UNIVERSIDADE DE BRASÍLIA
FACULDADE DE DIREITO

LEANDRO DA SILVA VALLIM JOBIM

DESAFIOS DO DIREITO PENAL NA INVESTIGAÇÃO E COMBATE DO CYBERBULLYING

Brasília / DF
2024

LEANDRO DA SILVA VALLIM JOBIM

DESAFIOS DO DIREITO PENAL NA INVESTIGAÇÃO E COMBATE DO CYBERBULLYING

Monografia apresentada à Faculdade de direito da Universidade de Brasília como requisito parcial para obtenção do grau de bacharel em Direito.

Orientadora**:** Profa. Dra. Fernanda de Carvalho Lage

Brasília / DF
2024

AGRADECIMENTOS

A conclusão deste trabalho só foi possível graças ao apoio e colaboração de muitas pessoas, às quais gostaria de expressar minha mais sincera gratidão.

Em primeiro lugar, agradeço à minha orientadora, Profa. Dra. Fernanda de Carvalho Lage, por sua orientação, paciência e dedicação. Sua expertise e orientação foram fundamentais para o desenvolvimento deste trabalho.

À minha esposa, Vanéli Vallim, expresso meu profundo agradecimento pelo amor, apoio e compreensão ao longo desta jornada. Sua presença constante e suas palavras de incentivo foram essenciais para que eu pudesse superar os desafios e concluir esta etapa.

Agradeço também aos meus familiares e amigos, que sempre estiveram ao meu lado, oferecendo apoio emocional e motivação nos momentos mais difíceis.

Por fim, agradeço a todos os professores do curso de Direito da UNB, cujos ensinamentos foram imprescindíveis para a construção deste trabalho, e a todos aqueles que, de alguma forma, contribuíram para a realização desta monografia.

RESUMO

A internet, ao permitir o intercâmbio remoto de informações, revolucionou as formas de comunicação e o acesso ao conhecimento, especialmente no Brasil a partir dos anos 90. Contudo, esse avanço também facilitou práticas ilícitas como o cyberbullying. Este fenômeno, uma forma de violência digital, estende o bullying tradicional para o ambiente virtual, onde a hostilidade pode ser amplificada pela viralização e permanência online, expondo vítimas, principalmente em ambientes escolares, a abusos contínuos. As consequências são graves, afetando profundamente a saúde mental das vítimas, podendo levar a depressão e suicídio. Em resposta, a legislação brasileira evoluiu com a Lei Nº 14.811/2024, que tipifica o bullying e o cyberbullying, impondo penalidades mais severas para abusos online, reconhecendo sua maior danosidade. Contudo, o direito penal ainda enfrenta desafios significativos na investigação desses crimes, como por exemplo a defasagem tecnológica dos meios de investigação dos órgãos de segurança pública. Neste contexto, a investigação e combate do cyberbullying se apresenta como questão de fundamental relevância jurídica e social, ante sua necessidade para a efetividade da coibição desta conduta almejada pelo legislador ao tipificá-la por meio da Lei Nº 14.811/2024. Assim, foi conduzida pesquisa de revisão bibliográfica, na qual doutrina, legislação e jurisprudência foram utilizadas objetivando a análise da efetividade do combate à prática do cyberbullying em face da atual disciplina jurídica para sua investigação e repressão.

Palavras-chave: Crimes Cibernéticos. Cyberbullying. Intimidação Sistemática. Meios de Investigação. Prova Digital.

ABSTRACT

The internet, by allowing the remote exchange of information, revolutionized forms of communication and access to knowledge, especially in Brazil from the 1990s onwards. However, this advance also facilitated illicit practices such as cyberbullying. This phenomenon, a form of digital violence, extends traditional bullying to the virtual environment, where hostility can be amplified by going viral and remaining online, exposing victims, especially in school environments, to continuous abuse. The consequences are serious, deeply affecting the mental health of victims, which can lead to depression and suicide. In response, Brazilian legislation evolved with Law No. 14,811/2024, which typifies bullying and cyberbullying, imposing more severe penalties for online abuse, recognizing its greater harm. However, criminal law still faces significant challenges in investigating these crimes, such as the technological lag in the means of investigation by public security bodies. In this context, the investigation and combat of cyberbullying presents itself as an issue of fundamental legal and social relevance, given its need for the effectiveness of curbing this conduct sought by the legislator when typifying it through Law No. 14,811/2024. Thus, bibliographical review research was conducted, in which doctrine, legislation and jurisprudence were used to analyze the effectiveness of combating the practice of cyberbullying in the face of the current legal discipline for its investigation and repression.

Keywords: Cyber Crimes. Cyberbullying. Systematic Intimidation. Means of Investigation. Digital Proof.

SUMÁRIO

INTRODUÇÃO

O advento da internet permitiu a troca de informações remotamente entre indivíduos, levando a um maior compartilhamento de conhecimento e à novas formas de comunicação, tendo sua utilização pela população em geral crescido exponencialmente no Brasil a partir da década de 1990. Contudo, as novas possibilidades de interação advindas desta tecnologia também permitiram sua utilização para fins escusos e como meio para o cometimento de ilícitos.

Nesse contexto, o cyberbullying emerge como um problema social crítico, caracterizado pelo uso da internet e de dispositivos eletrônicos para hostilizar, ameaçar ou humilhar indivíduos, especialmente entre adolescentes e jovens. Desta maneira, o cyberbullying se apresenta como forma de violência digital que estende os limites tradicionais do bullying para o vasto e acessível mundo virtual, representa um desafio significativo para o direito penal contemporâneo.

Ocorrendo predominantemente em ambientes escolares, a prática do bullying, compreendida como a intimidação sistemática e persistente da vítima por meio de agressões físicas, verbais e psicológicas, é um problema amplamente reconhecido como forma de agressão que acarreta impactos profundos na saúde mental e emocional das vítimas, levando a consequências graves como depressão, ansiedade e, em casos extremos, suicídio.

Contudo, este fenômeno ganha contornos ainda mais preocupantes ao considerarmos a capacidade de viralização e a permanência de conteúdos na internet, criando um ambiente em que vítimas de cyberbullying podem ser expostas a um ciclo contínuo de abuso sem as barreiras temporais e físicas que existem no bullying tradicional.

Por conseguinte, a tipificação do bullying pela Lei Nº 14.811/2024 representa um avanço significativo no combate a essa prática nociva. A nova legislação inclui o artigo 146-A no Código Penal Brasileiro, estabelecendo como crime a intimidação sistemática, seja ela física ou psicológica, praticada de forma repetitiva e intencional contra uma ou mais pessoas, sem motivação evidente. A lei prevê penas específicas para o bullying tradicional e penas mais severas para o cyberbullying, reconhecendo a maior gravidade e impacto das agressões realizadas no ambiente virtual.

Contudo, é inegável que a investigação e repressão dos crimes cometidos no ambiente virtual se apresenta como um desafio para o direito penal, sendo que muitas

vezes os órgãos de segurança pública responsáveis por sua investigação não estão preparados para lidar com esses tipos de crime dada a defasagem tecnológica entre os meios de investigação disponibilizados aos mesmos e a tecnologia utilizada pelos criminosos.

A investigação e combate do cyberbullying se apresenta como questão de fundamental relevância jurídica e social, ante sua necessidade para a efetividade da coibição desta conduta almejada pelo legislador ao tipificá-la por meio da Lei Nº 14.811/2024. Assim, foi conduzida pesquisa de revisão bibliográfica, na qual doutrina, legislação e jurisprudência foram utilizadas objetivando a análise da efetividade do combate à prática do cyberbullying em face da atual disciplina jurídica para sua investigação e repressão.

Desta maneira, no primeiro capítulo se buscou compreender como as alterações no campo do direito penal brasileiro suscitadas pelas novas tecnologias informáticas e de comunicação com o advento da internet. No segundo capítulo se procurou compreender o fenômeno do bullying e do cyberbullying e sua tipificação como o crime de intimidação sistemática pela Lei Nº 14.811/2024 para assim, no terceiro capítulo se proceder a análise dos desafios enfrentados pelo direito penal na investigação e combate à prática do cyberbullying.

1. O DIREITO PENAL E AS NOVAS REALIDADES TECNOLÓGICAS DA INTERNET

1.1 BREVE HISTÓRICO DA INTERNET

A internet, ou seja, o Sistema global de redes de computadores interligadas que utilizam um conjunto próprio de protocolos com o propósito de servir progressivamente usuários no mundo inteiro; permitiu a troca de informações remotamente entre indivíduos, levando a um maior compartilhamento de conhecimento e à novas formas de comunicação.

Neste contexto, sendo a conexão à rede mundial de computadores diretamente ligada ao manuseio de dispositivos informáticos, o computador se apresenta como ferramenta indissociável da gênese da internet. Desta maneira, ainda na década de 1940, o desenvolveu-se primeiro computador digital, o qual tinha finalidade de automatizar o cálculo de tabelas balísticas.

Sobre a questão, conforme bem aponta PINHEIRO (2021, p. 31) “ao final dos anos 1950, a Internet não passava de um projeto embrionário, o termo “globalização” não havia sido cunhado e a transmissão de dados por fibra óptica não existia. Informação era um item caro, pouco acessível e centralizado”.

Neste contexto, “os primórdios da Internet remetem à reação do governo norte-americano ao Projeto Sputnik da antiga União das Repúblicas Socialistas Soviéticas (URSS), capitaneadas pela Rússia, durante a guerra fria, em 1957” (ABREU, 2009 p.1-2). Assim, em 1962, através da iniciativa de Paul Baran, a internet teve sua origem a partir das pesquisas de tecnologia militar conduzidas pelos Estados Unidos como resposta ao lançamento do primeiro satélite espacial pela União Soviética, objetivando o estabelecimento de uma rede de telecomunicações para monitorar possíveis ataques nucleares soviéticos, como explica ABREU (2009, p.2):

> O nascimento da Internet está diretamente relacionado ao trabalho de peritos militares norte-americanos que desenvolveram a ARPANET, rede da Agência de Investigação de Projetos Avançados dos Estados Unidos, durante a disputa do poder mundial com a URSS. [...]
> O apoio financeiro do governo norte americano através da pesquisa promovida pelo Departamento de Defesa dos Estados Unidos por meio da ARPA - Administração dos Projetos de Pesquisa Avançada, já em 1968, foi o impulso para a implantação do sistema de informação em rede. Iniciada com objetivos militares, propondo uma sobrevivência aos elementos partícipes por não estarem conectados de modo

> hierárquico, característica marcante daquele setor, a disposição em rede permitia a não ameaça ao cabeça do programa, caso fosse atacada. Era crucial que a arquitetura do sistema fosse diferente daquela apresentada pela rede de telefonia norte-americana.

Desta maneira, com a ARPANET buscou-se delinear uma Rede de comunicações “totalmente independente que fosse invulnerável a qualquer tentativa de destruição ou controle por parte de qualquer entidade ou potência” consoante elucidam TURNER & MUÑOZ (1999, p. 29).

Desenhada de um modo que as comunicações militares pudessem ser realizadas por uma rede que não fosse exclusivamente dependente de um núcleo central. A ARPANET, contudo, começou de forma tímida, como explica LINS (2013, p. 16), “em 1969, a primeira ligação dessa rede foi efetuada, entre a Universidade de Stanford e a UCLA. Após um ano, apenas quatro computadores estavam ligados. Mas em 1971 a rede já havia crescido para uma dúzia de nodos”.

O desenvolvimento da ARPANET foi um marco para a rede mundial de computadores, especialmente porque ela permitiu que se consolidasse a ideia, com o passar dos anos, da importância de se criar e desenvolver uma rede que pudesse permitir a integração entre computadores (LINS, 2013).

Importante mencionar que, até a consolidação da *internet* ocorreu uma proliferação de redes de comunicação, as quais possuíam desígnios específicos, sendo geralmente utilizadas para a ligação de computadores de grande porte. Esse fenômeno foi imprescindível para a transformação da computação, especialmente porque algumas dessas redes, tais como SITA e IATA existem e são utilizadas na atualidade (LINS, 2013).

Por sua vez, a partir da década de 1990, a rede mundial de computadores atravessou um processo de expansão nunca visto. Conforme pontua PINHEIRO (2021, p. 40), “seu rápido crescimento deve-se a vários de seus recursos e facilidades de acesso e transmissão, que vão desde o correio eletrônico (e-mail) até o acesso a banco de dados e informações disponíveis na World Wide Web (WWW) ”.

Um relatório apresentado em janeiro de 2021, pela *We Are Social e Hootsuite*, mostrou que há mais de 4.60 bilhões de usuários dos meios digitais; esse mesmo relatório mencionou que existem mais de 5,20 bilhões de pessoas que utilizam aparelhos móveis. Ou seja, mais da metade da população do planeta está ligada à rede de internet. (ISTO É DINHEIRO, 2021).

É inquestionável que as transformações trazidas pela internet ao redor do mundo, alteraram e alteram as formas de comportamento das sociedades, assim, a ideia de um planeta desconectado foi afastada da mente das pessoas, justamente pela presença no sentido mais amplo do cotidiano da coletividade.

