasão de computadores	Apenas Convenção de Budapeste (Art.3ºe 4º). Nenhum tratado no sistema global de Direitos Humanos.	Art.154-A CPB, inserido pela lei 12.737/12 (Invadir dispositivo informático alheio).
Interrupção de serviços de TIC	Apenas Convenção de Budapeste (Art.4º). Nenhum tratado no sistema global de Direitos Humanos.	Art.266, §1º do CPB, alterado pela lei 12.737/12 (Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, incluindo o serviço telemático).
Inserção de dados falsos em sistemas	Apenas Convenção de Budapeste (Art.7º e 8º). Nenhum tratado no sistema global de Direitos Humanos.	Apenas quanto a sistemas da administração pública, com previsão no Art.313-A CPB (inserção de dados falsos nos sistemas Informatizados ou bancos de dados da Administração Pública)
Alteração de sistemas	Apenas Convenção de Budapeste (Art.7º e 8º). Nenhum tratado no sistema global de Direitos Humanos.	Apenas quanto a sistemas da administração pública, com previsão no Art.313-B CPB (Modificar ou alterar sistema de informações)
CRIMES CIBERNÉTICOS IMPRÓPRIOS		
TIPO DE CRIME	**TRATADOS INTERNACIONAIS (CRIME CIBERNÉTICO)**	**TIPIFICAÇÃO NO BRASIL**
Cyberbullying	Não há.	Não há previsão acerca da prática do delito na rede, sendo aplicada a previsão comum do código penal.

		Art. 138 CPB (Calúnia) Art. 139 CPB (Difamação) Art. 140 CPB (Injúria) Art. 147 CPB (Ameaça) Art. 153 CPB (Divulgação de segredo)
Vingança digital	Não há.	Lei 13.718/2018, que alterou o código penal e criou o tipo penal de "**Divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia** Art. 218-C. Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia: Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave.
Pirataria	Apenas Convenção de Budapeste (Art.10). Nenhum tratado no sistema global de Direitos Humanos.	Não há previsão acerca da prática do delito na rede, sendo aplicada a previsão comum do código penal. Art. 184 CPB (Violar direitos de autor e os que lhe são conexos) Lei 9.279/96 (Lei de propriedade industrial)
Induzimento a suicídio	Não há.	Não há previsão acerca da prática do delito na rede, sendo aplicada a previsão comum do código penal. Art. 122 CPB (Induzir ou instigar alguém a suicidar-se ou prestar-lhe auxílio para que o faça)
Extorsão	Não há.	Art. 158 CPB (Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa)
Furto e fraudes financeiras	Não há.	Art. 298, parágrafo único do CPB, alterado pela lei 12.737/12, que considera crime de falsificação de documento particular a falsificação de cartão.

		Art. 155, § 4º, II CPB **(**Subtrair, para si ou para outrem, coisa alheia móvel, II - com abuso de confiança, ou mediante fraude, escalada **ou destreza)** Art. 171 CPB (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**)
Lavagem de capitais	Não há quanto ao delito praticado pela conversão em criptomoedas por exemplo, há uma convenção tratando do tema em outras searas (convenções de Viena e de Palermo)	Art. 1º da Lei 9.613/98.
Pedofilia	Apenas Convenção de Budapeste (Art.9º). Nenhum tratado no sistema global de Direitos Humanos tratando do delito no âmbito da informática, apenas violações físicas (protocolo da convenção sobre direitos da criança)	Arts. 241 ss do ECA (Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente)
Racismo	Não há.	Art. 20 Lei 7.716/89 (Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional)
Perfis falsos em rede social	Não há.	Art. 307 CPB (Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem)

Fonte: Elaborado pelos autores

Como pode ser observado no quadro 3, não há tratado internacional tipificando vários dos crimes cibernéticos dos quais se tem notícia na atualidade. A legislação brasileira, contudo, está avançada no sentido de punir tais crimes, utilizando-se legislação específica ou outros instrumentos normativos.

