DESAFIOS JURÍDICOS NA ERA DIGITAL: A DEFESA DOS DIREITOS DAS VÍTIMAS EM CRIMES CIBERNÉTICOS PELO MINISTÉRIO PÚBLICO

LEGAL CHALLENGES IN THE DIGITAL AGE: THE DEFENSE OF THE RIGHTS OF VICTIMS IN CYBER CRIMES BY THE PUBLIC PROSECUTION OFFICE

Renata Caroliny Ribeiro e Silva[1]
Alesandro Gonçalves Barreto[2]

Resumo: O desevolvimento do presente artigo tem o intuito de trazer uma compreensão sobre a atuação do Ministério Público na proteção dos direitos das vítimas de crimes cibernéticos, visando compreender um panorama específico sobre os desafios que permeiam o âmbito investigativo e de apoio às vítimas afetadas. Para tanto, é preciso trazer uma análise panorâmica dessa modalidade de crime, principalmente com o seu aumento durante e após a pandemia da Covid-19, bem como é preciso analisar uma nova perspectiva do conceito de vitimologia e das principais caracterísicas desse crimes específicos. Considerando esses aspectos, o problema específico está centrado em investigar como a atuação do Ministério Público nos casos práticos pode servir para auxiliar a condição das vítimas e dos efeitos materiais e psicológicos por elas suportados. Nesse sentido, o objetivo geral está centrado em examinar a atuação do Ministério Público na defesa dos direitos das vítimas de crimes cibernéticos, visando investigar como as práticas institucionais podem contribuir para a proteção efetiva dos afetados por delitos digitais. Por sua vez, a pesquisa social será qualitativa, sendo estruturada com base no método hipotético-dedutivo, possibilitando entender a atuação prática do Ministério Público perante o combate e a prevenção desta modalidade de crime, principalmente com o foco na condição das vítimas e dos efeitos materiais e psicológicos por ela suportados.

1 Pós - Graduada em Direito Público pela Universidade Cândido de Morais - UNICAM (2014). Atualmente é Promotora de Justiça do Ministério Público do Estado de Goiás (2016-atual) e Coordenadora do Núcleo de Assessoramento Temático e de Fomento na Área Criminal para promoção de Direitos e de Apoio às Vítimas (NAT-Vítimas). E-mail: renatacaroliny@mpgo.mp.br. Cnpq Lattes: http://lattes.cnpq.br/0433667518886492.

2 Possui graduação pela Universidade Regional do Cariri (1998). Pós-graduado em Direito pela Universidade Federal do Piauí. Diretor da Unidade do Subsistema de Inteligência da Secretaria de Segurança Pública do Estado do Piauí de 2005 até 2016. Integrou o Grupo de Trabalho que revisou a Doutrina Nacional de Inteligência de Segurança Pública. Professor de Cursos de Inteligência Cibernética pela SENASP e SEOPIe nas Escolas de Magistratura do Mato Grosso, Paraíba e Bahia. Colaborador eventual da SESGE-MJ e Coordenador do NUFA - Núcleo de Fontes Abertas da Secretaria Extraordinária para Segurança de Grandes Eventos do Ministério da Justiça durante a Olimpíada do Rio de Janeiro em 2016. Atuou como Coordenador Geral de Contrainteligência da Diretoria de Inteligência e posteriormente como colaborador eventual da Secretaria Nacional de Segurança Pública. Atualmente é servidor mobilizado da Secretaria de Operações Integradas do Ministério da Justiça e Segurança Pública. delbarretoacademia@gmail.com. http://lattes.cnpq.br/7549439127781463.

Palavras-chave: Ministério Público; crimes cibernéticos; direitos vítimas.

Abstract: *The development of this article purposes to bring an understanding of the role of the Public Prosecutor's Office in protecting the rights of victims of cybercrime, aiming to understand a specific overview of the challenges that permeate the investigative and support scope for victims affected by the practice of cybercrimes. To this end, it is necessary to provide a panoramic analysis of cybercrimes and their increase, especially during and after the Covid-19 pandemic period, as well as to analyze a new perspective on the victimology's concept and the main characteristics of cybercrimes. Considering these aspects, the specific problem is centered on investigating how the actions of the Public Prosecutor's Office in practical cases of cybercrimes can serve to help the condition of victims and the material and psychological effects they suffer. In this sense, the general objective is centered on examining the role of the Public Prosecutor's Office in defending the rights of victims of cybercrimes, aiming to investigate how institutional practices can contribute to the effective protection of those affected by digital crimes. In turn, the social research will be qualitative, being structured based on the hypothetical-deductive method, making it possible to understand the practical actions of the Public Prosecutor's Office in combating and preventing the practice of cybercrimes, mainly focusing on the condition of victims and the material and psychological effects supported by them.*

Keywords*: prosecutor's office; cybercrimes; victim's rights.*

1. INTRODUÇÃO

O presente artigo propõe uma análise crítico-construtiva da atuação do Ministério Público na proteção dos direitos das vítimas de crimes cibernéticos, tendo a finalidade de delinear um panorama que busca compreender os desafios e avanços nesse campo específico do Direito. Essa problemática mostra-se pertinente, tendo em consideração o contexto jurídico do papel de fundamental importância que o Ministério Público exerce, principalmente no seu compromisso com a defesa dos direitos individuais e coletivos em sentido estrito, especialmente aqueles das vítimas.

Nesse sentido, considerando os aspectos acima delineados, percebe-se, enquanto problema específico, o intuito de investigar como a atuação do Ministério Público nos casos práticos de crimes cibernéticos pode servir para auxiliar a condição das vítimas e dos efeitos materiais e psicológicos por elas suportados.

A construção do problema em questão levou em consideração a importância em buscar compreender melhor a atuação do Ministério Público enquanto órgão de proteção dos direitos individuais e coletivos em sentido estrito, razão pela qual o objetivo geral vai examinar a atuação do

Ministério Público na defesa dos direitos das vítimas de crimes cibernéticos, visando investigar como as práticas institucionais podem contribuir para a proteção efetiva dos afetados por delitos digitais.

