

A (In)eficaz atuação do Direito Internacional na proteção dos direitos fundamentais diante da Cibercriminalidade

Xenofontes Curvelo Piló¹

INTRODUÇÃO

A existência de uma nova manifestação do fenômeno criminal, a cibercriminalidade. Com a aproximação dos seres humanos através da globalização da economia, das comunicações e dos indivíduos como consequência acompanhada pelo aumento da criminalidade. A popularização da internet que impactou o mundo, nos anos de 1990, revolucionando conceitos, invadindo lares, empresas, indústrias por fim uma invasão global em todos os lugares do mundo.

Os perigos advindos da conectividade surpreendentemente são desprezados. Um dos precedentes para o aumento da incidência do cibercrime foi a popularização da tecnologia e internet em todo o globo terrestre, também resultante da revolução tecnológica, facilitando ações criminosas dessa espécie, na medida em que se aumenta a quantidade de terminais conectados à rede de internet.

A imaterialidade fez com que novos negócios surgissem desde serviços exclusivamente virtuais, estratégias de atividade, produtos de uso em dispositivos como programas e jogos, além da dificuldade conceitual de determinação do local.

Nasce então os crimes cibernéticos, como uma nova modalidade de crime que pode abalar a própria essência e concepção de personalidade dos indivíduos que são vítimas, notadamente, casos de vingança digital, também conhecidos como revenge ou cyberbullying, intimidação moral ou humilhação pública praticada via internet.

¹ Doutorando e Mestre em Proteção dos Direitos Fundamentais pela Universidade de Itaúna/MG. Bacharel em Direito pela Faculdade Promove, Especialização em Direito Público lato sensu pelo CEAJUF, Especialização em Direito Público lato sensu pela Universidade de Itaúna/MG. Especialização em Ciências Penais lato sensu pelo Centro Universitário Newton Paiva, membro da ABJD - Associação Brasileira de Juristas pela Democracia. Advogado. xenopilo@yahoo.com.br. Currículo Lattes: <http://lattes.cnpq.br/8570712885711499>.

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

Marjie Britz, afirma que em 1997, um subgrupo do G8 voltado ao combate dos crimes de alta tecnologia, chamado G8 subgroup on Hig-tech Crime, criou uma rede denominada 24/7 High-tech Crime Point-of-Contact Network, que visa a interligar policiais de diversos países, inclusive não membros do G8, com a finalidade de facilitar a interlocução e a assistência mútua para repressão ao cibercrime.

Por outro lado, havendo diversas violações aos direitos fundamentais pelos criminosos através do chamado cibercrime, a pergunta que não cala a comunidade internacional e nacional está preparada juridicamente para lidar com os mesmos através da utilização da cibercriminalística nesta revolução tecnológica do século XXI?

Com a finalidade de responder a pergunta, o objetivo deste 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. Tendo objetivos específicos, tem-se de identificar os mecanismos específicos para proteção contra violações praticadas no ciberespaço, considerando o sistema global de proteção aos direitos humanos.

2- Crimes Cibernéticos e os direitos fundamentais-

Com a globalização e a divulgação da Internet, a ausência de limites nas fronteiras dos ciberespaços acomodam não apenas criações em prol da cidadania e da participação universal, mas facilitam que ocorram infrações comuns como os crimes contra o patrimônio e a honra, e os mesmos se moldem ao ciberespaço.

Sendo a internet utilizada, por pessoas inescrupulosas, como pratica de infrações penais vem levado desentendimentos pelo mundo, onde há questionamentos quanto a dificuldade de definir o tempo e o lugar de

determinada conduta criminosa, principalmente pelo fato de tais infrações podem partir de lugares diversos do mundo, e a inexistência de fronteiras típica da web podendo envolver vários ordenamentos jurídicos de países distintos tornando complexa e dificultosa um efetivo combate das atividades criminosas no ciberespaço, bem como estabelecer qual o país competente para processar, julgar e penalizar os infratores.

Atualmente, o Estado Democrático de Direito é adstrito pelos direitos fundamentais, que são “todas aquelas posições jurídicas concernentes às pessoas, que, do ponto de vista do direito constitucional positivo, foram, por seu conteúdo e importância, integradas ao texto da Constituição. (SARLET, 2007)

Continua o autor, na seara dos direitos fundamentais existem quatro dimensões, na atual doutrina constitucional. A primeira geração refere-se às garantias e direitos fundamentais, assumindo “particular relevo no rol desses direitos, especialmente pela sua inspiração jusnaturalista, os direitos à vida, à liberdade, à propriedade e à igualdade perante a lei.”