No que se refere ao contexto brasileiro, as primeiras experiências relativas ao uso da internet no país datam de 1988, ocasião em que a utilização da rede mundial de computadores passou a ser difundida no território nacional (CARVALHO, 2000). Não obstante a isso, a utilização da rede mundial de computadores com fins à transmissão de informações já aguçava “o interesse do Ministério das Comunicações (Minicom) desde 1975, quando baixou o decreto nº 301 que incumbia a Empresa Brasileira de Telecomunicações (Embratel) de instalar e explorar a transmissão eletrônica de dados” (CARVALHO, 2000 p. 78).

No Brasil, o uso da internet para fins comerciais começou apenas em 1995, visto que até esse momento a rede mundial de computadores possuía finalidade de atender a comunidade acadêmica (LINS, 2013). Conforme estabelecido por uma Nota Conjunta divulgada em 15 de maio desse ano pelos Ministérios das Comunicações e da Ciência e Tecnologia. Essa nota regulamentou e ressaltou a importância estratégica de proporcionar acesso à internet para toda a sociedade, visando à inserção do país na Era da Informação (BRASIL, 1995).

Diante desse panorama, observa-se que o acesso à internet pela sociedade brasileira iniciou-se somente 33 anos após sua criação global. No entanto, foi somente com a promulgação da Lei nº 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet, que estabeleceu princípios, garantias, direitos e deveres para o uso da internet no Brasil.

1.2 O ACESSO À INTERNET COMO DIREITO

O advento da internet permitiu a troca de informações remotamente entre indivíduos, levando a um maior compartilhamento de conhecimento e à novas formas de comunicação, de maneira que, como expõe BACCIOTTI (2014, p. 163), “não é possível, hoje, reconhecê-la apenas como tecnologia da informação que se utiliza de uma rede interconectada de computadores para a transferência de dados”.

Neste sentido, PINHEIRO (2021, p. 43) aduz que a expansão da tecnologia nos meios de comunicação sempre teve a finalidade de se desenvolver em uma espécie

de aldeia global, permitindo, assim, “que todas as pessoas do mundo pudessem ter acesso a um fato de modo simultâneo”.

Contudo, imperioso observar que a possibilidade oferecida pela Internet de qualquer pessoa ser receptor e transmissor no processo de comunicação abriu portas para novos modelos de transmissão de informação, onde o discurso está dando lugar ao diálogo; permite se compreender a internet como “verdadeira ferramenta habilitadora do potencial humano” (BACCIOTTI, 2014, p. 163).

Diante dessa sistemática, novas reinvindicações relativas à internet se incorporaram à agenda política da comunidade tais como “a luta pelo reconhecimento de um direito fundamental à internet, obrigando o estado a desenvolver políticas públicas capazes de permitir a inclusão digital de setores economicamente desfavorecidos” (MARMELSTEIN, 2008, p. 54)

Assim, em que pese o Brasil não ter sido um dos pioneiros na adoção de textos normativos voltados para a regulamentação do uso da internet, em 2014 foi implementado ao ordenamento jurídico pátrio o denominado Marco Civil da Internet (Lei Nº 12.965, de 23 de abril de 2014) com o intuito de consolidar os deveres e direitos para que o uso e desenvolvimento da internet no brasil pudesse se dar de forma livre e aberta, onde os usuários teriam a chance de se desenvolver alicerçados em uma base de segurança ao navegar nesses ambientes digitais, definindo assim normas onde os poderes públicos pudessem agir indo de encontro às possíveis violações e preservando a segurança dos internautas, assim como instituindo regras para a proteção de suas informações.

Sobre a questão, importante apontar que embora aprovado somente em 2014, o referido diploma encontrava-se em tramitação desde 2007; sendo sua aprovação influenciada, em parte, pela divulgação de diversos crimes internacionais em 2014, como notícias falsas dos Estados Unidos, sem autorização da agência norte-americana de segurança nacional (GARCIA, 2016).

Destaca-se que o Marco Civil da Internet foi a primeira iniciativa do Poder Executivo totalmente dedicada à especificação e aos eventos ocorridos na rede, demonstrando que a internet não é um espaço vazio, mas um lugar onde haveria também a presença do Governo, como bem lecionam SOUZA & LEMOS 2 (2016, p.1).

> o Marco Civil da Internet apresenta um novo cenário no qual o conceito de “Internet livre” está ligado não à ausência de leis, mas sim à existência de leis que possam garantir e preservar as liberdades que

> são usufruídas por todos justamente por causa da tecnologia e mais especificamente pelo desenvolvimento da Internet.
> Foi com essa motivação que o Marco Civil foi concebido: como uma lei que pudesse preservar as bases para a promoção das liberdades e dos direitos na Internet no Brasil. Distanciando-se assim de uma regulação repressiva da rede, o Brasil ofereceu um dos mais simbólicos exemplos que anima os debates globais sobre uma regulação da rede que tenha os direitos humanos como o seu fio condutor e que mantém o caráter principiológico para evitar uma caducidade precoce de seus dispositivos.

Por sua vez, com o advento do Marco Civil da Internet, o acesso à internet foi expressamente positivado como direito de todos, sendo sua promoção um dos objetivos norteadores da atividade legislativa relativa ao uso da internet no Brasil [1].

No mesmo contexto, a Lei Nº 12.965/2014, em seu art. 7º, também preceitua o acesso à internet como “essencial ao exercício da cidadania” (BRASIL, 2014). Por conseguinte, com o reconhecimento do acesso à internet como direito pelo Marco Civil da Internet, instituiu-se a necessidade da adoção de políticas públicas voltadas à universalização dessa ferramenta, visto que “a universalização dos serviços de informação e comunicação é condição fundamental, ainda que não exclusiva, para a inserção dos indivíduos como cidadãos, para se construir uma sociedade da informação para todos” (CASTELLS, 1999, p. 51).

No mais, urge destacar a Proposta de Emenda à Constituição Nº 47/2021 que objetiva o reconhecimento da inclusão digital como direito fundamental, com sua inclusão no rol do art. 5º da Constituição Federal (BRASIL, 2021)[2].

---

[1] 1 Art. 4º A disciplina do uso da internet no Brasil tem por objetivo a promoção:

I - do direito de acesso à internet a todos;
II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;
III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e
IV - da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.
(BRASIL, 2014)

[2] O avanço tecnológico das últimas décadas fez surgir a denominada sociedade da informação que se caracteriza pelo uso intensivo de produtos e serviços baseados nas tecnologias da informação e comunicação, com destaque para o extraordinário crescimento da internet.
As transformações econômicas e sociais promovidas por essas tecnologias afetaram também os direitos humanos que devem ser repensados e adaptados a essa nova realidade. Em um mundo cada vez mais conectado, o exercício da cidadania e a concretização de direitos sociais como educação, saúde e trabalho dependem da inclusão digital.
O acesso à internet, embora essencial, é apenas um dos instrumentos para a inclusão digital. É certo que o acesso à internet viabiliza a comunicação entre as pessoas, a obtenção de informação e a utilização de serviços de interesse público. Mas estar incluído digitalmente significa possuir capacidade

A proposta em tela, recebeu parecer favorável da Comissão de Constituição e Justiça e de Cidadania (CCJC) em 20 de junho de 2023. Neste contexto, a positivação da inclusão digital como direito fundamental, como proposto pela PEC Nº 47/2021, implica na obrigatoriedade da criação de mecanismos para a ampliação do acesso à internet pelo Poder Público, de maneira a efetivar tal direito fundamental.

1.3 CIBERESPAÇO, METAVERSO E NOVOS BENS JURÍDICOS

O ciberespaço, compreendido como o ambiente virtual no qual as pessoas utilizam a internet como uma ferramenta para se comunicar e conectar umas com as outras, representa o novo cenário no qual a sociedade se encontra interconectada e não é necessária a presença física para a comunicação entre os usuários (KUNRATH, 2014).

Por sua vez, originado em 1992, na obra de ficção científica *Snow Crash*, do escritor norte americano Neal Stephenson; o termo “metaverso” constituiria uma evolução dos ambientes virtuais *on-line* tradicionais, se referindo a um ambiente virtual expansivo e altamente interconectado, onde as pessoas podem interagir, socializar e participar de uma variedade de atividades digitais de forma imersiva por meio de várias plataformas e experiências que se conectam para criar um universo digital compartilhado (GODOY, 2022).

Desta maneira, enquanto no ambiente virtual *on-line* tradicional, o ciberespaço, os usuários se engajam principalmente em atividades restritas a uma única plataforma, como jogar um jogo específico ou participar de atividades limitadas; o *metaverso* transcende essas limitações, conectando diferentes plataformas e ambientes virtuais de maneira fluida, permitindo que os usuários migrem entre diferentes experiências sem barreiras rígidas (QATTAN, 2022).

Uma das características distintivas do *metaverso* é sua economia virtual e social mais complexa. Enquanto os ambientes virtuais online podem ter economias virtuais limitadas, o *metaverso* pode apresentar sistemas econômicos virtuais

---

de análise dos conteúdos disponíveis na rede para a formação da própria opinião, de maneira crítica, o que é essencial para o exercício da cidadania.
Nesse sentido, a inclusão digital se configura num direito fundamental a ser assegurado a todos. O Estado, por sua vez, deve agir para assegurar a todos uma efetiva inclusão digital que promova educação e cidadania, a ser alcançada com a ampliação do acesso à internet em todo território nacional.
(BRASIL, 2021)

abrangentes, onde os usuários podem comprar, vender e comercializar itens virtuais, bem como interagir socialmente de várias maneiras.

Todavia, conforme ressalta GARCÍA (2021, p. 19), deve-se ter em mente que no metaverso as interações “ocorrem por intermédio de equipamentos tecnológicos, a exemplo dos óculos de RV. Mas isso não impede que haja repercussão no mundo físico para os representantes legais dos personagens fictícios”. Desta maneira, na interação com o mundo real, o *metaverso* não constituiria um “outro” lugar, pelo contrário, representaria um modelo de realidade aumentada, um ambiente físico repleto de informações onde a *web 3D* é apenas um aplicativo, executado em circunstâncias especiais.

Por óbvio que tais interações no ambiente virtual irão repercutir no mundo real e o Direito será chamado a agir antes aos novos problemas que surgirão sabendo-se que o *metaverso* não se limita apenas ao entretenimento. Todavia, enquanto não juridicamente sujeito à disciplina específica, todas as interações em ambientes *on-line* devem ser compreendidas conforme as normas de direito tradicionais, não se excepcionando da aplicabilidade legal violações de direitos e deveres em razão de sua infração ser cometida virtualmente.

Neste contexto, o ambiente virtual, seja considerado enquanto ciberespaço ou como metaverso, suscitou a criação de novos bens jurídicos específicos a este ambiente, os denominados bens digitais. A saber: diversos estudiosos utilizam a terminologia “bem digital” para se referir tanto àqueles com valor econômico, quanto aqueles puramente informacionais, conforme aponta ALMEIDA (2019, p. 36)[3]

Por sua vez, bens digitais com valor estritamente econômico denominam-se criptoativos, ou seja, se consubstanciando na representação no ambiente virtual de um valor por meio de unidade própria, que não constitui moeda de curso legal, e que “cujo preço pode ser expresso em moeda soberana local ou estrangeira, transacionado eletronicamente com a utilização de criptografia e de tecnologias de registros distribuídos” conforme define a Instrução Normativa RFB Nº 1888, de 03 de maio de 2019 da Receita Federal.

[3] Segundo SHERRY (2012, p. 194) os bens digitais podem ser definidos como qualquer coisa possuída em meio digital. Podem ser categorizadas em dois grandes grupos:
1. coisas que podem ser armazenadas localmente em um dispositivo eletrônico de uma pessoa;
2. Ou coisas que são armazenadas em outros locais (nuvem), acessados através de contrato com o proprietário do dispositivo.

1.4 CRIMES CIBERNÉTICOS

Com o rápido avanço da tecnologia e a crescente conectividade global, os crimes cometidos através do uso de tecnologia da informação e da internet como meio ou alvo se tornaram uma preocupação significativa para governos, empresas e indivíduos em todo o mundo.

Todavia, o cometimento de ilícitos envolvendo dispositivos informáticos não é fenômeno recente, remontando à década de 1960, ou seja, mesmo anteriormente à utilização da internet. Sobre os primeiros crimes informáticos expõe JESUS & MILAGRE (2016, p. 19-20):

> [...] No mundo, a literatura internacional indica que os crimes informáticos tiveram seu início na década de 1960, onde identificamos as primeiras referências sobre o tema, em sua maioria delitos de alteração, cópia e sabotagem de sistemas computacionais. [...] [4]

Nesse contexto, JESUS & MILAGRE (2016) ressaltam que o crime informático é um fenômeno jurídico resultante das transformações tecnológicas ocorridas na sociedade, as quais refletem diretamente no âmbito dos estudos do direito penal. Desta maneira, os delitos informáticos passaram a ser relevantes para as ciências criminais quando começaram a trazer consequências jurídicas proeminentes para diversos bens tutelados por essa área do Direito.

Importante destacar que a denominação utilizada para se referir aos crimes que envolvem o uso da tecnologia informática não é consenso, com a adoção de diversas denominações para se referir aos mesmos, conforme aponta ROSA (2005, p. 53): “Há quem prefira as expressões "crimes de computador", "cybercrimes", "computer crimes", "delito informático", "crimes virtuais", "crimes eletrônicos", "crimes digitais", "crimes cibernéticos", "infocrimes" ou "crimes perpetrados pela Internet". São denominações distintas, mas que significam basicamente a mesma coisa”.