Por sua vez, no tocante aos objetivos específicos, eles vão estar voltados para explorar as leis e regulamentações relacionadas aos crimes cibernéticos e à proteção das vítimas, avaliando as disposições legais existentes e sua relação com o princípio da igualdade material; bem como para analisar os procedimentos processuais utilizados pelo Ministério Público na condução de casos paradigmas de crimes cibernéticos, identificando eventuais obstáculos, analisando as áreas de aprimoramento.

Assim, em seu aspecto metodológico, a pesquisa social é qualitativa e estruturada com base no método hipotético-dedutivo, possibilitando entender a atuação prática do Ministério Público perante o combate e a prevenção da prática de crimes cibernéticos, principalmente com o foco na condição das vítimas e dos efeitos materiais e psicológicos por ela suportados.

Nesse contexto, a revisão de bibliografia, principalmente com a análise de literatura, artigos, leis e notícias de jornais e revistas, tornou possível a formulação dos aspectos conceituais, principalmente na compreensão dos crimes cibernéticos, no resgate ao conceito amplo da vítima em seu aspecto subjetivo, possibilitando entender a existência e a necessidade da estruturação e a viabilidade desses institutos jurídicos capazes de resguardar a vítima, evitando os processos de revitimização e o apoio psicológico adequado.

Igualmente, o segundo momento vai abordar e demonstrar a importância e a necessidade da atuação do Ministério Público no aspecto prático relacionado aos crimes cibernéticos, momento oportuno para se abordar o tipo de crime e as partes envolvidas.

Em deslinde, haverá a abordagem dos aspectos práticos e as políticas públicas formuladas pelo Ministério Público no cuidado e resguardo das vítimas desses casos, principalmente para aquelas que sofrem exposição e são atacadas no espaço cibernético, compreendendo a importância dessas políticas públicas e sua capacidade de servir em auxílio direto à condição psicológica da vítima.

2. ASPECTOS GERAIS SOBRE OS CRIMES CIBERNÉTICOS

Com efeito, o ritmo das inovações em Tecnologia da Informação (TI), desde o surgimento da internet e a introdução do e-mail, em 1960, até o crescimento das plataformas de redes sociais no início dos anos 2000 e, mais recentemente, o desenvolvimento da Internet das Coisas (Internet of Things – IoT) e da rede 5G são realmente surpreendentes pela rapidez com que novas tecnologias passaram a afetar diversos aspectos da vida em sociedade.

Todavia, com o crescimento das novas formas de tecnologia e o seu alcance transfronteiriço, também houve o surgimento de novas condutas consideradas criminosas, pois violam diretamente os preceitos de liberdade, igualdade e dignidade da pessoa humana. Por essa razão, percebe-se que os crimes cometidos por meio da *World Wide Web* vêm aumentando vertiginosamente, conforme é demonstrado em relatório apresentado pela Organização das Nações Unidas (ONU).

Segundo a ONU, "Apenas 66% dos países salvaguardam os dados e a privacidade dos seus cidadãos", razão pela qual o Brasil tem apresentado um aumento significativo das denúncias de crimes cibernéticos, principalmente daqueles envolvendo a prática de discursos de ódio (ONU, 2020, *online*), de modo que, no ano de 2022, "mais de 74 mil denúncias de crimes envolvendo discurso de ódio pela Internet foram encaminhadas para a Central Nacional de Denúncias de Crimes Cibernéticos da Safernet (...) e representou aumento de 67,7% em relação a 2021" (CRUZ, 2023, *online*).

Além dessa informação, é pertinente ainda perceber o crescente uso da internet para a prática de crimes diversos. Em atenção aos dados disponibilizados pela *Safernet*, percebe-se que, nos seus 17 anos de funcionamento, em escala global, o crime que mais foi denunciado, com um total de 1.973.116 denúncias, foi o de pornografia infantil, "envolvendo 524.197 páginas (URLs) distintas (das quais 415.085 foram removidas), escritas em 10 idiomas". Atrás desse crime, encontra-se o de Apologia e Incitação a crimes contra a Vida, com um total de 767.938 denúncias, e o de Racismo, com um total de 606.125 denúncias (SAFERNET, 2022).

Ainda, segundo Steve Morgan, fundador e editor-chefe da *Cybersecurity Ventures*, caso fosse medido como um país, o cibercrime seria a terceira maior economia do mundo, atrás apenas dos Estados Unidos e da China. Ademais, estima-se que os custos com o cibercrime atingirão $10.5 trilhões de dólares anualmente até 2025, o que representa a maior transferência de riqueza econômica da história, custos esses que impõem maiores riscos a iniciativas de inovação e são exponencialmente maiores que o valor dispendido em danos provocados por catástrofes naturais. Além disso, acrescenta Morgan (2020, *online*), o cibercrime representa um ramo da economia mais lucrativo do que o comércio mundial de todas a principais drogas ilegais combinadas.

Destacada a evolução da cibercriminalidade, a par de definir o termo crimes cibernéticos, tal como adotado na Convenção de Budapeste, da qual o Brasil é signatário, explicitam Wendt e Jorge (2021, p.15) que pode ser considerado como sinônimo de crimes virtuais, e são aqueles cometidos por intermédio de computadores, subdividindo-se em aberto e exclusivamente cibernéticos. Enquanto estes necessariamente precisam da informática para serem praticados, aqueles podem ou não ser praticados pelo meio informático.

A título de exemplo e entre os crimes cibernéticos mais comumente praticados, conforme pontuado na obra de autoria de Alessandro Gonçalves Barreto e Natália Siqueira da Silva (2022), estão

as fraudes bancárias, estelionato eletrônico, clonagem de WhatsApp, sequestro de dados (*ramsonware*), boletos falsos, sites fraudulentos, golpes sentimentais, invasão de dispositivo informático, e alguns outros, como sextorsão, pedofilia, *stalking*, crimes contra a honra, leilão falso, apologia ao crime, preconceito e discriminação.

Relevante esclarecer que, na construção da pesquisa que ora se delineia, utilizaremos a conceituação de vítima advinda da ideia de que o objeto da vitimologia não está adstrito às vítimas diretas dos delitos, podendo estender-se para abranger as demais pessoas envolvidas em um processo vitimizatório.