Os crimes cibernéticos impróprios (aqueles que são cometidos também no mundo real) são mais facilmente coibidos pelas normas internas de cada nação, pois normas

penais já existem para coibir a prática no mundo real e são aplicadas às condutas praticas via rede mundial de computadores.

No entanto, os crimes cibernéticos próprios (aqueles que só existem no mundo virtual) necessitam de legislação específica, e os organismos internacionais de proteção aos direitos humanos, seja pelo sistema global, seja pelos sistemas regionais, deveriam induzir os estados partes a punir rigorosamente essa conduta, o que ainda não existe.

Como visto, a única convenção sobre crimes cibernéticos é a Convenção de Budapeste, e não há nesse tratado ou em qualquer outro previsão para punição, pelos estados signatários, dos seguintes delitos cometidos via internet: Invasão de domínios e perfis, Cyberbullying, Vingança digital, Induzimento a suicídio, Extorsão, Furto e fraudes financeiras, Racismo, Perfis falsos em rede social.

Em partes, a ausência dessa previsão se dá ao fato de que a convenção fora elaborada em 2001, e a expansão das redes sociais se deu a partir do advento do smartphone, logo, muitos desses delitos não apresentavam volume apto a trazer a preocupação da comunidade internacional como atualmente.

Nesse sentido, o estado brasileiro, como se viu pelo quadro, está adiantado em matéria de crimes cibernéticos, com diversas previsões em sua legislação que permitem a punição de quase todos os crimes cibernéticos conhecidos da atualidade.

Importante ressaltar que há os outros projetos em tramitação na Câmara dos Deputados quanto à tipificação de condutas no ciberespaço, a exemplo do Projeto de Lei nº 6.989, de 2017, que altera o Marco Civil para propor a retirada de conteúdo que induza a suicídio da rede mundial.

Por tudo isso, o que fica claro é que apesar de não ter aderido à Convenção de Budapeste, o Brasil possui legislação mínima sendo aplicada a alguns crimes cibernéticos, mas que não há no âmbito do sistema global de proteção aos direitos humanos e nem mesmo em sistemas regionais, qualquer tratado ou convenção sobre o tema que permita uma repressão uniforme e concatenada desses delitos.

CONSIDERAÇÕES FINAIS

Como demonstrado, o sistema global de proteção aos Direitos Humanos (sistema ONU) atualmente não possui mecanismos suficientes ou órgão voltado ao combate aos crimes cometidos por meio da internet. Embora inicialmente se imagine que essa pauta diga respeito à cooperação jurídica internacional pura e simples, há de se ponderar acerca

dos direitos humanos que merecem tutela especial, como a intimidade, a propriedade e a dignidade sexual das crianças enquanto grupo vulnerável.

A falta de tratado ou convenção internacional firmado no sistema ONU torna mais difícil a cooperação entre os estados para o combate mais profícuo aos cibercrimes. Como consequências da ausência de iniciativa do principal organismo internacional, tem-se alarmantes números acerca de prejuízos causados por essa nova modalidade de criminalidade organizada.

As fronteiras estatais são, nesse caso específico, um empecilho à existência de políticas uniformes de combate a esse modal de crime, já que os delinquentes do ciberespaço não conhecem ou respeitam quaisquer fronteiras pela própria lógica de funcionamento da rede mundial de computadores.

A convenção de Budapeste, a despeito de tratar especificamente do cibercrime, foi firmada apenas no sistema regional europeu, e mesmo aberta à assinatura de outros países, não dispõe de mecanismos de monitoramento ou sanções ao descumprimento de suas diretrizes, funcionando apenas como um tratado de cooperação jurídica internacional na matéria.

A comunidade internacional passa por um momento histórico de engessamento frente às novas ameaças tecnológicas, necessitando, portanto, de maior esforço e coesão dos Estados para enfrentamento da delinquência, sob pena de pulverização inócua de recursos humanos e materiais sem sucesso.