---

[4] A doutrina diverge acerca do primeiro delito informático cometido. Para alguns, o primeiro delito informático teria ocorrido no âmbito do MIT (Massachusetts Institute of Technology), no ano de 1964, onde um aluno de 18 anos teria cometido um ato classificado com cibercrime, tendo sido advertido pelos superiores4[4].
Outros ainda referenciam o primeiro caso de que se tem notícia sobre hacking no ano de 1978, na Universidade de Oxford, onde um estudante copiou de uma rede de computadores uma prova. Uma invasão seguida de uma cópia. Até essa data não existia lei sobre crimes informáticos nos Estados Unidos. [...]

Não obstante tal divergência terminológica, a doutrina igualmente diverge quanto ao papel da tecnologia informática para a conceituação de crime cibernético. Neste sentido, parte da doutrina compreende que eles podem se referir tanto aos crimes que utilizam a internet como meio e àqueles que atacam bens virtuais, como defendem JESUS & MILAGRE (2016, p. 49)[5].

Inobstante o uso deste termo para se referir a tais delitos, isto não implica que dentro do conceito "crimes informáticos" eles não se subdividam em diversas categorias, as quais demandam respostas específicas do direito. Assim, JESUS & MILAGRE (2016, p. 53-54) propõe classificação para os crimes informáticos em crimes informáticos próprios, impróprios, mistos e mediato ou indireto [6].

Contudo, a generalidade trazida pela conceituação de delitos virtuais não é vista de forma unânime pela literatura jurídica, isto porque, para outra parte da doutrina o bem jurídico digital é figura intrínseca dos delitos informáticos, o qual é constituído de elementos voltados à área virtual, tais como a própria informática, assim como a privacidade do usuário e a integridade dos dados e das informações abrigadas no espaço informático, como lecionam VIANNA & MACHADO (2013, p. 29)[7].

---

[5] Conceituamos crime informático como o fato típico e antijurídico cometido por meio da ou contra a tecnologia da informação. Decorre, pois, do Direito Informático, que é o conjunto de princípios, normas e entendimentos jurídicos oriundos da atividade informática. Assim, é um ato típico e antijurídico, cometido através da informática em geral, ou contra um sistema, dispositivo informático ou rede de computadores. Em verdade, pode-se afirmar que, no crime informático, a informática ou é o bem ofendido ou o meio para a ofensa a bens já protegidos pelo Direito Penal.

[6] Assim, classificamos os crimes informáticos em:

a) crimes informáticos próprios: em que o bem jurídico ofendido é a tecnologia da informação em si. Para estes delitos, a legislação penal era lacunosa, sendo que, diante do princípio da reserva penal, muitas práticas não poderiam ser enquadradas criminalmente;

b) crimes informáticos impróprios: em que a tecnologia da informação é o meio utilizado para agressão a bens jurídicos já protegidos pelo Código Penal brasileiro. Para estes delitos, a legislação criminal é suficiente, pois grande parte das condutas realizadas encontra correspondência em algum dos tipos penais;

c) crimes informáticos mistos: são crimes complexos em que, além da proteção do bem jurídico informático (inviolabilidade dos dados), a legislação protege outro bem jurídico. Ocorre a existência de dois tipos penais distintos, cada qual protegendo um bem jurídico;

d) crime informático mediato ou indireto: trata-se do delito informático praticado para a ocorrência de um delito não informático consumado ao final. Em Direito Informático, comumente um delito informático é cometido como meio para a prática de um delito-fim de ordem patrimonial.

[7] Em rigor, para que um delito seja considerado de caráter informático, é necessário que o bem jurídico por ele protegido seja a inviolabilidade de informações e dados, corolário do direito fundamental à privacidade e intimidade (art. 5º, X, da CR).

A simples utilização pelo agente de um computador para a execução de um delito, por si só, não configuraria um crime informático, caso o direito afetado não seja a informação automatizada. Ocorre, no entanto, que muitos autores acabaram, por analogia, denominando como crimes informáticos as infrações penais em que o computador serviu como mero instrumento utilizado na prática do delito. Apesar de imprópria, esta denominação se tornou muito popular e hoje é impossível ignorá-la.

Conforme se extrai da argumentação supracitada, definir o crime virtual como aquele tipo penal de qualquer natureza cometido por meio informático não se mostra como a conceituação mais correta em termos técnicos. Outrossim, em que pese haver uma multiplicidade de sinônimos para se referir às infrações penais cometidas no ciberespaço, JESUS & MILAGRE (2016, p. 50) advertem que “no Brasil, escolheu-se nomear os crimes cometidos contra a informática de “delitos informáticos”, termo usual em países de língua espanhola que se relaciona à ideia de proteção do objeto jurídico informática e informação”.

Neste sentido, a legislação penal, por meio da Lei Nº 12.737/12, tipifica como sendo crimes informáticos os crimes de “invasão de dispositivo informático”, de “interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública” e de “falsificação de cartão” (BRASIL, 2012).

É importante destacar que a relevância de práticas prejudiciais a terceiros no ciberespaço se deu com a popularização dos instrumentos eletrônicos e às facilidades de comunicação advindas com a rede mundial de computadores, fatores que contribuíram para a disseminação de atividades ao redor do mundo, especialmente aquelas de cunho ilícito. Nessa sistemática, Pinheiro (2021, p. 223) corrobora com a discussão asseverando que o crime eletrônico é, essencialmente, um crime de meio, ou seja, utiliza um ambiente virtual. Não é um crime de fim por natureza, exceto em casos de crimes cometidos por hackers, que podem ser classificados como estelionato, extorsão, falsidade ideológica, fraude, entre outros. Isso significa que o meio de execução pode ser virtual; no entanto, em muitos casos, o crime não é exclusivamente digital.

Para Pinheiro (2021, p. 223) a maioria dos crimes cometidos na internet também ocorre no mundo real, com a internet atuando como facilitadora devido ao anonimato que proporciona. Portanto, os conceitos de crime, delito, ato e efeito são os mesmos tanto no Direito Penal tradicional quanto no Direito Penal Digital. As principais inovações jurídicas no âmbito digital referem-se à territorialidade e à investigação probatória, além da necessidade de tipificação penal para algumas modalidades específicas, que, devido às suas características únicas, merecem uma tipificação penal própria.

Desta maneira, independentemente da denominação doutrinária adotada para os crimes cibernéticos, a prática de atos lesivos envolvendo dispositivos informáticos implicou na necessidade de paulatinamente serem introduzidas alterações na

legislação penal como resposta a estes novos cenários advindos do uso das tecnologias informáticas.

2. DA TIPIFICAÇÃO DO CYBERBULLYING

2.1 A PRÁTICA DE BULLYING

Embora a prática de atos de intimidação e violência no ambiente escolar não seja um fenômeno recente, a utilização do termo bullying para caracterizar esta prática remonta à década de 1970 na Suécia e, posteriormente, tendo ganhado maior evidência após o suicídio de três jovens na Noruega em razão do bullying sofrido pelos mesmos na escola, como explica Silva (2015, p.80).

Silva (2015) na Noruega, o bullying foi, por muitos anos, uma fonte de preocupação para pais e professores, que expressavam seus medos e ansiedades através dos meios de comunicação. No entanto, as autoridades educacionais do país não se manifestavam oficialmente sobre os casos nas escolas. Na década de 1980, um evento trágico mudou essa situação: três crianças, entre dez e quatorze anos, cometeram suicídio no norte da Noruega. As investigações revelaram que os maus-tratos sofridos por esses jovens, praticados por seus colegas de escola, foram a principal causa da tragédia. Em resposta à comoção nacional, o Ministério da Educação da Noruega lançou uma ampla campanha para combater efetivamente o bullying nas escolas.

Assim, sendo evidentes as consequências nefastas da prática, o *bullying* se apresenta como uma forma específica de violência praticada principalmente no ambiente escolar caracterizada pela agressão intencional repetitiva à vítima, usualmente praticada como forma de dominação e entretenimento:

> Os atos de violência (física ou não) ocorrem de forma intencional e repetitiva contra um ou mais alunos que se encontram impossibilitados de fazer frente às agressões sofridas. Tais comportamentos não apresentam motivações específicas ou justificáveis. Em última instância, significa dizer que, de forma “natural”, os mais fortes utilizam os mais frágeis como meros objetos de diversão, prazer e poder, com o intuito de maltratar, intimidar, humilhar e amedrontar suas vítimas. (CNJ, 2016, p.7)

Importante destacar que o bullying pode se apresentar na prática de diversas formas de violência que não somente física ou psicológica, mas também material, moral, sexual e virtual (cyberbullying). Conforme cartilha do Conselho Nacional de

Justiça, CNJ (2016, p.7), voltada à prevenção e combate do bullying, são atos característicos de tais forma de violência:

> • verbal (insultar, ofender, falar mal, colocar apelidos pejorativos, "zoar");
>
> • física e material (bater, empurrar, beliscar, roubar, furtar ou destruir pertences da vítima);
>
> • psicológica e moral (humilhar, excluir, discriminar, chantagear, intimidar, difamar);
>
> • sexual (abusar, violentar, assediar, insinuar);
>
> • virtual ou cyberbullying (bullying realizado por meio de ferramentas tecnológicas: celulares, filmadoras, internet etc.).

A prática do *bullying* está relacionada a um processo de violência realizado de forma cíclica em que existe uma relação de poder desigual, haja vista que a vítima não possui condições de se defender das agressões, as quais são perpetradas com o objetivo de fazer com que a dor de uma pessoa seja fonte de prazer e diversão para outras.

Desta maneira, conforme adverte PEREIRA (2019, p.13), "o bullying pode interferir na autoestima, concentração, motivação para os estudos e rendimento escolar, causando muitas vezes a reprovação do estudante e até sua saída da escola". Contudo, a violência contínua e sistemática a que as vítimas de bullying são submetidas não somente impacta sua vivência escolar, podendo também ter consequências significativas na sua saúde física e mental na vida adulta[8].

Ademais, o *bullying* também se diferencia de outras formas de violência por sua dinâmica envolver não somente vítimas e agressores, mas também seus espectadores, ou seja, "aqueles alunos que testemunham as ações dos agressores

[8] As consequências são as mais variadas possível e dependem muito de cada indivíduo, da sua estrutura, de vivências, de predisposição genética, da forma e da intensidade das agressões. No entanto, todas as vítimas, sem exceção, sofrem com os ataques de bullying (em maior ou menor proporção). Muitas levarão para a vida adulta marcas profundas das agressões e necessitarão de apoio psiquiátrico e/ou psicológico para a superação do problema.
Os problemas mais comuns são: desinteresse pela escola; problemas psicossomáticos; problemas comportamentais e psíquicos, como transtorno do pânico, depressão, anorexia e bulimia, fobia escolar, fobia social, ansiedade generalizada, entre outros. O bullying também pode agravar problemas preexistentes, devido ao tempo prolongado de estresse a que a vítima é submetida. Em casos mais graves, podem-se observar quadros de esquizofrenia, homicídio e suicídio.
(CNJ, 2016, p.9)

contra as vítimas, mas não tomam nenhuma atitude em relação a isso" (SILVA, 2015, p. 31).

Assim, sendo evidente para aqueles que presenciam as agressões que tais práticas são no mínimo moralmente erradas, quando não claramente criminosas; a omissão dos espectadores se apresenta como um elemento importante para sua perpetuação. Neste contexto, SILVA (2015, p.31-32) leciona que os espectadores podem ser classificados em três grupos[9].

Por sua vez, uma das manifestações dessa violência, que vem crescendo cada vez mais nos últimos anos devido ao avanço das tecnologias referentes às redes sociais, é o fenômeno do *cyberbullying.* Termo cunhado por Bill Belsey em 2005 para descrever o uso de tecnologias de informação e comunicação para a prática de ações ofensivas contra um indivíduo ou grupo:

> O cyberbullying envolve o uso de tecnologias de informação e comunicação, como e-mail, mensagens de texto de telefones celulares e pagers, mensagens instantâneas, sites pessoais difamatórios e sites difamatórios de pesquisas pessoais on-line, para apoiar o comportamento deliberado, repetido e hostil de um indivíduo. ou grupo, com a intenção de prejudicar outras pessoas.
> (BELSEY apud BAULMAN, 2007, p.3-4. Tradução nossa.)[10]

Todavia, o *cyberbullying* se apresenta como tendo consequências negativas muito mais severas do que o bullying presencial em razão de que a possibilidade de anonimato no ambiente virtual leva a prática de violências mais exacerbadas pela confiança do autor em não ser reconhecido.

---

[9] Espectadores passivos
Em geral, assumem essa postura por medo absoluto de se tornarem a próxima vítima. [...] Eles não concordam e até repelem as atitudes dos bullies; no entanto, ficam de mãos atadas para tomar qualquer atitude em defesa das vítimas. Nesse grupo encontram-se aqueles que, ao presenciar cenas de violência ou que trazem embaraços aos colegas, estão propensos a sofrer consequências psíquicas, uma vez que sua estrutura psicológica também é frágil. Espectadores ativos
Estão inclusos nesse grupo os alunos que, apesar de não participarem ativamente dos ataques contra as vítimas, manifestam apoio moral aos agressores, com risadas e palavras de incentivo. Não se envolvem diretamente, mas isso não significa, em absoluto, que deixem de se divertir com o que veem. [...]Espectadores neutros Entre eles, podemos perceber os alunos que, por uma questão sociocultural (originários de lares desestruturados ou de comunidades em que a violência faz parte do cotidiano), não demonstram sensibilidade pelas situações de bullying que presenciam. São acometidos por uma anestesia emocional, em função do próprio contexto social no qual estão inseridos. [...]