Nesse sentido, é preciso considerar que o atual momento enfrentado pela sociedade brasileira demanda uma resposta efetiva e sensível às vítimas, considerando a complexidade crescente dos casos legais e a evolução das formas de vitimização, incluindo crimes digitais e novas modalidades de violência cibernética. Além disso, percebe-se a necessidade de se realizar uma análise crítica das práticas atuais, a fim de contribuir para o aprimoramento contínuo do sistema de proteção, resultando em um Ministério Público mais eficaz na promoção da justiça e na salvaguarda dos direitos das vítimas.

Importante entender que o enfoque criminológico na pessoa da vítima perpassou momentos de total destaque a pouco ou nenhum interesse, motivo pelo qual é crucial desenvolver uma temática que devolva às vítimas a deferência que merecem.

Com efeito, o estudo da evolução das formas de resolução de conflitos, que passou pelas fases de autotutela, autocomposição e jurisdição, demonstra que o olhar para a vítima foi perdendo espaço, à medida que o direito de resposta ao delito, originalmente com protagonismo daquele que foi violado em seus direitos, passou para um poder central, desde os primórdios da Monarquia. Isso porque, na origem, a sociedade importava-se mais com a pessoa vitimada do que com o fato em si.

Todavia, com as mudanças da sociedade capitalista e o advento da teoria causalista do delito, o desvalor do resultado, com a objetividade da análise da lesão, afastou a relevância do estudo da vítima, de caráter subjetivo. Somente com a consolidação das teorias funcionalistas, em especial, da imputação objetiva, houve a retomada da importância de também se considerar a vítima como fundamental na ecologia do delito.

Especificamente sobre a cibercriminologia, verifica-se que as vítimas desse tipo de criminalidade necessitam de um olhar atento das autoridades e aplicadores do Direito, já que:

> legislações surgiram para proteger bens jurídicos antigos violados por novos modos e também para proteger novos valores. Vítimas especiais foram surgindo. Novos *modus operandi*. Novas dinâmicas e golpes. Espécie nova de delinquência, novas doenças, novos problemas psicológicos, e assim por diante. (SYDOW, 2022, p. 734).

Por isso, os crimes cibernéticos inauguraram uma nova área de pesquisa em vitimologia, a qual se mostra complexa devido aos novos aspectos desses tipos de crimes no sentido vitimológico, como a tecnologia envolvida, a possibilidade remota de atingir vítimas adistância, o potencial de atingir diversas vítimas com uma única ação, etc.

De acordo com pesquisas prévias, há características específicas dos crimes cibernéticos, diferentemente dos crimes em geral, que influenciam o impacto causado às vítimas, como: 1) a intrusão na vida privada ou no dia a dia da vítima; 2) a imprevisibilidade, incontrolabilidade e intangibilidade do crime; 3) a intencionalidade e propósito do ofensor; 4) a potencial distância social entre ofensor e vítima; e 5) os níveis de contribuição da vítima para a ocorrência do crime (BORWELL; STOL, 2021).

Comumente, vítimas de crimes cibernéticos relatam sentirem raiva, medo, mal-estar, pensamentos persecutórios em suas próprias casas e impotentes de se defenderem, mesmo sendo confiantes em relação ao uso das tecnologias. Ademais, geralmente sentem-se com vergonha e culpadas quando são trapaceadas pelos autores desses crimes, acusando-se por não terem agido de maneira diversa para se protegerem[3].

Ademais, alguns aspectos do cibercrime, como escalabilidade, ser transfronteiriço, intangível e permanente, resultam em duradoura e recorrente vitimização, com prováveis consequências recidivas (LEUKFELDT et al., 2018).

Para exemplificar, diferentemente dos crimes de assédio ou *bullying* cometidos de forma *offline*, quando praticados de forma *online*, como a ofensa não possui um final claro, provoca nas pessoas em geral uma necessidade de maior cuidado ao compartilhar suas visões de mundo abertamente. E, por ser cometido de maneira *online*, o ofensor é capaz de atingir as vítimas a qualquer hora e em qualquer lugar, o que faz com que essas não se sintam seguras em lugar nenhum. Também, os ofensores sentem-se intocáveis, porque operam a distância e de maneira anônima, o que faz com que, na perspectiva das vítimas, eles possam sempre reaparecer para cometer novamente o crime (LEUKFELDT et al, 2018).

Com relação a delitos de sextorsão, crimes contra a honra, assédio e *stalking*, verifica-se que o longo alcance que as imagens ou mensagens indesejadas podem ser espalhadas na internet induzem nas vítimas alto nível de ansiedade, devido à percepção de que aquele conteúdo pode ficar *online* por prazo permanente e indeterminado.

3 Disponível em: <https://www.victimsupport.org.uk/crime-info/types-crime/cyber-crime/>. Acesso em: 5 mai. 2024.

Pertinente abordar que a violência cibernética também possui suas peculiaridades, sendo conceituada como "aquela praticada por meio das redes sociais, fóruns, mensagens privadas e outros espaços virtuais" (TJRJ, 2024, p.10):

> A violência on-line pode ocorrer por meio de e-mails ameaçadores ou de assédio, mensagens instantâneas ou posts de informações on-line. Pode ser direcionada a uma pessoa específica, entrando em contato diretamente com ela, ou resultar na divulgação de informações pessoais dessa pessoa, causando constrangimento, medo ou raiva (TJRJ, 2024, p. 11).

Outro ponto a ser analisado é o fato de que as pessoas compreendem seus aparelhos eletrônicos como uma extensão de si mesmas, fazendo com que o sentimento obtido com relação aos cibercrimes seja tão ou mais invasivo que crimes cometidos fisicamente (AGUSTINA, 2015), o que se intensificará progressivamente, à medida que avatares forem sendo adotados de forma personificada no metaverso.

Pertinente a inclusão, nesse aspecto, da teoria do ciborgue, de Donna Haraway, segundo a qual usuários de dispositivos como *smartphones* e computadores tornaram-se uma mistura de humanos e máquinas, denominados ciborgues, o que resultará no desaparecimento dos limites atualmente experimentados entre tecnologia e o indivíduo em caso de ataques a algum dispositivo eletrônico.

De um ponto de vista prático, ademais, a produção de conhecimento a respeito do impacto de crimes cibernéticos para as vítimas, com a noção das diferenças intrínsecas se comparado às consequências dos crimes em geral, pode aprimorar políticas de atendimento às vítimas pelas Delegacias de Polícia, Ministério Público e Poder Judiciário.