Essas novas formas de violação aos direitos fundamentais tendem a ampliar-se com o advento da tecnologia, com potencial para desfigurar a organização político-administrativa que hoje é conhecida, o que deve ser o foco de atenção da comunidade internacional. A privacidade, como visto, e as transações financeiras (propriedade) devem ser objeto de especial proteção normativa e políticas integracionistas por parte dos estados membros da ONU, sob pena de um colapso do sistema financeiro, acarretando sérias perdas para toda a população do globo.

O crime cibernético é uma realidade que bate às portas da comunidade internacional, caso não seja combatido com vigor, poderá trazer sérios danos não só aos Estados enquanto organização política, como a toda a população do globo. Um tratado internacional específico, portanto, com a criação de mecanismos de monitoramento e firmando novas formas de cooperação jurídica, é medida de urgência a ser adotada pela Organização das Nações Unidas.

A transferência de grande parte das atividades comuns e fundamentais para o ciberespaço faz com que a sociedade de hoje dependa fortemente dos sistemas de informação e comunicação. É crucial adaptar as leis que serão capazes de enfrentar os desafios das novas tecnologias de informação e comunicação.

REFERÊNCIAS

ALEXY, Robert**.** Derecho, moral y la existencia de los derechos humanos. **Signos Filosóficos**, v. 15, n. 30, p. 153-171, 2013.

ALEXY, Robert. Trad. Virgílio Afonso da Silva. **Teoria dos Direitos Fundamentais**. 5ªed. São Paulo: Editora Malheiros, 2015.

ARAÚJO AC, LUNARDI VL, SILVEIRA RS, THOFEHRN MB, PORTO AR. Relacionamentos e interações no adolescer saudável. **Revista Gaúcha de Enfermagem**, Porto Alegre, v. 31, n. 1, p. 136-42, 2010.

ARENQUE, Susan C. Violência Cibernética: Reconhecendo e Resistindo ao Abuso em Ambientes Online. **Mulheres Asiáticas**, v. 14 (Verão), p. 187-212, 2002.

ARENDT, Hannah. **As origens do totalitarismo** (trad. Roberto Raposo). São Paulo: Cia. das Letras, 1997.

BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética à Luz do Marco Civil da Internet**. Rio de Janeiro: Brasport. 2016.

BRAR, Harmandeep Singh; KUMAR, Gulshan. Cybercrimes: A Proposed Taxonomy and Challenges. **Journal of Computer Networks and Communications**. v. 2018, p 1-11. DOI: https://doi.org/10.1155/2018/1798659.

BRASIL. Lei "Azeredo". **Lei nº. 12.735 de 30 de novembro de 2012**. Disponível em:< http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm>. Acesso em 25 Set. de 2018.

_____. **Lei "Carolina Dieckman"**. Lei nº. 12.737 de 30 de novembro de 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em 30 Set. de 2018.

_____. **Marco Civil da Internet**. Lei nº. 12.965 de 23 de abril de 2014. Disponível em:< http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 30 Set. de 2018.

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. **Roteiro de atuação: crimes cibernéticos**. 2 ed. rev. - Brasília: MPF/2ªCCR, 2013.

CALDERON, Barbara. **Deep e Dark Web: A internet que você conhece é apenas a ponta do iceberg**. Rio de Janeiro: Alta Books, 2017.

CAMPOS, Gabriel Silveira de Queirós. A importância dos sistemas regionais de proteção aos direitos humanos e a implementação das decisões de responsabilização internacional do estado: breve análise do caso brasileiro. In: VITORELLI, Edilson (Org.), **Temas aprofundados do Ministério Público Federal**. 2ed. Salvador: Juspodium, v. 1, p. 579-591, 2013.