[10] No original: Cyberbullying involves the use of information and communication technologies such as e-mail, cell phone and pager text messages, instant messaging, defamatory personal Web sites, and defamatory online personal polling Web sites, to support deliberate, repeated, and hostile behaviour by an individual or group, that is intended to harm others.

Sobre o aspecto, Alves (2017) leciona que o anonimato associado a esse tipo de agressão tem sido reconhecido como um fator que potencializa comportamentos antissociais e reduz a disposição dos observadores em ajudar (Dooley & Cross, 2009). Enquanto no bullying tradicional a vítima e o agressor se conhecem e estão cara a cara, no cyberbullying a vítima não sabe quem está por trás das agressões anônimas. Esse anonimato pode, inclusive, intensificar a agressão, já que o agressor sente uma confiança maior por não ser identificado.

Nesse diapasão, apesar do *cyberbullying* basear-se em uma discrepância de poder, nos mesmos moldes do *bullying,* por certo, a diferença fulcral entre essas duas práticas é o fato de que no *cyberbullying "*tem um enorme impacto para além do momento em que é executado, uma vez que o que é colocado na Internet irá permanecer online ultrapassando deste modo os limites do espaço pessoal e físico" (ALVES, 2017, p. 11). Conforme a Cartilha do CNJ (2016, p. 8) [11].

Dessa forma, tendo em vista a amplitude de formas em que a violência oriunda do *bullying* e do *cyberbullying* pode se manifestar, profissionais de diversas áreas do comportamento humano e das ciências em geral vêm estudando os motivos que levam ao crescimento expressivo dessa prática violenta, bem como meios de impedir que essas continuem a reverberar. Na seara do direito, a discussão se dá acerca da importância da coibição desta prática.

2.2 TRATAMENTO JURÍDICO DO BULLYNG E DO CYBERBULLYNG

Com o expressivo crescimento de denúncias relativas à prática de *bullying* nos colégios, a necessidade de atuação jurídica acerca da questão se demonstra como de fundamental necessidade haja vista o lastro de direitos violados por tal prática; podendo ser citados, dentre eles, os direitos à vida, à saúde, à liberdade e direito à educação como aponta o relatório "Violência Escolar e Bullying" da Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO, 2019, p.5).

[11] Uma das formas mais agressivas de bullying, que ganha cada vez mais espaços sem fronteiras, é o cyberbullying ou bullying virtual. Os ataques ocorrem por meio de ferramentas tecnológicas, como celulares, filmadoras, máquinas fotográficas, internet e seus recursos (e-mails, sites de relacionamentos, vídeos). Além de a propagação das difamações ser praticamente instantânea, o efeito multiplicador do sofrimento das vítimas é imensurável. O cyberbullying extrapola, em muito, os muros das escolas e expõe a vítima ao escárnio público. Os praticantes desse modo de perversidade também se valem do anonimato e, sem nenhum constrangimento, atingem a vítima da forma mais vil possível. Traumas e consequências advindos do bullying virtual são dramáticos.

> Todas as formas de violência escolar e bullying violam o direito fundamental à educação e, da mesma forma, ambientes de aprendizagem não seguros reduzem a qualidade da educação para todos os estudantes. Nenhum país será capaz de atingir uma educação inclusiva e de qualidade se os estudantes estiverem expostos à violência na escola. A violência escolar e o bullying também podem afetar seriamente a saúde e o bem-estar de crianças e adolescentes, com consequências negativas que persistem até a idade adulta.

Diante deste cenário, o legislador instituiu o Programa de Combate à Intimidação Sistemática (*Bullying*) por meio da Lei 13.185/2015, bem como criou a Lei 13.663/2018, a qual alterou o art. 12 da Lei 9.394/96 (que estabelece as diretrizes e bases da educação nacional), de modo a incluir os incisos IX e X que visam a promoção de medidas de conscientização, prevenção e combate ao *bullying,* além do estabelecimento de ações com fins a promover a cultura de paz nas instituições de ensino.

Inobstante os possíveis direitos violados em decorrência dos atos de violência praticados, imperioso observar que a prática do bullying em sua essência constitui afronta a própria garantia constitucional de respeito à dignidade da pessoa humana. Conforme ensina NUCCI (2021, p.64): "Nada pode tecer de justo e realisticamente isonômico que passe ao largo da dignidade humana, base sobre a qual todos os direitos e garantias individuais são erguidos e sustentados".

Neste sentido, mesmo antes da tipificação do bullying pela Lei Nº 14.811/2024, a jurisprudência já reconhecia este tipo de violência como caracterizadora de dano moral, como se observa em um julgado de 2016 do Tribunal de Justiça do Distrito Federal[12].

---

[12] consumidor. Apelação cível. Bullying. Violação a direitos da personalidade evidenciados. Falha da prestação de serviço. Excludente de responsabilidade por ato de terceiro. Afastada. Dano moral configurado. Valor da indenização reduzido. Sentença parcialmente reformada.

1. Segundo a Lei nº 13.185/2015 ataques físicos, insultos pessoais, comentários sistemáticos e apelidos pejorativos, ameaças por quaisquer meios, grafites depreciativos, expressões preconceituosas, isolamento social consciente e premeditado, pilhérias (zombarias) são alguns exemplos de atos que podem ser considerados Bulling.
2. No caso dos autos restou incontroversa a ocorrência de alguns desses atos, especialmente o que se constata a partir da mídia à fl. 30, cujas mensagens se enquadram nos conceitos trazidos pelo artigo 2º da referida lei.
3. Comprovada a ocorrência de intimidações sistemáticas contra a Apelada, patente é a violação aos seus direitos da personalidade, razão pela qual restam configurados os danos extrapatrimoniais, os quais são, portanto, passíveis de serem compensados.
4. O Apelante, como centro de ensino, é incumbido do dever de guarda, devendo, assim, proporcionar um ambiente seguro e voltado às práticas educacionais, de modo a assegurar o saudável desenvolvimento cognitivo dos estudantes. No entanto, ao deixar de fiscalizar e apurar de forma efetiva

Neste contexto, quando submetida à jurisdição penal, a prática do *bullying* usualmente era tratada como caracterizadora do crime de constrangimento ilegal (art. 146, CP), ou seja, somente quando da violência/ameaça resultasse no constrangimento da vítima “a não fazer o que a lei permite, ou a fazer o que ela não manda” (BRASIL, 1940).

Desta maneira, a propositura para a tipificação do bullying como um crime específico teve origem no substitutivo ao Projeto de Lei Nº 4.224/2021, elaborado pela Comissão de Previdência, Assistência Social, Infância, Adolescência e Família, em 19 de junho de 2023, ao analisar o referido projeto, fundamentando sua necessidade para uma adequada proteção à criança e ao adolescente no ambiente escolar:

> A sociedade brasileira vivência momentos de rápidas transformações, muitas delas potencializadas pelo acesso a rede mundial de computadores e suas ferramentas de interação social (as conhecidas redes sociais), como por exemplo, o Facebook, Instagram, Tiktok, Youtube, Telegram e o próprio Whatsapp.
> Muito embora seja de grande valia a disseminação do conhecimento e da informação por diversas formas, é cedido que a rede mundial de computadores, infelizmente, também tem sido utilizada para disseminação de práticas delituosas, entre elas, a difusão de informações com incitação a crimes contra a integridade física ou psicológica de crianças e adolescentes, professores e funcionários de escolas públicas e privadas.
> A nossa proposta de substitutivo ao presente Projeto de Lei pretende estabelecer medidas de proteção às crianças e aos adolescentes contra violências em estabelecimento educacional ou similar, através da institucionalização de um protocolo de segurança escolar, sob a coordenação do Poder Executivo Municipal e do Distrito Federal e em conjunto com os órgãos de segurança pública, saúde e comunidade escolar.

---

os fatos ocorridos em suas dependências, permitindo-se, assim, a prática reiterada de bullying contra a apelada, a qual não lhe restou outra alternativa a não ser mudar de colégio, tem-se por evidenciada a conduta negligente do apelante e a prestação de um serviço defeituoso, na medida em que o ambiente escolar ofertado pelo apelante não ofereceu a segurança razoável que dele se podia esperar.
5. Não há de ser reconhecida a excludente de responsabilidade civil por ato atribuído a terceiro, mormente quando se verificar uma postura negligente por parte do apelante, que resultou na prestação de um serviço defeituoso, como é o caso em tela, motivo pelo qual cabível é a condenação do apelante ao pagamento de quantum a título de danos morais em favor da apelada.
6. Para a valoração do dano moral deve-se considerar a proporcionalidade entre o dano sofrido e as consequências causadas, bem como as condições econômico-financeiras da vítima e do agente causador do dano. O quantum indenizatório não deve induzir ao enriquecimento ilícito, ao contrário, deve trazer ao ofendido algum alento no seu sofrimento, bem como repreender a conduta do seu ofensor.
7. Apelação conhecida e parcialmente provida. Maioria.
(TJ-DF. Acórdão 946381, 20150610117859APC, Relator: GILBERTO PEREIRA DE OLIVEIRA, Relator Designado:FÁTIMA RAFAEL 3ª TURMA CÍVEL, data de julgamento: 1/6/2016, publicado no DJE: 10/6/2016. Pág.: 272/287)

> Importante destacar a institucionalização e construção coletiva do protocolo de segurança escolar em todos os entes federados, a fim de garantir medidas de proteção às crianças e aos adolescentes contra qualquer tipo de violência, tais como, física, psicológica, sexual, “bullying”, porte de drogas, arma branca ou arma de fogo, roubos, furtos, ameaças, racismo, discriminação e atentados.
> [...]
> No âmbito das escolas e com a potencialização das redes sociais, o ambiente eletrônico torna mais ativo e recorrente as agressões, podendo chegar à sua forma mais odiosa, a agressão física. Neste sentido, o “cyberbullying” é a prática de “bullying” por meio de ambientes virtuais, tornando-se mais massacrante, tendo em vista que não há forma de fuga por parte da vítima. Desta maneira, a vítima, mesmo que isolada, pode receber mensagens ameaçadoras e ofensas em suas redes sociais com alto potencial destrutivo. (CPI Dos Maus-Tratos Contra Crianças e Adolescentes do Senado Federal) (BRASIL, 2023)

O referido projeto de lei objetivava instituir medidas de proteção à criança e ao adolescente contra violências, originalmente propondo o aumento das penas cominadas para o crime de induzimento ou auxílio à automutilação ou suicídio (art.122, CP) quando a conduta fosse realizada por meio da rede mundial de computadores ou transmitida em tempo real e para o crime de maus-tratos (art. 136, CP) quando cometidos contra menores de 14 anos; bem como a inclusão de diversos crimes cometidos contra crianças e adolescentes como hediondos.

Com o advento da Lei Nº 14.811, de 12 de janeiro de 2024, a prática do bullying foi especificamente tipificada, de forma a constituir o crime de Intimidação Sistemática por meio da inserção do art.146-A no Código Penal:

> Art. 6º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar acrescido do seguinte art. 146-A:
>
> **"Intimidação sistemática (*bullying*)**
> Art. 146-A. Intimidar sistematicamente, individualmente ou em grupo, mediante violência física ou psicológica, uma ou mais pessoas, de modo intencional e repetitivo, sem motivação evidente, por meio de atos de intimidação, de humilhação ou de discriminação ou de ações verbais, morais, sexuais, sociais, psicológicas, físicas, materiais ou virtuais:
> Pena - multa, se a conduta não constituir crime mais grave.
>
> **Intimidação sistemática virtual (*cyberbullying*)**
> *Parágrafo único.* Se a conduta é realizada por meio da rede de computadores, de rede social, de aplicativos, de jogos on-line ou por qualquer outro meio ou ambiente digital, ou transmitida em tempo real:
> Pena - reclusão, de 2 (dois) anos a 4 (quatro) anos, e multa, se a conduta não constituir crime mais grave."

(BRASIL, 2024)

O Código Penal passou a contar com previsão expressa quanto a prática de *bullying* como ilícito penal, tipificando a intimidação sistemática caracterizadora de sua prática em si como crime dado o reconhecimento de suas consequências nefastas para a saúde mental das vítimas e, em especial, para o desenvolvimento saudável delas quando infligida a crianças e ao adolescente.