O que não se deve e não se pode violar, principalmente através de crimes virtuais, são os direitos que correspondem a direitos garantidos à sociedade de forma individual ou coletiva, fundamentais à existência do indivíduo com pleno gozo do princípio da dignidade da pessoa humana.

2.1 A Cibercriminalística como ferramenta contra os crimes cibernéticos de violação dos direitos fundamentais.

A interpretação é elemento fundamental para os crimes modernos pois a grande maioria desses não possui tipificação legal imediata e deve ser enquadrada no ordenamento jurídico existente.

Spencer Toth Sydow afirma que a cibercriminalística é o campo de estudo que se concentra na investigação de crimes cibernéticos, que são aqueles cometidos por meio da internet ou de dispositivos eletrônicos. Incluindo a análise de dados digitais, a coleta de evidências eletrônicas, a identificação de suspeitos e a prevenção de futuros crimes. A cibercriminalística envolve o uso de tecnologia e ferramentas específicas para coletar e analisar informações digitais em casos criminais. (Sydow, 2022).

O autor ainda professa que há um imenso universo a ser estudado, explorado, debatido e redesenhado. Havendo uma infinidade de crimes cometidos utilizando da rede e que merecem a devida atenção. A rede, como a vida real, tem tendências e momentos que, se precisados, permitem a verificação de picos cíclicos de criminalidade específica como a ransomware (bloqueio de acesso de dados).

O que acontece no mundo real, também acontece no mundo cibernético, ou seja, crimes sempre deixam vestígios. Destacando que os vestígios da computação são digitais são informações armazenadas, em uma sequência lógica. O Código de Processo Penal expressa em seu artigo 158 que “quando a infração deixar vestígios será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado”.

A variedade de crimes cometidos pelo uso da internet é espantosa, e até mesmo homicídios já foram cometidos com o uso da rede. Exemplo é o caso de John Edward Robinson- primeiro serial killer conhecido que utilizava a rede , para aliciar suas vítimas, para a prática de relações sadomasoquistas, o mesmo foi condenado no ano de 2000 pela morte de três mulheres e acusado pela morte de oito mulheres nos Estados Unidos. (BRITZ, 2009).

A enumeração dos direitos humanos não é exaustiva ou até mesmo *numerus clausus* e sim aberto às novas necessidades da espécie humana para promoção da dignidade da pessoa humana. Deste modo, o direito à intimidade, por exemplo, traz obrigação ao Estado e aos particulares na forma que a “ausência de direito”, vez que não é 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), porém o direito à propriedade seria uma espécie de sujeição de particulares e do Estado ao indivíduo proprietário.

Os direitos fundamentais do ser humano são protegidos através de normas internacionais de direitos humanos, contudo, não há norma específica no tratamento das violações de direitos humanos mencionados por meio da rede de conexão global, a internet .

É forçoso divulgar que o funcionamento do sistema global de proteção aos direitos humanos para as normas internacionais que protegem os direitos

fundamentais, inexistindo assim norma específica no âmbito da comunidade internacional.

3- O Direito Internacional e o Cibercrime.

Considera-se que a internet é utilizada como ferramenta de comunicação geral, servindo tanto para contatos pessoais privados como para negócios, sejam eles lícitos ou ilícitos, por mais que venhamos a preservar a privacidade dos usuários não se pode negar também o direito de segurança coletiva e a obediência as leis do país onde se desenvolve sua atividade, desta feita os obstáculos gerados com o mau uso da internet poderiam ser evitados através de acordos de cooperação de permuta de dados entre países.

Spencer Sydow advoga que colisão de legislações de países diferentes, envolvidos, contudo, em uma rede comum mostrou a dificuldade para a investigação, apuração e punição de condutas ali perpetradas. Realidades sociais e jurídicas diversas, caminhando num mesmo trilho. Investigações policiais passaram cada vez mais misturar competências. (SYDOW, 2022)

O autor ainda professa que ano após ano os meios de mídia especializada apresentam crescimento dos delitos praticados através da rede mundial de computadores e da tecnologia. A verdade é que a criação de um novo segmento da vida em sociedade exige dedicação de um novo ramo de estudo comportamental. A cibercriminologia estuda o crime, o comportamento do cibercriminoso, as cibervitimas, as ciberleis e a ciber investigação. (SYDOW, 2022)

Fato é que a existência de um imenso universo a ser estudado, explorado, debatido e redesenhado, uma infinidade de crimes cometidos utilizando-se da rede e que merecem a devida atenção. A rede, como a vida real, tem tendencias e momentos que, permitem a verificação de picos de criminalidade.