CAMPOS, Gabriel Silveira de Queirós. O combate ao terrorismo no âmbito das nações unidas: o Sistema de sanções direcionadas a indivíduos, as garantias procedimentais do due process of law e os direitos humanos. In: VITORELLI, Edilson (Org.), **Temas aprofundados do Ministério Público Federal**. 2ed.Salvador: Juspodium, v. 1, p. 565-577, 2013.

CANONGIA, Claudia; MANDARINO, Raphael. Segurança cibernética: o desafio da nova Sociedade da Informação. **Parceria. Estratégica**, Brasília, v.14, n. 29, p. 21-46, 2009.

CANOTILHO, Jose Joaquim Gomes. Dogmática de Direitos Fundamentais e Direito privado. In: SARLET, Ingo Wolfgang (Org.), **Constituição, Direitos Fundamentais e Direito Privado**. 2ªed. Porto Alegre: Livraria do Advogado, 2006.

CONVENÇÃO DE BUDAPESTE. **Convenção sobre o cibercrime**. 2001. Disponível em < http://ccji.pgr.mpf.gov.br/documentos/docs_documentos/convencao_cibercrime.pdf >. Acesso em 27 mar. 2019.

DA SILVA CORRÊA, Angélica; RODRIGUES, Cristina Carla; DO AMARAL, Jordana Siteneski. O uso das novas tecnologias frente aos casos de crimes contra a honra: um olhar sobre casos de injúria racial cometidos na internet no Brasil. **Direitos Humanos Contemporâneos**, p. 23-48, 2018.

FERRAZ JÚNIOR, T. S. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito**, v. 88, p. 439-459, 1993.

GORENSTEIN, Fabiana. HIDAKA, Leonardo Jun Ferreira. LIMA, BENVENUTO. Jr., Jayme. (org.). **Manual de Direitos humanos Internacional acesso aos Sistemas global e Regional de Proteção dos Direitos Humanos**. GajopMndh, 2016. Disponível em: <https://www.uniceub.br/media/181730/Texto4.pdf>. Acesso em: 20 ago. 2018.

HINDUJA, Sameer; PATCHIN, Justin W. Bullying, Cyberbullying e Suicídio. **Arquivos de Pesquisa Suicida**, v.14, n. 3, p. 206-221, 2010.

JAPIASSÚ, Carlos Eduardo A. O direito penal internacional e os crimes internacionais. **Revista Interdisciplinar de Direito**, v. 9, n. 1, p. 69-90, 2012.

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

KNIGHT, Peter T. **A internet no Brasil**. Bloomington: AuthorHouse, 2014.

MACHADO, Diego Pereira; DEL'OLMO, Florisbal de Souza. **Direito da Integração, Direito Comunitário, Mertcosul e União Européia**. Salvador: Juspodivm Editora, 2011.

MANDARINO JUNIOR, Raphael; CANONGIA, Cláudia. (Org.). **Livro verde: segurança cibernética no Brasil**. Brasília: GSIPR/SE/DSIC, 2010.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 7ªed. rev. São Paulo: Saraiva, 2012.

MOURA, Milene Rosa de Almeida; COSTA, Luzia Sigoli Fernandes; NAKAGAWA, Elisa Yumi. Diálogos entre Interação Humano-Computador e Ciência, Tecnologia e Sociedade. **Informação & Informação**, v. 23, n. 3, p. 565-585, 2018. DOI: http://dx.doi.org/10.5433/1981-8920.2018v23n3p565.

NATÁRIO, Rui Manuel Piteira. O Combate ao Cibercrime: Anarquia e Ordem no Ciberespaço. **Revista Militar**, n. 2541, p. 823-858. Portugal, 2013. Disponível em: <https://www.revistamilitar.pt/artigopdf/854>. Acesso em 26. Mar. 2019.

NORTON. **Norton Cybersecurity Insights Report**. Disponível em:< https://br.norton.com/norton-cybersecurity-insights-report-global?inid=hho_norton.com_cy bersecurityinsights_hero_seeglobalrpt>. Acesso em 16 jan. 2019.