Ademais, conforme é possível se observar da leitura do supramencionado dispositivo, o legislador cominou pena substancialmente mais severa para a prática do cyberbullying por compreender que tal delito quando cometido em sua modalidade virtual por meio da internet possui danosidade muito maior do que quando cometido em sua forma presencial. Neste sentido, SLONJE & SMITH (2008, p. 148) apontam como fatores para a maior danosidade da prática virtual do bullying:

> A literatura publicada sobre o cyberbullying, juntamente com um número crescente de websites sobre o tema, identificou uma série de características do cyberbullying que muitas vezes o distinguem da maioria das formas tradicionais de bullying. Uma delas é a dificuldade de fugir disso. Ao contrário das formas tradicionais de bullying escolar, em que, assim que a vítima chega a casa, fica longe do bullying até ao dia seguinte, no cyberbullying a vítima pode continuar a receber mensagens de texto ou e-mails onde quer que esteja. Outra é a amplitude do público potencial. O cyberbullying pode atingir audiências particularmente grandes num grupo de pares, em comparação com os pequenos grupos que são o público habitual no bullying tradicional. Por exemplo, quando alguém baixa uma imagem ou um videoclipe com a intenção de envergonhar a pessoa no clipe, o público que poderá ver esses clipes/vídeos pode ser muito grande. Outra característica comum do cyberbullying é a invisibilidade daqueles que praticam o bullying: o cyberbullying não é uma experiência presencial e (tal como a propagação de boatos) proporciona aos que praticam o bullying algum grau de “invisibilidade” e, por vezes, de anonimato. Na sequência disto, em comparação com a maior parte do bullying tradicional, a pessoa que pratica o cyberbullying pode estar menos consciente ou mesmo inconsciente das consequências causadas pelas suas ações. Sem esse feedback direto, poderá haver menos oportunidades de empatia ou remorso e também poderá haver menos oportunidades de intervenção do espectador.
> (Tradução nossa)[13]

[13] No original: The published literature on cyberbullying, together with an increasing number of websites on the topic, has identified a number of features of cyberbullying that often distinguish it from most traditional forms of bullying. One is the difficulty of getting away from it. Unlike traditional forms of school bullying, where once the victim gets home they are away from the bullying until the next day, with cyberbullying the victim may continue to receive text messages or emails wherever they are. Another is the breadth of potential audience. Cyberbullying can reach particularly large audiences in a peer group compared with the small groups that are the

Por sua vez, como apontado por SLONJE & SMITH (2008), o indivíduo que se torna vítima da prática do cyberbullying não encontra paz ou proteção em seu próprio lar, o qual deveria seu local de proteção, amparo e segurança; consonante definição dada pela própria Constituição Federal de 1988 ao dispor que "a casa é asilo inviolável do indivíduo" (art. 5º, XI). De acordo com SANTOS (2011, p.12-13):

> A preservação da honra, da imagem e da intimidade da criança e do adolescente se veem ameaçadas especialmente pela prática do cyberbullying, que além de ter seu alcance expandido ao nível mundial, potencializando a ofensa à honra e à imagem, tem também natureza invasiva e persegue a criança em todos os ambientes, violando sua intimidade.
> [...] A situação se agrava diante da emergência do cyberbullying, que passa a perseguir a criança e o adolescente fora do ambiente escolar, colocando a vítima ao alcance do agressor em qualquer lugar, por meio da facilidade proporcionada pelos instrumentos tecnológicos atuais aos quais toda criança ou adolescente tem acesso (celular, Internet etc.).

Por conseguinte, a capacidade do *cyberbullying* em constranger de forma generalizada sua vítima, dada a velocidade com a qual mensagens, fotos, vídeos, dentre outras mídias são compartilhadas e propagadas, torna o cyberbullying mais danoso que o *bullying.* Assim, se verifica extremamente adequada a instituição de punição mais severa à prática do "*bullying* virtual".

2.3 CYBERBULLYNG COMO ATO INFRACIONAL E A RESPONSABILIZAÇÃO PENAL DOS PAIS DO MENOR INFRATOR

Conforme anteriormente exposto, a iniciativa de dispor expressamente no Código Penal acerca das práticas do *bullying* e do *cyberbullying,* se deu em decorrência de sua inserção entre um conjunto amplo de medidas instituídas pela Lei

---

usual audience in traditional bullying. For example, when someone downloads a picture or video clip with intention to embarrass the person in the clip, the audience that may see these clips/ videos can be very large. Another common characteristic of cyberbullying is the invisibility of those doing the bullying: cyberbullying is not a face-to-face experience, and (like rumor-spreading) provides those doing the bullying with some degree of "invisibility" and at times anonymity. Following on from this, compared to most traditional bullying, the person carrying out cyberbullying may be less aware or even unaware of the consequences caused by his or her actions. Without such direct feedback there may be fewer opportunities for empathy or remorse and there may also be less opportunity for bystander intervention.

Nº 14.811/2024 com o objetivo de fortalecer a proteção legal dada às crianças e aos adolescentes, como observa-se em sua ementa[14].

Nesta esteira, como se observa da leitura do art.146-A, caput e parágrafo único, a redação dada para a tipificação do bullying não traz restrição quando a necessidade de que a vítima seja menor de idade. Assim, inobstante a possibilidade da prática do bullying tendo por vítimas indivíduos adultos, é evidente que a tipificação do bullying decorreu da necessidade de sua coibição para assegurar as crianças e adolescentes sua proteção integral.

> Deve-se entender a proteção integral como o conjunto de direitos que são próprios apenas aos cidadãos imaturos; estes direitos, diferentemente daqueles fundamentais reconhecidos a todos os cidadãos, concretizam-se em pretensões nem tanto em relação a um comportamento negativo (abster-se da violação daqueles direitos) quanto a um comportamento positivo por parte da autoridade pública e dos outros cidadãos, de regra adultos encarregados de assegurar esta proteção especial. Por força da proteção integral, crianças e adolescentes têm o direito de que os adultos façam coisas em favor deles. (CURY, 2005, p. 33)

Contudo, embora inegável as consequências particularmente gravosas para as vítimas do bullying quando tal violência ocorre em sua infância ou adolescência, também é imperioso ressaltar ser notável que sua prática também é realizada de forma preponderante por crianças e adolescentes.

Assim, um dos pontos de análise fundamental para compreender a eficácia da tipificação do *bullying* e do *cyberbullying* forem praticados por menor, é que, nesse caso, estar-se-á tratando de ato infracional. De acordo com a legislação pátria, tanto na Constituição Federal quanto no Código Penal e no Estatuto da Criança e do Adolescente são considerados inimputáveis os menores de 18 anos. De acordo com o art. 228 da Constituição, estes ficam sujeitos às normas constantes em legislação especial.

O Estatuto da Criança e do Adolescente, portanto, prevê expressamente em seu art. 103 que as condutas tidas como crime ou contravenção penal, quando

[14] Institui medidas de proteção à criança e ao adolescente contra a violência nos estabelecimentos educacionais ou similares, prevê a Política Nacional de Prevenção e Combate ao Abuso e Exploração Sexual da Criança e do Adolescente e altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), e as Leis nºs 8.072, de 25 de julho de 1990 (Lei dos Crimes Hediondos), e 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente).

praticadas por menor, passam a ser consideradas ato infracional. O ECA, em seu art. 112 e 122, dispões sobre quais medidas são pertinentes ao ato infracional, *in verbis*:

> Art. 112. Verificada a prática de ato infracional, a autoridade competente poderá aplicar ao adolescente as seguintes medidas:
>
> I - advertência;
> II - obrigação de reparar o dano;
> III - prestação de serviços à comunidade;
> IV - liberdade assistida;
> V - inserção em regime de semi-liberdade;
> VI - internação em estabelecimento educacional;
> VII - qualquer uma das previstas no art. 101, I a VI.
> § 1º A medida aplicada ao adolescente levará em conta a sua capacidade de cumpri-la, as circunstâncias e a gravidade da infração.
>
> Art. 122. A medida de internação só poderá ser aplicada quando:
>
> I - tratar-se de ato infracional cometido mediante grave ameaça ou violência a pessoa;
> II - por reiteração no cometimento de outras infrações graves;
> III - por descumprimento reiterado e injustificável da medida anteriormente imposta.
> (BRASIL, 1990)

A Constituição de 1988 ainda previu a criação de um sistema de justiça juvenil, destinado a atender aos casos de crianças e adolescentes que cometem atos infracionais; justificando assim seu tratamento diferenciado em consonância com o entendimento dos menores como “pessoas em desenvolvimento” como lecionam CUCCI & CUCCI (2011, pg. 79):

> [...] a proteção integral tem como fundamento a concepção de que a criança e o adolescente são sujeitos de direitos, frente à família, à sociedade e ao Estado. Rompe com a ideia de que sejam simples objetos de intervenção no mundo adulto, colocando-os como titulares de direitos comuns a toda e qualquer pessoa, bem como de direitos especiais decorrentes da condição peculiar de pessoas em processo de desenvolvimento.

Logo, a maioridade penal não se justifica somente por um mero arbítrio do legislador, mas reflete a atenção prioritária e diferenciada dada à esta pessoa em desenvolvimento de forma que as medidas socioeducativas impostas em decorrência do cometimento de infração penal pelo menor são pautadas por sua proposta pedagógica objetivando a reinserção social do jovem.

Nesse diapasão, é sabido, pois, que um indivíduo abaixo dos 18 anos de idade não possui, biologicamente, desenvolvimento mental completo para ser penalmente responsabilizado por seus atos. Além disso, a sua percepção dos fatos e da vida é diferente da que um indivíduo adulto e experiente possui, de modo que suas ações são eivadas de vício no entendimento pleno da realidade de maneira a justificar a atual maioridade penal adotada.

Diante do exposto, é possível se verificar a ocorrência de uma situação particularmente problemática quanto a eficácia da tipificação do bullying, ora que, tendo sido instituído com o objetivo de garantir maior proteção às crianças e adolescentes, vítimas preponderantes da conduta; sua efetividade demanda a punição penal de seus autores, os quais também são preponderantemente menores.

Assim, o *bullying* quando for praticado por menor, especialmente na modalidade simples, tem uma punição extremamente leve, a qual culminará, provavelmente, na aplicação de mera advertência ao menor infrator. Logo, em tais hipóteses, ante a impossibilidade da plena aplicação de sua punição aos menores infratores, a eficácia da criminalização do bullying resta ameaçada tanto em relação à sua função punitiva, mas também preventiva.

Desta maneira, no que concerne ao cyberbullying em particular, a necessidade de responsabilização penal dos pais do menor infrator se faz essencial para a consecução da proteção dos direitos das crianças e adolescentes vítimas pretendida pela instituição do tipo penal em tela.

Neste contexto, os pais figuram como atores diretamente responsáveis por prevenir e combater a prática do cyber*bullying* no ambiente doméstico e, quando não o fazem, também devem ser enquadrados enquanto partícipes por omissão. Tal medida encontra justificativa perante a obrigatoriedade de vigilância quanto ao comportamento dos menores, bem como o monitoramento das atividades *online* destes.

Acerca deste dever de vigilância imposto aos pais em decorrência da guarda exercida sobre os filhos menores leciona Madaleno (2020, p. 494) [15]

[15] A guarda compreende a vigilância [...] porque os pais são responsáveis pelos atos ilícitos praticados pelos seus filhos menores e incapazes, assim como é dos progenitores o encargo de formação e educação da prole, de forma a que os filhos obtenham os conhecimentos necessários para exercerem a sempre árdua tarefa de lutarem diariamente pela sua vida, e depois pela vida de seus próprios filhos, suplantando os ciclos da existência humana, moldados de geração para geração.

No que se refere ao dever de vigilância e à responsabilidade de indenização acima mencionados, torna-se claro que os genitores, por exemplo, ao permitir aos menores o uso de tecnologias de comunicação, vetores do *cyberbullying,* tornam-se responsáveis por monitorar sua utilização. Sobre essa questão, inclusive anteriormente à promulgação da Lei Nº 14.811/2024, a jurisprudência já compreendia pela procedência da responsabilização civil dos pais pela prática de *cyberbullying* cometido por seus filhos impondo seu dever de indenizar os danos morais causados por sua prática[16].

Todavia, inobstante a responsabilidade civil dos pais pelos danos advindos das condutadas perpetradas por seus filhos menores, no cyberbullying tal responsabilização penal e não somente civil advém do controle que efetivamente os pais possuem sobre o acesso e a utilização dos aparelhos de comunicação pelo menor para a prática de cyberbullying (como computadores e telefones celulares).

Diferentemente do que ocorre em relação ao controle possível dos pais sobre a prática do bullying em sua modalidade tradicional, o exercício de tal controle no cyberbullying se apresenta como medida factualmente possível de ser adotada pelos pais. Logo, nos casos em que se verifica a prática de *cyberbullying* é imperioso que se analise a omissão dos pais em coibir e prevenir tais práticas por seus filhos sob pena de serem enquadrados como partícipes por omissão.

Acerca da participação por omissão, embora consista em situação de difícil conceituação e definição de parâmetros, o tratamento dos delitos omissivos é tema que vem sendo desenvolvido pela doutrina e por construções jurisprudenciais, como bem leciona RASSI (2012, 189-190) [17], “a responsabilidade sobre o controle de

---

[16] AÇÃO DE INDENIZAÇÃO. COMUNIDADE VIRTUAL DO ORKUT. MENSAGENS DEPRECIATIVAS A PROFESSOR. RESPONSABILIDADE DOS PAIS. Os danos morais causados por divulgação, em comunidade virtual, Orkut, de mensagens depreciativas, denegrindo a imagem de professor. Identificado por nome, mediante linguagem chula e de baixo calão, e com ameaças de depredação a seu patrimônio, devem ser ressarcidos. Incumbe aos pais, por dever legal de vigilância, a responsabilidade pelos ilícitos cometidos por filhos incapazes sob sua guarda.
(TJRO, Ap. Civil 100.007.2006.011349-2, Rel: juiz Edenir Sebastião Albuquerque da Rosa, DJ 20.08.2008, grifo nosso).