3-1. A (in)eficácia do Direito Internacional em relação ao Cibercrime na proteção dos direitos fundamentais-

Com toda essa incorporação social ao meio digital, os crimes praticados do mundo real não estariam apartados do mundo paralelo virtual, assim, a cada dia existe a ameaça ao indivíduo por meio do cibercrime. Seja através de furto de informações, seja de vendas de produtos ilegais, ou até mesmo de publicações com informações falsas prejudiciais.

Alessandro Barreto, professa ser importante ressaltar que os cibercrimes, tal qual os outros delitos graves, como tráfico internacional de drogas, de pessoas e o terrorismo, não são alcançados pela competência do Tribunal Penal Internacional. Os crimes internacionais sob a égide do direito penal internacional, são limitados a genocídio, agressão, crimes de guerra e contra humanidade. Este diminuto escopo se dá pela fragilidade do direito internacional em relação ao direito interno dos países. A independência das nações, conferida pela soberania, torna sinuosa a criminalização de condutas delitivas diante de diversos obstáculos decorrentes de interesses políticos, religiosos e econômicos.(BARRETO,2020)

No cenário internacional, a questão econômica é priorizada em relação o social e é atribuído uma posição de destaque às empresas e entes financeiros internacionais, com identidade de destaque nas relações de governo e de importância no processo globalizante. A internet não foi criada inicialmente com o objetivo a que se serve hoje. Inicialmente, conforme Diniz (2015), a rede mundial foi concebida com intuito acadêmico e militar, sendo que as forças armadas oficiais objetivavam comandar uma força nova de tecnologia com o fim de observação e captação de informações dos inimigos.

A segurança nos meios eletrônicos, infelizmente, ainda é uma questão a ser avançada tecnologicamente, vez que, muitos são os avanços e também há muito a ser desenvolvido. Várias empresas na área de tecnologia da informação expandem e atualizam sistemas de segurança diuturnamente, pois os ataques contrários também são constantes e rápidos. Um dos enormes problemas da forma de consumo por meio da internet é precisamente a segurança nas transações, pois depreende-se do uso de dados pessoais, bancários, de cartões de crédito, etc.

O medo de utilização está na possibilidade de desvio de finalidade desses dados (MARQUES, 2013). De acordo com Marques (2013), a segurança sempre é motivo de preocupação do ser humano; afinal a proteção à vida é fundamental. No mundo digital a proteção é para os dados pessoais, já que ninguém quer ver seus dados usados de forma indevida ou ilícita. Na medida em que o mercado digital cresce, aumentam também as tentativas de burlar esse sistema. Assim, as

empresas que estão em destaque no mundo digital são sempre alvos constantes de pessoas mal-intencionadas (hackers).

As tecnologias de segurança existentes são diariamente testadas e põem à prova a privacidade dos dados de usuários e empresas, mesmo que utilizados corretamente, dentro das indicações técnicas. A privacidade sobre as informações, como cartões de crédito, contas bancárias e senhas devem ser protegidas com o uso correto da segurança e frequentemente modernizadas a fim de acompanhar o processo criminoso que circunda o mundo virtual, e disso depende o sucesso e expansão do comércio eletrônico. Tal vulnerabilidade existente na rede faz com que as empresas do ramo tenham que investir cada vez mais nos sistemas de segurança, tornando-os mais eficazes em se tratando de proteção, com novos softwares.

Conforme dados da Interpol, há muitas organizações internacionais regionais, com finalidade de cobertura restrita ou ampla de estados e regiões, fazendo esforços para manter a segurança cibernética e harmonizar o meio social virtual e seus deslindes com tais medidas internacionais para combater o cibercrime. Na região Ásia-Pacífico, a APEC controla suas 21 economias membros para fim de promover a segurança cibernética com enfrentamento dos riscos trazidos pelo cibercrime. A APEC tem conduzido um projeto de capacitação sobre cibercrimes para os entes membros em relação a estruturas legais e investigativas, onde as economias mais avançadas da APEC apoiam outras economias- membros no treinamento de pessoal legislativo e investigativo (INTERPOL, 2012).

A Convenção de Budapeste reconheceu em seus termos a conveniência de estender as salvaguardas para todos os direitos e liberdades fundamentais, pois que universais, e, especificamente o direito ao respeito pela privacidade, tendo em conta o crescente fluxo através das fronteiras dos dados pessoais sujeitos a tratamento informático, e a necessidade conciliar os valores fundamentais do respeito à privacidade e ao livre fluxo de informação entre os povos. A União Europeia tomou uma série de medidas para combater a cibercriminalidade, impulsionando política coordenada de aplicação da lei e de harmonização jurídica. A liberdade civil também tem sido um foco no campo anti cibercrime.