Assim, inevitável anotar a diferença existente entre as forças de segurança pública destinadas a reprimir crimes, já que, enquanto há estruturas preventivas bem atuantes para a proteção física das vítimas de crimes em geral, tal como a Patrulha Maria da Penha, no âmbito da Polícia Militar, na seara digital, a atuação preventiva ainda é desprovida de tais organismos especializados.

Ademais, a adoção de práticas para combater crimes cibernéticos perpassa pela criação de novos modelos de atuação, que levem em consideração a interestadualidade e transnacionalidade delitiva, que acarreta dificuldades, inclusive, na definição da competência para processamento da investigação e ação penal.

Com isso, urge o fortalecimento de órgãos centrais de investigação para o direcionamento de demandas, com a identificação de especialidades entre as diversas unidades do Ministério Público brasileiro, a fim de evitar a superposição de investigações sobre as mesmas pessoas ou organizações criminosas.

Desse modo, a especialização do atendimento às vítimas de crimes digitais por parte do Ministério Público, com enfoque de gênero, inclusive, contribuirá para a prevenção geral do delito, a cessação de atuações que provoquem a vitimização secundária e terciária, o respeito de seus direitos perante as plataformas digitais, também na qualidade de consumidores que são, e perante o Judiciário como um todo, mediante a obtenção de resultados práticos, rápidos e eficientes nas demandas a ele dirigidas.

Por fim, o tema é de grande valia, pois há pouca produção acadêmica que aborde o papel fundamental do Ministério Público na proteção e atendimento dessas vítimas. Há estratégica variedade de artigos escritos por parte do segmento da advocacia que a enaltecem no desempenho da função de orientar e dialogar com as vítimas de crimes cibernéticos.

Todavia, salvo melhor juízo, e sem declinar a importância de existirem vários atores exercendo esse múnus, o Ministério Público é instituição constitucionalmente vocacionada para proteger as vítimas, porquanto desenhada como titular da ação penal, a quem compete primordialmente o exercício de

> zelar para que sejam assegurados os direitos à informação, segurança, apoio, proteção física, patrimonial, psicológica, documental, inclusive de dados pessoais, participação e reparação dos danos materiais, psicológicos e morais suportados pelas vítimas em decorrência de delitos penais e atos infracionais (artigo 4º da Res. n. 243/2021 do Conselho Nacional do Ministério Público – CNMP).

3. PONDERAÇÕES SOBRE A ATUAÇÃO PRÁTICA DO MINISTÉRIO PÚBLICO FRENTE AO CIBERCRIME

Ciente de seu papel constitucional de titular da ação penal e defensor dos direitos e garantias fundamentais, o Ministério Público pode desempenhar um papel crucial na proteção das vítimas e na promoção de um ambiente digital mais seguro, por meio da adoção de uma série de medidas. Isso porque, para além de órgão de persecução penal, o Ministério Público deve se preocupar com a prevenção e a reparação de crimes, entre eles os cibernéticos.

Com efeito, da análise dos crimes cibernéticos, percebemos que as principais vítimas, embora possam incluir qualquer pessoa que utilize a internet, são crianças e adolescentes, extremamente vulneráveis a *cyberbullying*[4] e exposição a conteúdo inapropriado; e idosos, devido à falta de familia-

4 A Lei n. 14.811/24, sancionada pelo presidente Luiz Inácio Lula da Silva, incluiu no Código Penal os crimes de *bullying* e *cyberbullying* em seu artigo 146-A, com penas de multa e de reclusão, de 2 a 4 anos, e multa, respectivamente, se a conduta não constituir crime mais grave.

ridade com práticas digitais seguras. Mas também incluem empresas de variados ramos, como instituições financeiras, que podem ser alvo de ataques cibernéticos visando ao roubo de dados com ou sem direitos autorais, de titularidade de milhares de clientes – então vítimas secundárias, ou a interrupção de serviços, ou extorsão (*ramsonware*). O mesmo ocorre com o Governo, cujos órgãos e secretarias, por guardarem informações sensíveis, estão sujeitos aos mais variados crimes cibernéticos.

Nesse sentido, a diversidade de vítimas destaca a importância de medidas abrangentes para proteger diferentes setores da sociedade contra crimes digitais. A fim de proteger os direitos das vítimas, primeiramente, é necessário educar as pessoas sobre os riscos *online* e a adoção de boas práticas de segurança na internet, bem como incentivar práticas de segurança digital na criação de tecnologias. Também é fundamental apoiar e promover leis que protejam as vítimas de crimes digitais e que garantam a privacidade *online* das vítimas.

Ademais, é necessário que haja o incentivo para que as vítimas colaborem com autoridades competentes, denunciando os incidentes ocorridos que as afetem de forma individual e coletiva, diminuindo o índice de cifras negras ainda gritante nesse espaço.

Dentre as variadas frentes de atuação, destacam-se a promoção da conscientização por meio de programas educacionais para informar a população sobre riscos e práticas seguras na internet[5]; a participação na criação e atualização de leis que abordem questões específicas relacionadas aos crimes digitais; a implementação de tecnologias que fortaleçam a segurança digital em seus sistemas internos; a criação de estruturas específicas dentro do Ministério Público[6] e o treinamento contínuo de seu membros e servidores para lidar com casos complexos; a fiscalização do cumprimento de leis

5 O projeto "Ministério Público pela educação digital nas escolas" foi desenvolvido pelo Ministério Público Federal em parceria com a ONG SaferNet Brasil em 2009. Outra sugestão, é fomentar a comemoração do Dia Internacional da Internet Segura, em 7 de fevereiro, criado com o objetivo de incentivar o uso livre e seguro de computadores e celulares por parte de instituições e usuários, com foco principal nos mais jovens, por meio de palestras e cursos voltados aos públicos interno e externo. Ainda, destaca-se a atuação do MPMG (2024), o qual tem realizado divulgações na rede social do Instagram informando sobre o golpe do amor no mês da mulher.