[17] Apesar das dificuldades conceituais de se estabelecer parâmetros claros sobre a participação por omissão, este é um problema contemporâneo importante para a aplicação do direito e independentemente das soluções propostas pela doutrina tem chegado aos tribunais e exigido uma solução mais premente. A participação por omissão, dessa forma, vem encontrando acolhida nas construções jurisprudenciais e desenvolvendo-se concomitantemente ao tratamento dos delitos omissivos.
A necessidade em reconhecer a participação por omissão surge na jurisprudência pelo inconveniente em se punir determinadas condutas omissivas de menor gravidade, relacionadas à participação em um delito, com as graves penas previstas para os casos de autoria.

condutas de terceiros perigosos variará sensivelmente, de acordo com o grau de dependência do terceiro", complementando acerca dos requisitos para que tal omissão de controle se afigure como passível de punição na esfera penal:

> A omissão deve estar inserida no curso dos acontecimentos de forma a facilitar a comissão de um delito. A mera passividade não é elemento normativo suficiente para qualificar uma omissão como colaboração ou intervenção no delito. Segundo Guillermo Contreras, nos casos em que a omissão houver contribuído decisivamente para o resultado, tem-se a hipótese de autoria omissiva. Ao contrário, se a omissão só poderia ter dificultado a ação, mas em nenhum caso impedi-la, então estaríamos diante de um caso de participação por omissão. Para o autor, o omitente comete um delito de omissão imprópria somente quando a vulneração de uma posição de proteção ou de controle permite estabelecer uma estrita equiparação (causalidade e imputação objetiva) entre o comportamento ativo e passivo acerca do resultado. (RASSI, 2012, p. 197)

Desta maneira, a omissão dos pais em não exercer seu dever de vigilância sobre as atividades de seus filhos na internet e, sobretudo, em não obstar sua utilização destes dispositivos de comunicação quando notificados da prática de cyberbullying, se apresenta como hipótese caracterizadora de participação delitiva.

Em linhas gerais, quando se fala em participação por omissão, pressupõe-se que tal omissão se enquadre no curso dos acontecimentos fazendo com que o cometimento do delito principal se torne mais fácil. Contudo, para a responsabilização penal do agente omisso é preciso também se verificar a exigibilidade não somente legal, mas também social da conduta e o risco que esta representa efetivamente, conforme leciona RASSI (2012, p. 201) [18].

Aliás, chama-nos muito a atenção o fato de que os autores que se dedicam, atualmente, a entender os crimes omissivos impróprios e a propor alternativas viáveis para a sua restrição tenham sempre argumentos de "justiça", bom senso, do razoável da punição, sem que, ao fim e ao cabo, essas aspirações sejam traduzidas num instrumental jurídico que faça jus a estas críticas. O que se nota é uma dificuldade da teoria do Direito encontrar os instrumentos técnicos adequados (a definição das fronteiras do conceito de garante e dos crimes omissivos impróprios) para traduzir este apelo de razoabilidade feito pela doutrina mais restritiva do direito penal.

[18] As teorias tradicionais da participação, como visto anteriormente, permitem uma abertura considerável do leque de condutas que podem ser incriminadas a título de participação, uma vez baseadas na verificação de uma conduta causal e consciente de favorecimento, sem que, contudo, haja um elemento subjetivo suficiente para sua reprovabilidade.

Os instrumentos da imputação objetiva visam minorar estes efeitos através da introdução de considerações normativas para avaliação da participação, a fim de restringir as hipóteses das ações ou omissões que possam configurar a participação. Estes elementos normativos passam, especialmente, pela exigência de que a conduta seja uma superação do incremento do risco permitido e pela avaliação da proximidade com o bem jurídico.

A omissão penalmente relevante é, nestes termos, o critério normativo de imputação objetiva a ser aplicado, segundo nosso entendimento, para delimitar a participação punível da impunidade das condutas cotidianas.

Assim, tendo em vista que a tipificação do cyberbullying fundamentou-se em sua necessidade para garantir adequada proteção as crianças e adolescentes vítimas desta prática extremamente nociva ao seu desenvolvimento saudável, é possível se concluir que a omissão dos pais do menor autor quando relativa à atos de simples para sua cessação (como a retirada de acesso a dispositivos de comunicação) é relevante, reprovável e constitui efetivamente a assunção do risco dos resultados notadamente sabidos que a prática de cyberbullying pode acarretar.

Ademais, quanto a reprovabilidade desta omissão, importante ressaltar que a proteção à criança e ao adolescente objetivada pela criminalização do bullying também é atingida quando os pais impedem que seu filho menor pratique bullying, ora que, a omissão em educar também fere o direito do menor ao seu desenvolvimento saudável.

Por conseguinte, é possível concluir que a ação dos pais é fundamental para que se dificulte a prática de *cyberbullying,* pelo menos no ambiente doméstico, sendo sua omissão, nesses casos, potencialmente decisiva na concretização do delito, situação em que a reprovabilidade de tal conduta é elevada. Logo, visando a plena eficácia social e jurídica da norma em comento, ou seja, com fins à punibilidade efetiva das práticas do *cyberbullying,* faz-se necessária a consolidação da figura do partícipe por omissão nos casos de *cyberbullying* praticados por menor*,* haja vista a responsabilidade dos pais de agir para prevenir ou impedir tais práticas.

A responsabilização dos responsáveis legais desses menores como partícipes por omissão se apresenta não somente como juridicamente adequada e coerente, mas como necessária para a efetividade do combate à prática, dado o caráter preventivo da pena ao impor aos adultos imputáveis temor e respeito à norma e, assim, incentivar a adoção de medidas proativas dos pais para impedir seus filhos de descumpri-la.

3 – DESAFIOS DO DIREITO PENAL NA INVESTIGAÇÃO E COMBATE DO CYBERBULLYING

3.1 DA INVESTIGAÇÃO DO CYBERBULLYNG

A investigação de crimes cibernéticos, como o cyberbullying, requer um conjunto detalhado de procedimentos que são essenciais para a identificação, coleta e preservação de evidências digitais e, assim, garantir tanto a integridade quanto a admissibilidade das provas em ambientes jurídicos em decorrência das características peculiares dos crimes cibernéticos. Conforme dispõe o Manual Prático de Investigação de Crimes Cibernéticos do Ministério Público Federal (2006, pg. 15):

> De modo geral, podemos dizer que as evidências dos crimes cibernéticos apresentam as seguintes características:
> a) possuem formato complexo (arquivos, fotos, dados digitalizados etc.);
> b) são voláteis, i.e., podem ser apagadas, alteradas ou perdidas facilmente;
> c) costumam estar misturadas a uma grande quantidade de dados legítimos, demandando, por isso, uma análise apurada pelos técnicos e peritos que participam da persecução penal.

Importante ressaltar que, ao lidar com evidências digitais é fundamental entender que as informações na internet podem ser facilmente alteradas ou excluídas. Isso impõe aos investigadores a responsabilidade de agir rapidamente e com precisão técnica para assegurar que todas as evidências sejam coletadas e preservadas de forma adequada.

Na investigação dos crimes virtuais a preservação e validação das evidências obtidas também constitui elemento de vital importância para sua utilização em eventual processo judicial criminal. Desta maneira, a verificação da integridade dos dados coletados e a correta documentação do processo de coleta são essenciais para a admissibilidade das provas digitais.

A evidência digital, contudo, é notoriamente volátil, inicialmente anônima e suscetível a alterações ou modificações, inclusive podendo ser excluída sem aviso prévio. Exemplos comuns de evidências digitais incluem arquivos temporários, cookies, o momento de inicialização de um computador e os logs de acesso.

Por conseguinte, a preservação dessas evidências representa um desafio significativo, devendo todas as etapas envolvidas para sua obtenção serem devidamente documentadas. Assim, a integridade e autenticidade das informações precisam ser comprovadas através de uma cadeia de custódia clara, garantindo que as evidências coletadas representem fielmente os dados originais obtidos da aplicação de internet.

Desta maneira, importante ressaltar que a preservação das evidências digitais pode ser feita pela própria vítima. Um método eficaz para preservar conteúdo em casos de crimes virtuais é a elaboração de uma ata notarial em cartório, criando um documento público que descreve um evento ou circunstância relatada por uma das partes; sendo este método preferível ao uso de capturas de tela, cuja validade legal pode ser questionável.

Ademais, o procedimento adequado para a elaboração destas atas notariais com vistas a preservação de evidências digitais dependerá da natureza da evidência em tela, como expõe BARRETO & BRASIL (2016, p.70-73). [19]

[19] No momento da lavratura da ata notarial ou certidão, o elaborador deve ser objetivo e impessoal no relato dos fatos, não fazendo constar qualquer juízo de valor no corpo do documento, apenas relatando o que viu e/ou ouviu. No bojo do documento, deverá constar o requerimento da parte interessada para que o tabelião/escrivão intervenha na elaboração da ata ou certidão, bem como a indicação de local, hora, dia, mês e ano de sua realização. Tanto a ata notarial quanto a certidão lavrada por escrivão de polícia podem seguir os procedimentos relatados a seguir:
a) Constatar um fato na internet:
Descrição do caminho percorrido, descrevendo a metodologia adotada.
Data e horário do acesso.
Acesso ao conteúdo da URL mencionada pelo requerente.
Transcrição do conteúdo, caso se trate de texto ou de áudio com a gravação do conteúdo em mídia não regravável, indicando a URL completa.
No caso de vídeo, gravação em mídia ótica, bem como a descrição, em síntese, das cenas vistas.
Capturar trechos do conteúdo e anexar ao documento.
b) Acesso a conteúdo de telefone celular: normalmente apresentado pela vítima ou por seu representante legal para verificar o envio ou recebimento de mensagens de texto, acesso a conteúdo de internet, acesso a webmail ou qualquer outra função que esteja armazenada no celular do requerente. Tal diligência não substitui a perícia técnica, se for o caso. Deve conter: Descrição do aparelho telefônico, constando marca, modelo, cor, IMEI, número de série do chip e o respectivo número de telefone com DDD.
Etapas que percorreu até acessar o conteúdo (metodologia): softwares, aplicativos e pastas acessadas.
Captura de telas e transcrição fiel do conteúdo.
Gravação do conteúdo em mídia não regravável.
c) Constatar e-mail enviado ou recebido na internet:
Descrição do caminho percorrido (metodologia).
Acesso ao conteúdo do e-mail, que deverá ser aberto pelo requerente na presença do tabelião/escrivão. Deve mencionar apenas o endereço de e-mail acessado, sem a necessidade da senha.
Acessar o cabeçalho do e-mail e apontar de onde a mensagem foi enviada, registrando o caminho específico seguido por ela, além de data, remetente, destinatário, assunto e momento do envio.
Transcrição do conteúdo que se encontra no corpo do texto do e-mail. No caso de anexos, deve-se extrair e anexar em mídia não regravável.
Captura de telas e imagens.

Assim, o adequado procedimento para a investigação e coleta de provas dos crimes virtuais está diretamente atrelado ao meio utilizado para a perpetração dos atos criminosos (MPF, 2006). Neste sentido, no crime de cyberbullying, nos termos do parágrafo único do art. 146-A (BRASIL, 1940), ou seja, quando os atos de intimidação característicos do bullying não constituem crime mais grave; é possível se vislumbrar como principais meios para sua prática a criação de websites, o envio de e-mails, a utilização de aplicativos de mensagens (como o WhatsApp e o Telegram) e de redes sociais (como o Facebook e o Instagram).

Gravação do conteúdo em mídia não regravável.
d) Acesso a conteúdo de apps de comunicação via internet (WhatsApp, Viber, Telegram):
Descrição do caminho percorrido (metodologia).
Identificar os interlocutores associados na aplicação com o respectivo número de telefone. Inserir as mensagens trocadas referentes aos diálogos.
Mencionar os grupos de usuários nos quais o conteúdo foi mencionado.
Captura de telas e imagens.
Gravação do conteúdo em mídia não regravável.
e) Conteúdo postado no Facebook:
Descrição do caminho percorrido (metodologia).
Endereço de e-mail do requerente e do responsável pela postagem do conteúdo, com o respectivo nome de usuário ou número de identificação da conta do perfil no Facebook.
Dia e hora da postagem.
Informar URLs nas quais o conteúdo se encontra disponibilizado.
Informar quantas curtidas e compartilhamentos foram feitos no respectivo conteúdo, com a identificação dos usuários que assim procederam, bem como se ações foram feitas para o grupo de amigos ou para usuários selecionados (nível de alcance da postagem).
Captura de telas e imagens.
Gravação do conteúdo em mídia não regravável.
f) Conteúdo postado no Twitter:
Descrição do caminho percorrido (metodologia).
Dia, local e hora da postagem do conteúdo.
Informações sobre a conta do requerente e do responsável pela postagem do conteúdo no Twitter, caso possua, tais como: nome do usuário e login (@xxxxxxxxx), localização caso disponibilize, seguidores e seguidos.
Transcrição integral do conteúdo.
URL na qual o conteúdo se encontra disponibilizado com o link encurtado.
Alcance do tweet com informações de quantos viram e interagiram com o conteúdo postado.
Captura de telas e imagens.
Gravação do conteúdo em mídia não regravável.
g) Conteúdo postado no Instagram:
Descrição do caminho percorrido (metodologia).
Dia, local (caso disponibilizado) e hora da postagem do conteúdo.
Caso seja acessado alguns dias após o fato, não se pode precisar a data da postagem.
Informações do requerente e do responsável pela postagem do conteúdo (nome de usuário e login, seguidores e seguidos, número de posts).
Comentários e número de pessoas que curtiram.
Caso tenha informações sobre a localização do conteúdo postado, deverão ser consignadas no documento.
Captura de telas e imagens.
Gravação do conteúdo em mídia não regravável.