NORTON. **Relatório de Crimes Cibernéticos: O impacto humano**. Disponível em:< http://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_Portuguese-Human%20Impact-A4_Aug18.pdf >. Acesso em 16 jan. 2019.

NUNES, Danilo Henrique; LEHFELD, Lucas Souza. Cidadania digital: direitos, deveres, lides cibernéticas e responsabilidade civil no ordenamento jurídico brasileiro. **Revista de Estudos Jurídicos**, UNESP, Franca, ano 22, n. 35, p. 437-454, 2018. Disponível em: < https://ojs.franca.unesp.br/index.php/estudosjuridicosunesp/article/viewFile/2542/2359> . Acesso em 27 mar. 2019.

PINHEIRO, Patricia Peck . **Direito digital**. 5. ed. rev.,atual. e ampl. de acordo com as Leis n. 12.735 e 12.737, de 2012 — São Paulo : Saraiva, 2013.

PIOVESAN, Flávia. **Direitos humanos e o direito constitucional internacional**. 14. ed., rev. e atual.– São Paulo : Saraiva, 2013.

PORTELA, Paulo Henrique Gonçalves. **Direito Internacional Público e Privado**. 4ª ed. Rev, amp. e at. Salvador: Justpodivm Editora, 2012.

RAMOS, André de Carvalho. **Curso de direitos humanos**. 4ª ed. São Paulo: Saraiva, 2017.

_____. **Teoria geral dos direitos humanos na ordem internacional**. 2ª ed. Editora Saraiva. São Paulo: 2011.

RAWLS, John**. O direito dos povos ; seguido de A ideia de razão pública revista**. Trad. Luís Carlos Borges. São Paulo: Martins Fontes, 2001.

REZEK, Francisco. **Direito Internacional Público, curso elementar**. 13ª ed. Revista e atualizada. Saraiva: São Paulo, 2011.

SCHJOLBERG, Stein. **The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva**. 2008. Disponível em: <http://www.cybercrimelaw.net/documents/cybercrime_history.pdf>. Acesso em: 18 setembro de 2018.

SHAW, Malcolm N. **International Law**. Sixth edition. Cambridge University Press The Edinburgh Building, Cambridge CB2 8RU, UK.2008.

SILVEIRA, Maria Ana Barroso de Moura. **Da problemática da investigação criminal em ambiente digital: em especial, sobre a possibilidade de utilização de malware como meio oculto de obtenção de prova**. Dissertação (Mestrado Forense). Universidade Católica Portuguesa, Faculdade de Direito - Escola de Lisboa, Lisboa, Portugal, 2017.

SCHATZ, Daniel; BASHROUSH, Rabih; WALL, Julie. Towards a more representative definition of cyber security. **Journal of Digital Forensics, Security and Law**, v. 12, n. 2, p. 8, 2017.

STALLINGS, William; BROWN, Lawrie. **Segurança de computadores: princípios e práticas**. Rio de Janeiro: Elsevier, 2014.

ULRICH, Fernando. **Bitcoin: moeda na era virtual**. São Paulo: Instituto Ludwig von Mises, 2014.

VALENTE, Mariana Giorgetti; NERIS, Natália; RUIZ, Juliana Pacetta; BULGARELLI, Lucas. **O Corpo é o Código: estratégias jurídicas de enfrentamento ao revenge porn no Brasil**. InternetLab: São Paulo, 2016. Disponível em <http://www.internetlab.org.br/wp-content/uploads/2016/07/OCorpoOCodigo.pdf>. Acesso em 18 Fev. 2019.

WESTIN, Alan F. Privacy and freedom. **Washington and Lee Law Review**, v. 25, n. 1, p. 166, 1968.

Recebido em: 01/03/2022

Aprovado em: 30/03/2022

Publicado em: 04/05/2022