6 Entre inúmeros Ministérios Públicos brasileiros, o Ministério Público do Estado de Goiás instituiu o Grupo de Atuação Especial de Combate ao Crime Cibernético (CYBERGAECO), por meio do Ato PGJ n. 98, de 5 de outubro de 2023, considerando "o crescimento exponencial de crimes praticados em meios cibernéticos, vinculados à criminalidade organizada ou não, os efeitos danosos de tais condutas e a necessidade de aprimorar a estrutura interna do Ministério Público do Estado de Goiás para atuar no combate de tais práticas de maneira global e eficaz, bem como para oferecer apoio às Promotorias de Justiça criminais com atuação no tema".

relacionadas à proteção de dados pessoais; e a realização de parcerias com a sociedade civil[7], a fim de ampliar o alcance das iniciativas de proteção às vítimas contra crimes digitais, por meio do desenvolvimento de tecnologias seguras aos usuários.

Relevante apontar a formalização, em 2017, de Termo de Mútua Cooperação Técnica, Científica e Operacional entre o Ministério Público Federal, a *Safernet* Brasil e o Núcleo de Informação e Coordenação do Ponto BR (NIC.BR) com a finalidade de unir esforços para prevenir e combater a pornografia infantil, a prática de racismo e outras formas de discriminação, instrumentalizadas via internet, o que prevê a união de esforços e objetivos institucionais, o intercâmbio e difusão de tecnologias, o desenvolvimento de projetos e atividades voltados para o treinamento de recursos humanos, por meio de parcerias de estudos e pesquisas, intercâmbio de informações e tecnologias e promoção de campanhas conjuntas de conscientização da sociedade.

Mais detalhadamente, é importante que os Ministérios Públicos Estaduais e da União criem em suas estruturas Núcleos ou Centros de Apoio e Atendimento Especializado às Vítimas[8], sendo um dos focos as especificidades das vítimas de crimes cibernéticos, com enfoque em aspectos de gênero da revitimização, inclusive:

> De acordo com a ONG SAFERNET, o número de denúncias de crimes na Internet relacionados a violência contra a mulher aumentou em 2018 consideravelmente. A vítima desse crime, além de ser "responsabilizada e julgada" por várias pessoas, o agressor, na maioria das vezes é poupado pela sociedade. Além das consequências do machismo estrutural, existe a condenação no ponto de vista moral da sociedade, que insiste em querer controlar a vida moral e sexual da mulher. Exemplo: a manifestação da sexualidade da mulher

.....

7 Uma cooperação entre *United States Army Sexual Harassment/Assault Response and Prevention (SHARP)* e *Academy at Fort Leavenworth, ICT*, criou o *Digital Interactive Victim Intake Simulation (DIVIS)*, uma experiência prática de entrevista inicial padronizada, simulada e interativa com vítimas. Esse sistema permite aos participantes treinarem com uma vítima virtual em cenários realistas e altamente emocionais, similarmente a uma interpretação de papéis. Esse aplicativo de treinamento aproveita a tecnologia de pesquisa existente para ajudar a cultivar habilidades de comunicação interpessoal, como construção de relacionamento e escuta ativa, e tem como objetivo melhorar o ensino em sala de aula, proporcionando uma experiência envolvente e interativa com uma vítima digital. Os participantes são capazes de usar linguagem natural para conduzir uma entrevista de admissão com uma "Vítima Digital"; a sessão é gravada e uma revisão pós-ação semiautônoma fornece reprodução registrada das ações verbais e não verbais do aluno para avaliação do líder do facilitador. (Tradução livre de "a standardized, simulated and interactive victim-intake interview practice experience. This system enables Sexual Assault Response Coordinator (SARC) and Victim Advocate (VA) students to practice with a digital-based victim in realistic and highly emotional scenarios, similar to role-playing. This training application leverages existing research technology to help cultivate interpersonal communication skills, like rapport building and active listening, and sets out to improve upon classroom instruction by providing an engaging and interactive experience with a digital victim. SARC and VA trainees are able to use natural language to conduct an intake interview with a "Digital Victim"; the session is recorded, and a semi-autonomous After-Action Review provides logged playback of the student's verbal and non-verbal actions for facilitator lead assessment.") (USC, 2019, *online*).

8 O Conselho Nacional do Ministério Público instituiu o Comitê Ministerial de Defesa dos Direitos das Vítimas (CMDD-Vítimas), com a finalidade de elaborar estudos, promover discussões e articulações, apresentar propostas e projetos e realizar monitoramento de temas relacionados à organização e ao funcionamento do Ministério Público no tema Direito das Vítimas. O ato foi publicado por meio da Portaria CNMP-Presi n. 178/2022 no Diário Oficial da União. Dentre vários Ministérios Públicos do país que já criaram estruturas internas voltadas para as vítimas, destaca-se o Ministério Público do Estado de Goiás, que, por meio do Ato PGJ n. 113/2023, criou o Núcleo de Assessoramento Temático e de Fomento à Articulação na Área Criminal para promoção de Direitos e de Apoio às Vítimas (NAT Vítimas).

> gera um julgamento social "natural/ espontâneo", enquanto um homem que tem sua foto íntima divulgada, é visto apenas como uma forma de afirmação da sua masculinidade ou virilidade, afastando qualquer tipo de julgamento moral. (UNICEF, 2019, *online*).

Outra possibilidade a ser analisada pelas estruturas de TI dos Ministérios Públicos brasileiros é a criação de tecnologias para dinamizar o atendimento imediato às vítimas, pelo envio de relatórios de registros de atendimento integrado (RAI) ou Boletins de Ocorrência, elaborados pelas Polícias Militar e Civil, de vítimas de crimes cibernéticos diretamente às Promotorias de Justiça com atribuição para sua análise, e consequente diálogo com a referida vítima, a fim de estabelecer rápida conexão para obtenção de provas, análise da necessidade de pedir a preservação de conteúdo em plataformas digitais, ou ajuizar pedido cautelar para afastamento do sigilo de dados telemáticos, em conjunto ou paralelamente às atividades investigativas desenvolvidas pelas Delegacias de Polícia.

Outra ponderação de suma importância relacionada com a busca pelos resultados práticos da atuação ministerial na proteção eficaz dos direitos das vítimas de crimes cibernéticos, que foi engendrada para cessar a prática delitiva em meio cibernético e a revitimização, decorre de atuação do Núcleo de Investigações de Crime Cibernéticos (NICC – CyberGaeco), do Ministério Público de São Paulo (MPSP).