3.1.1 Websites

Na investigação de crimes cibernéticos, a análise de websites assume uma importância fundamental, especialmente no contexto do cyberbullying. Os websites (compreendidos tanto como as páginas web publicadas em domínio próprio, quanto os blogs sem domínio próprio) podem servir como palco para a manifestação de comportamentos abusivos, onde conteúdos difamatórios, ameaçadores ou humilhantes são postados com o intuito de intimidar ou assediar vítimas.

A investigação dos atos de cyberbullying cometidos por meio dessas plataformas requer não apenas acessar o endereço URL do site envolvido, mas também garantir que todas as evidências digitais, como páginas web e conteúdos associados sejam cuidadosamente preservadas, inclusive registrando-se quaisquer interações online que possam ter contribuído para o cyberbullying.

Devido à natureza volátil das informações online, que podem ser facilmente alteradas ou excluídas pelos usuários ou administradores do site, é essencial capturar uma cópia integral do conteúdo do website. Para tanto, a autoridade policial dispõe de diversos instrumentos para a coleta e preservação deste tipo de evidências, tais como:

> Existem aplicativos – por exemplo, o HTTrack4 - que permitem o download de sites inteiros, incluindo textos e fotos publicadas. Utilizar estes aplicativos é um artifício interessante para casos em que o volume de dados é grande. Após o download, os arquivos podem ser encaminhados para o órgão competente através de e-mails, disquetes e, se possível, em mídia não-regravável (CD-R)
> (MPF, 2006, p.19)

Além disso, tais aplicativos criam arquivos de log que documentam detalhes críticos, como a data, a hora e a URL específica acessada; dados fundamentais para estabelecer o contexto da atividade criminosa e que podem ser cruciais para traçar a origem e a natureza do cyberbullying. Por exemplo, um registro de log pode revelar que uma série de postagens abusivas foi feita de uma URL específica em momentos que coincidem com os relatos da vítima sobre quando o assédio ocorreu.

Outras ferramentas também são essenciais na investigação de websites. Navegadores em modo texto, como o LYNX, permitem a identificação rápida de links internos e externos do site investigado (MPF, 2006). Essas informações podem ajudar

a corroborar a narrativa da vítima e fornecer evidências concretas que podem ser usadas para responsabilizar os agressores.

Por sua vez, sendo a integridade das evidências de suma importância, em situações em que não é possível gravar os dados em mídias não-regraváveis como CDs, o uso de softwares como MD5Sum é recomendado para verificar a integridade dos dados:

> O MD5Sum é um aplicativo de verificação da integridade dos dados; na prática ele garante que os dados que foram gravados no momento da produção da prova não sofreram nenhum tipo de adulteração em todo o trâmite do processo.
> Tecnicamente, ao criarmos uma cópia de algum arquivo, criamos também sua assinatura baseada no arquivo original. Esta assinatura, em forma de um arquivo, acompanhará a cópia e permitirá que a qualquer momento o destinatário verifique se o arquivo recebido é idêntico ao original.
> (MPF, 2006, p.20-21)

Uma vez preservadas as evidências digitais, o próximo passo envolve a identificação do servidor que hospeda a página. Para sites nacionais, que terminam em ".br", o registro pode ser consultado através do NIC.br, que fornece informações detalhadas sobre o administrador do domínio e o provedor de serviços. Para domínios internacionais, serviços como WHOIS fornecem meios para localizar o responsável pelo site, embora isso possa envolver desafios adicionais caso o site esteja hospedado fora do Brasil e não haja conexões evidentes com o país (MPF, 2006). Esta etapa é crucial para determinar a jurisdição e a viabilidade de ações legais subsequentes.

3.1.2 E-mails

E-mails são uma ferramenta comum em diversas formas de atividades criminosas online, variando desde a comunicação direta entre criminosos até a execução de fraudes e a disseminação de malwares (MPF, 2006). Desta forma, o e-mail também pode ser um vetor significativo para o cyberbullying, ora que, em muitos casos, os agressores utilizam e-mails para enviar mensagens ameaçadoras, difamatórias ou perturbadoras diretamente às suas vítimas, ou para disseminar conteúdo prejudicial sobre elas a terceiros.

Neste contexto, a investigação de casos de cyberbullying via e-mail requer uma atenção meticulosa aos detalhes deste tipo de comunicação, demandando-se não

somente a preservação do conteúdo da mensagem, mas também do cabeçalho destes e-mails, o qual contém informações relativas a origem da mensagem, horários de envio e recebimento e a rota que a mensagem percorreu através de servidores de internet; dados essenciais para se rastrear e identificar os responsáveis pelo seu envio.

Este cabeçalho é particularmente importante porque, mesmo que o campo "de" (remetente) possa ser facilmente falsificado, o cabeçalho geralmente contém informações verídicas sobre a origem do e-mail. Contudo, dependendo do provedor de e-mail utilizado, a localização do cabeçalho deve ser realizada de diferentes maneiras:

> Em aplicativos como o Outlook ou Outlook Express, o cabeçalho de um e-mail pode ser acessado abrindo a mensagem e clicando Alt + Enter. Outra opção é clicar, com o botão direito do mouse, em cima da mensagem recebida e selecionar “Opções”. Na parte de baixo da janela aberta, há uma série de informações, agrupadas no título “Cabeçalho de Internet”.
> No groupwise (aplicativo utilizado no Ministério Público Federal), podemos localizar o cabeçalho de um e-mail abrindo a mensagem e clicando no Menu Arquivo – Anexos – Ver. Selecione o arquivo MIME.822.
> Nos acessos feitos via Internet – como nos sistemas WEBMAIL e WEBACESS – os provedores costumam trazer opções no MENU que permitem editar e imprimir cabeçalhos de e-mails. Algumas dessas opções aparecem com o título “ver código fonte da mensagem” ou “verificar código completo”, ou ainda “mensagem em formato texto”. Caso não existam estas opções, basta encaminhar o e-mail para uma outra conta, e usar o Outlook para editar o cabeçalho de e-mail.
> (MPF, 2006, p.29)

Diante dos desafios impostos pela natureza digital e frequentemente anônima dos e-mails, caso o cabeçalho do e-mail forneça um endereço IP, pode-se utilizar esse dado para descobrir a qual operadora de internet esse IP está associado. Nesta hipótese, as autoridades podem requisitar a quebra do sigilo telemático para que provedores de serviços de internet forneçam “cópia, em mídia não-regravável (CD-R), das páginas investigadas e os logs, isto é, os registros de criação e alteração da página” (MPF, 2006, p.26), informações necessárias para a comprovação da materialidade do delito e possivelmente também de seu autor.

A quebra do sigilo telemático também pode ser requerida quando o endereço de e-mail do remetente é conhecido mesmo que não seja possível identificar o IP. Nos

termos Manual Prático de Investigação de Crimes Cibernéticos do Ministério Público Federal (2006, pg. 15)[20].

Por sua vez, se a identificação do IP não for possível diretamente, a interceptação de dados telemáticos é uma ferramenta poderosa para coletar evidências e identificar os autores de crimes cibernéticos, podendo ser requerida pela autoridade policial ou pelo Ministério Públicos, nos termos da Lei Nº 9.296/96, possibilitando o monitoramento das comunicações realizadas por meio da conta de e-mail investigada:

> Sugerimos que o Ministério Público ou a autoridade policial requeiram a criação de uma "conta-espelho", isto é, uma conta de e-mail que contenha todas as correspondências eletrônicas recebidas e enviadas pelo usuário investigado. Com essa providência, a autoridade responsável pela investigação poderá monitorar, em tempo real, as comunicações eletrônicas feitas pelo usuário investigado.
> (MPF, 2006, p.31)

Ademais, também é fundamental analisar outros elementos associados aos e-mails em casos de cyberbullying; como arquivos anexos e links incluídos nos e-mails direcionando o acesso a sites que hospedam conteúdo abusivo ou difamatório.

3.1.3 Aplicativos de Mensagem

A comunicação através de aplicativos de mensagens instantâneas como WhatsApp e Telegram se tornou uma arena comum para uma variedade de interações sociais, incluindo, infelizmente, práticas criminosas como o cyberbullying. A garantia de privacidade que esses serviços oferecem em razão do emprego de criptografia de ponta a ponta, embora represente uma salvaguarda essencial para a privacidade dos usuários, também constituem um obstáculo significativo para as investigações criminais.

Com a utilização de criptografia de ponta a ponta, as mensagens são criptografadas no dispositivo do remetente e só podem ser descriptografadas no

[20] Se não foi possível localizar o número IP que originou a mensagem, mas há o endereço eletrônico do remetente (exemplo: joaodasilva@terra.com.br), a autoridade policial ou o membro do Ministério Público podem requerer judicialmente a quebra do sigilo de dados telemáticos para que o provedor do e-mail (no exemplo, o Terra) forneça o número IP da máquina que autenticou esta conta, na data e horário do e-mail remetido (ver modelo anexo). Caso queiram uma abrangência maior, poderão pedir a relação de todos os IPs gerados no momento de autenticação da conta, num determinado período (um mês, por exemplo).

dispositivo do destinatário, impedindo qualquer interceptação do conteúdo das mensagens por terceiros, incluindo os próprios provedores dos serviços (BARRETO & BRASIL, 2016).

Contudo, inobstante a utilização desta tecnologia ter dificultado a investigação criminal deste meio de comunicação cibernético, importante apontar que os próprios aplicativos preveem, em seus termos de serviço, a remoção do material e banimento do usuário em caso de sua a utilização para o cometimento de atividades ilícitas (ou consideradas como indevidas). Neste sentido, BARRETO & BRASIL (2016, p. 130-131) discorrem sobre tal política adotada pelo WhatsApp [21].

O processo para acessar as mensagens em investigações envolve etapas legais complexas, incluindo a obtenção de uma ordem judicial que detalha a necessidade da interceptação das comunicações para fins de investigação. E, mesmo com uma autorização judicial, o acesso é geralmente limitado aos metadados, como os horários em que as mensagens foram enviadas e recebidas e os identificadores dos usuários envolvidos nas conversas, sem acesso ao conteúdo real das mensagens.

A coleta de evidências através desses aplicativos enfrenta diversos desafios. Primeiramente, os provedores de serviços como WhatsApp e Telegram mantêm políticas estritas de proteção de dados e privacidade e resistem a fornecer dados dos usuários, a menos que haja uma necessidade legal clara e justificada. Além disso, muitos servidores que armazenam dados de usuários estão localizados em jurisdições internacionais, dificultando assim sua investigação, como bem explicam BARRETO & BRASIL (2016, p. 143):

> A evolução tecnológica, também acompanhada por criminosos, praticamente impossibilita que os órgãos investigativos individualizem a autoria e materialidade de crimes complexos sem o auxílio da própria tecnologia. A migração dos criminosos para a utilização de ferramentas que permitem não serem alcançados pela investigação

[21] Em seus Termos de Serviço, o WhatsApp só permite o uso lícito e aceitável da aplicação, não permitindo a sua utilização em: (a) de forma a violar, apropriar-se indevidamente ou infringir direitos do WhatsApp, dos nossos usuários ou de terceiros, inclusive direitos de privacidade, de publicidade, de propriedade intelectual ou outros direitos de propriedade; (b) de forma ilícita, obscena, difamatória, ameaçadora, intimidadora, assediante, odiosa, ofensiva em termos raciais ou étnicos, ou instigue ou encoraje condutas que sejam ilícitas ou inadequadas, inclusive a incitação a crimes violentos; (c) envolvendo declarações falsas, incorretas ou enganosas; (d) para se passar por outrem; (e) para enviar comunicações ilícitas ou não permitidas, mensagens em massa, mensagens automáticas, ligações automáticas e afins; ou (f) de forma a envolver o uso não pessoal dos nossos serviços, a menos que esteja autorizado por nós.

> faz com que se necessite justamente destes dados para o deslinde do procedimento investigatório.
> A exigência de um provedor, quanto à necessidade de cooperação jurídica internacional formal para o fornecimento de informações, compromete a celeridade e a viabilidade da apuração de delitos, que normalmente necessitam de respostas imediatas e pontuais. A cooperação deve ser colocada como um meio que pode ser utilizado, mas não como único caminho, não sendo adequado para a grande maioria das investigações.

Além disso, a quebra da criptografia para a investigação criminal se apresenta como matéria polemica, envolvendo questões legais e éticas principalmente no que tange ao direito à privacidade. Qualquer tentativa de quebrar a criptografia de ponta a ponta ou de acessar as comunicações de forma não autorizada pode ser vista como uma violação dos direitos civis, trazendo sérias consequências legais para os órgãos de aplicação da lei.

Neste contexto, o acesso as mensagens armazenadas em aparelhos celulares, incluindo aquelas contidas em aplicativos criptografados, pela autoridade policial não requer autorização judicial específica quando a apreensão do aparelho ocorrer no momento de prisão em flagrante ou em razão de mandado de busca e apreensão; conforme entendimento consolidado na jurisprudência do Superior Tribunal de Justiça[22].