A Organização dos Estados Americanos (OEA), como outras organizações regionais, com 35 Estados membros, também está muito preocupada com a questão do cibercrime. Por meio de seu fórum para os Ministros da Justiça ou Procuradores-Gerais das Américas, a OEA reconhece há muito tempo o papel central que uma estrutura legal sólida desempenha no combate ao cibercrime e na proteção da internet.

O fato é que o direito penal internacional tradicional tem por objetivo harmonizar o direito substantivo e coordenar o direito processual sobre as ofensas que existem na sociedade desde o surgimento da humanidade. Em razão da complexidade estrutural e universalidade da Internet, pelas frágeis leis que regulam o ciberespaço, pela ineficácia na prática das leis internas de um país, somada a dificuldade de identificar e processar um criminoso que atinge diversas nações, os cibercriminosos atuam livremente certos da impunidade.

CONSIDERAÇÕES FINAIS

Há um imenso universo a ser estudado, explorado, debatido e redesenhado em relação ao cibercrime. É indiscutível que a rede seja mundial, mesmo havendo mistura indiscernível de usuários por toda a supervia, mesmo que o ambiente virtual gere uma sensação de universalidade e igualdade material e formal, nessa seara podendo ocorrer crimes cibernéticos. Reportando a Pablos Molina, o mesmo advoga que para o estudo criminológico há três formas de prevenção de conflitos para qualquer espécie de infração penal, sendo a prevenção primária- implementação de medidas indiretas de prevenção-, a prevenção secundária- sobre grupos sociais propensos ao crime- e a prevenção terciária- prevenir a reincidência voltada ao delinquente.

É fundamental um esforço global, com atuação em vários segmentos sociais, onde leis sejam bem elaboradas, homogêneas e atualizadas com as demandas advindas do ciberespaço e processos céleres que se amoldem à dinâmica dos cibercrimes são imprescindíveis para uma tutela eficaz. A sistemática de informações globalizadas acomoda um número crescente de ofensas transnacionais. A circunstância da rede do cibercrime faz com que seja uma das ofensas mais globalizadas das ameaças atuais e mais modernizadas do futuro.

O cibercrime tem efeitos devastadores no mundo físico. O cenário é ainda mais complicado pela própria natureza do espaço cibernético manifestado no anonimato no espaço e no tempo, e a não atribuição de ações e ausência de fronteiras internacionais.

Pari e passo questões envolvendo a internet quando há colisão entre o direito brasileiro e o direito internacional é necessário para a solução desses conflitos através de criação de regras advindas do Direito Internacional tanto por meio de tratados, acordos de colaboração internacional ou qualquer outro meio solução de controvérsias.

Bibliografia

BARRETO, Alesandro Gonçalves Karina Kufa, Marcelo Mesquita Silva- Cibercrimes e seus reflexos no direito brasileiro- Juspodium- Salvador- 2020, p.99

BRITZ, Marjie T. Computer forensics and cibercrime: na introduction. New Jersey Prntice Hall, 2009, p. 207

BRITZ, Marjie T. Computer forensics and cibercrime: na introduction. New Jersey Prntice Hall, 2009, p. 7-8

DINIZ, E. H.; Fonseca, C. E. C.; e Meirelles, F. S. Tecnologia bancária no Brasil: uma história de conquistas, uma visão do futuro. São Paulo: FGV. 2015, p.15

INTERPOL. Disponível em: <<https://www.interpol.int/News-andmedia/Publications2/Fact-sheets2>>. Acesso em: 27 nov. 2023.

MARQUES, Érico V. Uma análise das novas formas de participação dos bancos no ambiente de negócios na era digital. Relatório de Pesquisa. Centro de Excelência Bancária. EAESP-FGV. 2013, p.12

PABLOS DE MOLINA, Antonio Garcia, Criminologia,5ª Ed. Revista dos Tribunais, São Paulo, 2006, p. 312

SARLET, Ingo Wolfgang. A eficácia dos direitos fundamentais. 8. ed. rev. atual. Porto Alegre: Livraria do Advogado, 2007. p.77.

SYDOW, Spencer Toth- Direito Penal Informático- 3ª ed.- Ed. Juspodium-2022- Salvador- p.734

Sydow, Spencer Toth, Direito Penal Informático- 3ª ed., Editora Juspodium, Salvador, 2022, p.733