Em situação na qual a vítima teve vídeos pornográficos, montados falsamente com sua fotografia, disseminados na internet, o Promotor de Justiça Richard Gantus Encinas pleiteou judicialmente "ações disruptivas" que buscaram a cessação imediata da atividade criminosa *online*, sem prejuízo da imposição da pena ao final do processo.

Com o foco na prevenção de maiores danos, retirando a publicidade desses vídeos e fotografias, utilizou-se das técnicas de desindexação e *site blocking*. Mediante sua implementação, respectivamente, foi determinado aos principais sites de busca que procedessem à desindexação das palavras-chaves associadas e os *links* para então determinar aos Provedores de Conexão que impedissem o acesso a esses *links* e *websites* indicados.

Assim, logrou-se que a capacidade de resposta do aparelho judicial às necessidades dessa vítima fosse facilitada em conformidade ao que prevê o artigo 6º, 'd', da Declaração n. 40/34 da ONU[9], por meio de: "medidas para minimizar os transtornos causados às vítimas, proteger a sua privacidade, se necessário, e garantir a sua segurança, bem como a das suas famílias e testemunhas favoráveis, contra manobras de intimidação e represálias".

9 Declaração dos Princípios Básicos de Justiça Relativos às vítimas da Criminalidade e de Abuso de Poder.

Não seria demasiado pensar, também, no emprego de técnicas de *machine learning* para metrificar as incidências das diferentes tipologias de crimes cibernéticos, para focar nas principais vítimas e apoiar as decisões institucionais: a) implementando *chatbots* para fornecer informações iniciais e apoio emocional às vítimas, respondendo a perguntas frequentes e encaminhando casos mais complexos para profissionais humanos; b) empregando ferramentas de monitoramento de redes sociais impulsionadas por *machine learning* para identificar possíveis ameaças, bem como para coletar informações relevantes em investigações; c) construindo ferramentas automáticas de detecção de crimes cibernéticos, auxiliando na identificação precoce de atividades suspeitas e na coleta de evidências digitais; d) utilizando *machine learning* para analisar padrões de comportamento *online*, identificando comportamentos típicos de perpetradores de crimes cibernéticos e facilitando investigações.

É fundamental, para isso, entender e conferir as devidas responsabilidades às aplicações de internet, para que sejam formalizados termos de cooperação técnica, cuja finalidade primordial seja o estabelecimento de canal direto de vítimas de crimes digitais com as autoridades, facilitando os meios de acesso da população à justiça, bem assim que essas aplicações promovam alertas às autoridades sempre que houver a detecção, por meio da moderação de conteúdo[10], de eventuais crimes cibernéticos[11].

Com efeito, sabe-se que as maiores plataformas digitais, como Google, Meta, Microsoft e, também, Ifood, Uber, 99Taxis, possuem canal de acesso exclusivo a agentes da lei (*law enforcement*), que objetivam dinamizar as requisições de dados por autoridades, como promotores de Justiça, delegados, juízes, entre outros. Todavia, há demora no atendimento das demandas e burocracia, devido a fatores como escassez de mão de obra humana para análise jurídica dos pedidos, dificuldade de compreensão exata da legislação que protege os dados (LGPD), modificação de entendimentos jurisprudenciais quanto ao conceito de dados cadastrais, cujo fornecimento independe de reserva de jurisdição, e formalidades exigidas para preservação de conteúdo e acesso a dados sigilosos, o que termina por delongar injustificadamente as investigações em curso, prejudicando o direito das vítimas à sua reparação.

10 Importante ferramenta de moderação de conteúdo para proteger potenciais vítimas contra a extorsão sexual e o abuso de imagens íntimas foi recentemente anunciada pelo Instagram, em 11 de abril de 2024. Trata-se de um novo recurso de segurança para as DMs (mensagens diretas) em relação a nudes, que irão ser desfocadas em chats com pessoas abaixo dos 18 anos. "Além disso, a rede social vai adicionar novos recursos nos canais de denúncia para o encaminhamento mais ágil e eficaz aos órgãos regionais responsáveis. As iniciativas da Meta para combater a exploração sexual e o abuso de imagens íntimas são anunciadas dias após o governo brasileiro regulamentar os direitos de crianças e adolescentes em ambientes digitais — o que inclui o Instagram. Disponível em: <https://canaltech.com.br/redes-sociais/instagram-vai-borrar-nudes-enviados-para-adolescentes-285353/>.

11 Um exemplo de cooperação já realizada com finalidade de proteção de vítimas foi a estabelecida entre a Meta (dona de Facebook, Instagram e WhatsApp) e o Ministério da Justiça, por meio do projeto chamado "Amber Alerts", a fim de emitir alertas nos feeds das redes sociais, com fotos e descrição das roupas que foram vistas pela última vez, de pessoas desaparecidas, para usuários em um raio de 160km, para ajudar o público a encontrá-las. (META, 2023, *online*). Outra iniciativa louvável foi a formalização de cooperação técnica entre a Meta e o Tribunal Superior Eleitoral, por ocasião das eleições de 2022, que previu ações para disseminação de informações confiáveis, mediante a disponibilização de ferramentas, como megafone, para divulgação de mensagens aos usuários brasileiros sobre as Eleições, rótulo eleitoral, *stickers* e *chatbot*, bem assim iniciativas de alfabetização midiática e capacitação, canal de denúncias, etc. (TSE, 2022, *online*).

Por fim, é pertinente ponderar e trazer a existência de iniciativas de outros países que visam a cuidar, proteger e resguardar a vítima de crimes cibernéticos, as quais podem ser espelhadas pelas Instituições nacionais, dentre as quais destacam-se:

> a) o sítio eletrônico utilizado nos Estados Unidos, o qual foi criado e divulgado enquanto um canal oficial do Departamento de Justiça, tendo a finalidade de auxiliar as vítimas a terem informações sobre os crimes cibernéticos, a poderem buscar ajuda específica e especializada, bem como disponibilizar um canal de comunicação no qual a vítima pode realizar sua denúncia[12];
>
> b) outra iniciativa foi identificada na Irlanda, onde o Departamento de Justiça daquela localidade disponibilizou um sítio eletrônico com a mesma finalidade da acima indicada, contudo, além de disponibilizar um disque-denúncia, eles também disponibilizam a possibilidade de a vítima enviar sua denúncia por e-mail ou por mensagens de texto (SMS)[13];
>
> c) outro exemplo, bastante similar aos demais, por meio do *Action Fraud*, foi realizado pela Polícia de Londres em conjunto com o Escritório Nacional de Inteligência em Fraudes (*National Fraud Intelligence Bureau*-NFIB) do Reino Unido, com o objetivo de estabelecer canal telefônico e *online* para receber denúncias de fraude e cibercrimes, oferecer ajuda e aconselhamentos às vítimas[14].

Contudo, não se tem notícia no cenário brasileiro sobre a existência de similar forma de atuação rápida e ágil, como um sítio eletrônico composto por um disque-denúncia específico, com informações sobre os crimes cibernéticos e sobre como a vítima pode buscar sua proteção. Assim, referidas iniciativas podem ser tomadas enquanto referência para a melhoria das práticas realizadas no cenário brasileiro, inclusive pelo próprio Ministério Público na execução, proposição e desenvolvimento de políticas públicas, pensando cada vez mais no cuidado para com a condição psicológica da vítima de crimes cibernéticos.

Com efeito, iniciativas desse jaez devem ser pensadas não apenas enquanto meio de trazer proteção para as vítimas, mas também enquanto um mecanismo capaz de concretizar a luta e a efetiva prevenção contra as práticas de cibercrimes, principalmente se as autoridades que ficarem responsáveis por receber as denúncias dos sítios eletrônicos agirem de forma rápida e enérgica.

Principalmente no tocante à proteção de crianças e adolescente, ou seja, na luta contra a pornografia infantil, essa iniciativa vai no mesmo direcionamento do artigo 21 da Resolução n. 245, de 5 de abril de 2024, que dispõe sobre os direitos das crianças e adolescentes em ambiente digital e

.....

12 O sítio eletrônico dos Estados Unidos para o auxílio das vítimas pode ser acessado pelo seguinte link: <https://ovc.ojp.gov/taxonomy/term/cyber-crime>.

13 O sítio eletrônico da Irlanda para o auxílio das vítimas pode ser acessado pelo seguinte link: <https://www.crimevictimshelpline.ie/after-a-crime/cyber-crime>.

14 Disponível em: <https://www.actionfraud.police.uk/what-is-action-fraud, acesso em 5/5/24>. Link acessível mediante uso de VPN conectada ao Reino Unido.

determina que as empresas que venham a disponibilizar ambientes e serviços digitais têm a obrigação de

> disponibilizar e divulgar amplamente canais de fácil acesso e em linguagem simples, acessível e de fácil compreensão para crianças, para escuta, diálogo e recebimento de denúncias de conteúdos nocivos ou ilegais, sem prejuízo dos direitos de revisão das decisões e acesso à informação sobre os procedimentos de moderação.

Consequentemente, a atuação do Ministério Público, ao propor essa iniciativa enquanto política pública voltada à proteção e ao cuidado com as vítimas, não exclui a responsabilidade das empresas provedoras de criarem um canal de comunicação, em atenção ao dispositivo acima. Importante ainda que, logo após receber qualquer denúncia, as autoridades sejam imediatamente acionadas para tomarem as medidas cabíveis, em cumprimento aos demais artigos da resolução acima indicada.

Igualmente, as empresas citadas da Resolução n. 25/2024 passam a ter a obrigação de publicar relatórios anuais, informando sobre as medidas adotadas, sobre a transparência dos seus sistemas, bem como da destinação dos dados privados que estão sendo recebidos pelos usuários.

Por sua vez, mostra-se de importância ímpar a atuação do Ministério Público para que as disposições constantes na Resolução n. 25/2024 venham a ser efetivamente cumpridas e realizadas, uma vez que o artigo 30 traz as condições da sua participação enquanto um dos órgãos responsáveis pelo tratamento de denúncias de violação dos direitos de crianças e adolescentes no ambiente digital pelas empresas provedoras. Além disso, o órgão deve adotar, enquanto prática comum, a fiscalização dessas empresas provedoras, visando agir de forma preventiva e com foco na proteção e no adequado resguardo para as vítimas.

4. CONSIDERAÇÕES FINAIS

Considerando os dados apresentados, é possível entender o crescimento e a importância em buscar uma melhor percepção e abordagem dos aspectos criminais para as ações praticadas mediante o uso das novas tecnologias. É uma certeza que o avanço e a melhoria das tecnologias não vão parar, ao mesmo tempo em que seu caráter transfronteiriço possibilita a disseminação de informações de forma automática e incontrolável.

Por essa razão, é preciso uma atuação mais concreta de todos os países na busca pela viabilidade de mecanismos e dispositivos que possam salvaguardar os dados e a privacidade das pessoas que fazem uso da internet, visando proteger e evitar os danos materiais e morais que os crimes cibernéticos podem causar para as vítimas.

Nesse sentido, é preciso uma mudança drástica nas atuações dos órgãos de investigação e nos auxiliares, como o Ministério Público, visando promover mecanismos específicos que venham não apenas para solucionar o delito, mas com um olhar e uma condição mais humana, pensando a situação da vítima, a qual não quer ser incluída em um contínuo processo de revitimização.

O advento dos cibercrimes demanda essa mudança na percepção da vítima e no modo como ela vai obter uma resposta ágil e eficaz, principalmente dos órgãos investigadores e dos primeiros a tomarem conhecimento da prática do delito.

Por sua vez, é importante que o Ministério Publico permaneça concentrado no incremento de suas atuações e suas políticas públicas, visando proteger e resguardar a vítima, além de ser necessária a busca pela melhoria dos mecanismos de proteção, principalmente centrados na agilidade e na minimização dos danos para a imagem da vítima.

Assim, é preciso conferir as devidas responsabilidades às aplicações de internet, para que sejam formalizados termos de cooperação técnica, cuja finalidade primordial seja o estabelecimento de canal direto de vítimas de crimes digitais com as autoridades, facilitando os meios de acesso da população à justiça, principalmente mediante a redução do excesso de burocracia para lidar e agir com destreza perante a luta na repressão aos crimes cibernéticos.

REFERÊNCIAS

BARRETO, Alesandro Gonçalves; SILVA, Natália Siqueira da. **É bom demais para ser verdade?** Prefácio Ricardo Magno Teixeira Fonseca. Apresentação Laerte Peotta de Mello. Apoio Observatório dos Crimes Cibernéticos. Ebook. São Paulo, 2022. Disponível em: <https://www.seguranca.galafassi.com.br/cartilha_policia.pdf>. Acesso em: 14 abr. 2024.

BRASIL. **Resolução n. 245, de 5 de abril de 2024**. Dispõe sobre os direitos das crianças e adolescentes em ambiente digital. Disponível em: <https://in.gov.br/en/web/dou/-/resolucao-n-245-de-5-de-abril-de-2024-552695799>. Acesso em: 14 abr. 2024.

BORWELL, Jildau; JANSEN, Jurjen; STOL, Wouter. **Comparing the victimization impact of cybercrime and traditional crime: literature review and future research directions.** vol.3, n. 3, p.85-110. Journal of digital social research, 2021.

CRUZ, Elaine Patrícia. **Denúncias de crimes com discurso de ódio na Internet crescem em 2022.** AgênciaBrasil, 2023. Disponível em: <https://agenciabrasil.ebc.com.br/direitos-humanos/noticia/2023-02/denuncias-de-crimes-na-Internet-com-discurso-de-odio-crescem-em-2022>. Acesso em: 30 jan. 2024.

DEMARCO, J.; CHEEVERS, C.; DAVIDSON, J.; BOGAERTS, S.; PACE, U.; AIKEN, M.P.; CARETTI, V.; SCHIMMENTI, A.; BIFULCO, A. **Digital dangers and cyber-victimisation: a study of European adolescent online risky behaviour for sexual exploitation.** Clinical Neuropsychiatry. 14 (1). 2017, pp. 104-112.

HADA, Brenda; REIS, Elisa Meirelles. **UNICEF alerta: meninas que têm imagens íntimas vazadas na internet não contam com redes de proteção e apoio. Elas sofrem sozinhas ou só falam com as amigas.** UNICEF, 2019. Disponível em: <https://www.unicef.org/brazil/comunicados-de-imprensa/unicef-alerta-meninas-que-tem-imagens-intimas-vazadas-na-internet-nao?fbclid=IwAR3rjUXQrPgJx-jh9SG-1qAA1XECq0753nlfevPp1ZxTgSDNgShy205mz7E>. Acesso em: 17 maio 2024.

HAWDON, J. **Cybercrime: Victimization, Perpetration, and Techniques.** Am J Crim Just 46, 837–842 (2021). Disponível em: <https://doi.org/10.1007/s12103-021-09652-7>. Acesso em: 30 jan. 2024.

LEUKFELDT, E. R., NOTTÉ, R. J.; MALSCH, M. (2018**). Slachtofferschap van online criminaliteit**. Een onderzoek naar behoeften, gevolgen en verantwoordlijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit. Den Haag: Ministerie van Justitie en Veiligheid. Disponível em: <https://victimologie.nl/netwerkleden/rutger-leukfeldt/#:~:text=(2018).,Ministerie%20van%20Justitie%20en%20Veiligheid>. Acesso em: 17 maio 2024.

MARTELLOZZO, Elena; JANE, Emma A. **Cybercrime and its Victims (Routledge Studies in Crime and Society)**. Nova York, Routledge, 2017.

META. **Parceria entre Ministério da Justiça e Meta ajudará a localizar crianças desaparecidas no Brasil**. META, 2023. Disponível em: <https://about.fb.com/br/news/2023/08/parceria-entre-ministerio-da-justica-e-meta-ajudara-a-localizar-criancas-desaparecidas-no-brasil/>. Acesso em: 30 jan. 2024.

MINISTÉRIO PÚBLICO DE MINAS GERAIS – MPMG. **Alerta MPMG: conheça e evite o golpe do amor!** Minas Gerais, 2024, *online*. Disponível em: <https://www.instagram.com/p/C477qvIucRQ/?igsh=azdzdjBzeDlvNGZh&img_index=2>. Acesso em: 13 abr. 2024.

MORGAN, Steve. **O Crime Cibernético Custará ao Mundo US$ 10,5 Trilhões Anualmente até 2025.** Cybercrime Magazine, 2020, *online*. Disponível em: <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>. Acesso em: 22 jan. 2024.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **ONU diz que usuários da Internet têm dados desprotegidos em um terço dos países.** ONU, 2020. Disponível em: <https://news.un.org/pt/story/2020/04/1712072>. Acesso em: 30 jan. 2024.

QUAYLE, E., AIKEN, M. P., CARTWRIGHT, A. **Understanding the dynamics of online victimisation and victim narratives as an enabler for prevention.** *In:* International Collaboration: An Enabler for Preven-

tion. Symposium conducted at the meeting of the Virtual Global Taskforce, Abu Dhabi, 2012.

SAFERNET. Central Nacional de Denúncias. **Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos**. *Online*, 2022. Disponível em: <https://indicadores.safernet.org.br/index.html>. Acesso em: 13 abr. 2024.

SYDOW, Spencer Toth. **Curso de Direito Penal Informático**. 4ª ed. São Paulo, Editora Juspodivm, 2022.

TJRJ – Tribunal de Justiça do Rio de Janeiro. **Violência cibernética contra as mulheres**. Cartilha. Rio de Janeiro, 2024. Disponível em: <https://portaltj.tjrj.jus.br/documents/d/guest/cartilha_violencia_cibernetica>. Acesso em: 12 abr. 2024

TSE - TRIBUNAL SUPERIOR ELEITORAL. **Memorando de Entendimento-Tse n. 03/2022**. TSE, 2022. Disponível em: <https://www.justicaeleitoral.jus.br/desinformacao/arquivos/termos-de-cooperacao-plataformas-digitais/facebook-e-instagram.pdf>. Acesso em: 30 jan. 2024.

USC - Institute for Creative Technologies. **Digital Interactive Victim Intake Simulator (DIVIS).** Project Leaders: David Nelson, David Cobbins, and Alesia Gainer.USC, 2019. Disponível em: <https://ict.usc.edu/research/projects/digital-interactive-victim-intake-simulator-divis/>. Acesso em: 21 jan. 2024.

WENDT, Emerson. **Crimes cibernéticos: ameaças e procedimentos de investigação.** Rio de Janeiro: Brasport, 2021.