---

[22] processual penal. Recurso ordinário em habeas corpus. Tráfico de drogas e associação ao tráfico. Dados armazenados no aparelho celular. Inaplicabilidade do art. 5°, xii, da constituição federal e da lei n. 9.296/96. Proteção das comunicações em fluxo. Dados armazenados. Informações relacionadas à vida privada e à intimidade. Inviolabilidade. Art. 5°, x, da carta magna. Acesso e utilização. Necessidade de autorização judicial. Inteligência do art. 3° da lei n. 9.472/97 e do art. 7° da lei n. 12.965/14. Telefone celular apreendido em cumprimento a ordem judicial de busca e apreensão. Desnecessidade de nova autorização judicial para análise e utilização dos dados neles armazenados. Recurso não provido.
I - O sigilo a que se refere o art. 5º, XII, da Constituição da República é em relação à interceptação telefônica ou telemática propriamente dita, ou seja, é da comunicação de dados, e não dos dados em si mesmos. Desta forma, a obtenção do conteúdo de conversas e mensagens armazenadas em aparelho de telefone celular ou smartphones não se subordina aos ditames da Lei n. 9.296/96.
II - Contudo, os dados armazenados nos aparelhos celulares decorrentes de envio ou recebimento de dados via mensagens SMS, programas ou aplicativos de troca de mensagens (dentre eles o "WhatsApp"), ou mesmo por correio eletrônico, dizem respeito à intimidade e à vida privada do indivíduo, sendo, portanto, invioláveis, nos termos do art. 5°, X, da Constituição Federal.
Assim, somente podem ser acessados e utilizados mediante prévia autorização judicial, nos termos do art. 3° da Lei n. 9.472/97 e do art. 7° da Lei n. 12.965/14.
III - A jurisprudência das duas Turmas da Terceira Seção deste Tribunal Superior firmou-se no sentido de ser ilícita a prova obtida diretamente dos dados constantes de aparelho celular, decorrentes de mensagens de textos SMS, conversas por meio de programa ou aplicativos ("WhatsApp"), mensagens enviadas ou recebidas por meio de correio eletrônico, obtidos diretamente pela polícia no momento do flagrante, sem prévia autorização judicial para análise dos dados armazenados no telefone móvel.
IV - No presente caso, contudo, o aparelho celular foi preendido em cumprimento a ordem judicial que autorizou a busca e apreensão nos endereços ligados aos corréus, tendo a recorrente sido presa em flagrante na ocasião, na posse de uma mochila contendo tabletes de maconha.

Diante do exposto, a dificuldade para a coleta de evidências em ambientes digitais relativas ao uso de aplicativos de mensagens com criptografia de ponta a ponta, se apresenta como elemento crucial no comprometimento da eficácia das investigações de crimes cibernéticos.

Todavia, especificamente no que concerne a prática de cyberbullying, estas dificuldades são substancialmente mitigadas ante seu cometimento ser realizado usualmente por indivíduos conhecidos da vítima. Desta forma, em muitos casos, o próprio conteúdo das mensagens de cyberbullying (como referências a eventos previamente ocorridos envolvendo a vítima) permite a indicação do grupo de indivíduos possivelmente envolvidos no seu envio e compartilhamento, ou mesmo, a indicação individualizada dos autores de cada ato praticado.

3.1.4 Redes Sociais

A investigação de postagens em redes sociais, como Facebook e Instagram, desempenha um papel crucial em casos de cyberbullying, dado o uso extensivo dessas plataformas para a comunicação diária. Desta maneira, para a investigação da prática de cyberbullying nestas plataformas, os investigadores podem acessar postagens que são compartilhadas publicamente sem a necessidade de uma ordem judicial. No entanto, postagens privadas ou protegidas por configurações de privacidade do usuário requerem processos legais mais complexos, em respeito aos direitos a privacidade e proteção de dados digitais dos usuários.

Além disso, as próprias plataformas de redes sociais possuem políticas de resposta a solicitações legais que precisam ser seguidas. Empresas como Facebook e Instagram têm equipes dedicadas a responder a pedidos legais de dados, mas essas solicitações devem ser claramente justificadas e legalmente fundamentadas para serem atendidas. Isso inclui a necessidade de cumprir com as leis de proteção de dados e privacidade, o que pode limitar o tipo de dados que podem ser

---

V - Se ocorreu a busca e apreensão dos aparelhos de telefone celular, não há óbice para se adentrar ao seu conteúdo já armazenado, porquanto necessário ao deslinde do feito, sendo prescindível nova autorização judicial para análise e utilização dos dados neles armazenados.
Recurso ordinário não provido.
(STJ. RHC n. 77.232/SC, relator Ministro Felix Fischer, Quinta Turma, julgado em 3/10/2017, DJe de 16/10/2017.)

compartilhados. Neste contexto, Barreto e Brasil (2016, p. 58) dispõe acerca de tais políticas adotadas pelo Facebook [23].

Uma vez identificada a postagem, a próxima etapa envolve a coleta de evidências. Isso inclui não apenas a postagem em si, mas também metadados associados como a hora da postagem, informações de geolocalização (se disponíveis), e a identificação do autor da postagem. Sobre estes dados necessários para se estabelecer a linha do tempo dos eventos e para vincular atividades digitais a indivíduos específicos, lecionam Barreto e Brasil (2016, p. 59)[24].

A obtenção de acesso a esses dados, especialmente quando são privados, exige ordens judiciais. Os investigadores devem demonstrar a relevância e a necessidade dos dados solicitados para a investigação, e as ordens judiciais devem ser precisas em termos do escopo e da natureza das informações requeridas.

Por sua vez, importante ressaltar que com o advento da Lei Nº 14.811/2024, a utilização das redes sociais para a criação de perfis falsos da vítima objetivando sua humilhação, anteriormente tratada como caracterizadora do crime de Falsa Identidade[25], também constitui cyberbullying.

Neste contexto, uma vez que a criação de perfis falsos para a prática de cyberbullying se apresenta como hipótese de atribuição de falsa identidade para

---

[23] O Facebook possibilita, através da plataforma Law Enforcement Online, a solicitação da preservação de perfis e seus dados sem a necessidade de ordem judicial. O acesso é feito através de, portal este que também é utilizado em casos envolvendo o Instagram. Para ter acesso, é necessário que o solicitante esteja encarregado de uma investigação em andamento. Destaque-se que não será criado um novo perfil da rede social do solicitante, apenas ocorrerá a vinculação de um email institucional ao caso que será aberto no provedor de aplicação, sendo viabilizado o acesso on-line ao grupo Facebook. Em casos de situação de emergência que envolva perigo para uma criança, risco de morte ou danos corporais a qualquer pessoa, as informações serão enviadas de forma mais rápida e efetiva. Nessa situação, não haverá necessidade, em um primeiro momento, de ordem judicial para a obtenção desses dados. Essas solicitações não estão acessíveis ao usuário comum nem repassam dados em casos de litigância em conteúdo civil diretamente ao solicitante.

[24] A plataforma para auxílio às autoridades policiais ainda faz uma diferença entre registros de informações da conta e das que contenham conteúdo de comunicação. Para o primeiro caso, necessita de uma ordem judicial o fornecimento de cabeçalho de mensagens e endereços de IP (logs de acesso com início e fim de cada conexão), além de registros básicos de usuários, tais como: nome completo, endereço, conta de e-mail, telefone registrado em caso de verificação de segunda etapa, dentre outros dados úteis. Quando se tratar de conteúdo de comunicações, em tempo real, incluindo mensagens (conteúdo de mensagens inbox), fotos, vídeos, publicações no mural e informações de localização, a plataforma exige um mandado de busca telemático ou de interceptação telemática para fornecê-lo.
No momento da representação para a expedição de mandado judicial, a autoridade solicitante deverá mostrar a necessidade de constar no respectivo documento a proibição, por parte da empresa de notificação, de ordem judicial ao suspeito, a fim de que a investigação não seja comprometida.

[25] Falsa identidade - Art. 307 - Atribuir-se ou atribuir a terceira falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem:
Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave. (BRASIL, 1940)

causar dano a vítima, o novo tipo penal recrudesceu substancialmente a punição para tal conduta quando praticada para a intimidação sistemática da vítima por constituir crime mais grave do que o de Falsa Identidade, apenado somente com detenção de 3 meses a 1 ano ante a pena cominada de 2 a 4 anos de reclusão para sua prática como cyberbullying.

3.2 DA CARACTERIZAÇÃO DO CYBERBULLYING ANTE O DIREITO À LIBERDADE DE EXPRESSÃO

A liberdade de expressão, consagrada na Lei Maior de 1988, é elemento fundamental que integra o rol de garantias fundamentais constantes em uma sociedade liberal. A liberdade de expressão garante o pleno gozo do direito opinativo, crítico e construtivo da democracia; assim, é este direito que garante a evolução dos dispositivos legais, haja vista que a participação opinativa do povo no processo jurídico e legislativo pátrio é peça-chave para o seu justo funcionamento.

Nesse ínterim, a Constituição Federal de 1988 trata da questão em diversos artigos, quais sejam:

> Art. 5º: Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> [...]
> IV – é livre a manifestação do pensamento, sendo vedado o anonimato
> [...]
> IX – é livre a expressão da atividade intelectual, artística, científica e de comunicação, independente de licença ou censura.
>
> Art. 220. A manifestação do pensamento, criação, a expressão e a informação, sob qualquer forma, processo ou veículo, não sofrerão qualquer restrição, observado o disposto nesta Constituição.
> [...]
> § 2º É vedada toda e qualquer censura de natureza política, ideológica e artística.
> (BRASIL, 1988)

Desta maneira, é possível perceber que existe uma linha tênue entre a livre manifestação do pensamento e da expressão e as afirmações que possam violar a honra, a imagem e demais direitos inerentes dos indivíduos. Eis, portanto, um

complexo assunto debatido pela doutrina e pela jurisprudência e para o qual não parece haver uma resposta única e precisa.

Todavia, ante discursos de ódio em evidente oposição com as demais normas constitucionais que defendem o Estado Democrático de Direito e a dignidade da vida humana como fundamento da própria República Federativa do Brasil iniciou-se o questionamento sobre os limites da liberdade de expressão quando o teor do que se exprime é afrontoso às próprias normas constitucionais.

Ora que, a liberdade de expressão, prevista nos art. 5º, incisos IV e IX, e art. 220, caput e parágrafo 2º, possui contornos para sua mitigação frente à sua colisão com outros direitos constitucionalmente garantidos, uma vez que em razão do caráter principiológico da Constituição todas suas disposições devem ser interpretadas em conjunto, não constituindo cada uma individualmente uma regra absoluta, mas sim um conjunto de princípios coesos.

Desta sorte, não existindo um escalonamento entre normas constitucionais, ou mesmo uma única forma interpretativa e integrativa adequada para a harmonização das diretrizes constitucionais quando da colisão de princípios no caso concreto. Neste sentido, ALEXY (2008) propõe que os princípios possuem dimensões de importância distintos, ou seja, frente ao caso concreto, para o exercício de sopesamento de princípios, não se trata de escolher aleatoriamente qual princípio deve se sobrepor a outro, mas sim estabelecer o grau de importância de determinados princípios em detrimento de outros no caso concreto; o que não implica na declaração de sua invalidade ou na criação de regra especial de exceção, apenas na valoração dos mesmos frente à determinada situação.

Neste contexto, o Supremo Tribunal Federal tem firmado seu entendimento de que a liberdade de expressão não ampara manifestações preconceituosas ou a incitação de violência e intolerância, conforme se observa em julgado de 2003 [26].

---

[26] HABEAS-CORPUS. PUBLICAÇÃO DE LIVROS: ANTI-SEMITISMO. RACISMO. CRIME IMPRESCRITÍVEL. CONCEITUAÇÃO. ABRANGÊNCIA CONSTITUCIONAL. LIBERDADE DE EXPRESSÃO. LIMITES. ORDEM DENEGADA.
1. Escrever, editar, divulgar e comerciar livros "fazendo apologia de ideias preconceituosas e discriminatórias" contra a comunidade judaica (Lei 7716/89, artigo 20, na redação dada pela Lei 8081/90) constitui crime de racismo sujeito às cláusulas de inafiançabilidade e imprescritibilidade (CF, artigo 5º, XLII).
[...]
7. A Constituição Federal de 1988 impôs aos agentes de delitos dessa natureza, pela gravidade e repulsividade da ofensa, a cláusula de imprescritibilidade, para que fique, ad perpetuam rei memoriam, verberado o repúdio e a abjeção da sociedade nacional à sua prática. 8. Racismo. Abrangência. Compatibilização dos conceitos etimológicos, etnológicos, sociológicos, antropológicos ou biológicos,

Desta maneira, uma vez identificado que o conteúdo vinculado se consubstancia como ato de agressão “de modo intencional e repetitivo, sem motivação evidente, por meio de atos de intimidação, de humilhação ou de discriminação” (BRASIL, 1940) característico da prática de cyberbullying, não constituindo mera opinião ou crítica o Poder Judiciário pode e deve adotar medidas visando sua remoção e a punição de seus autores.

Todavia, determinar o que pode ser considerado como manifestação de opinião ou crítica e o que constitui ato de intimidação ou humilhação, não é necessariamente tão óbvio nos casos concretos, de maneira que o estabelecimento de critérios legais ou jurisprudenciais sobre a questão se faz necessário de forma a garantir segurança jurídica.

Neste sentido, merece destaque a decisão do Ministro Luís Roberto Barroso, no julgamento do RESP nº 972-29/MG, ao apresentar uma limitação do conceito de

---

de modo a construir a definição jurídico-constitucional do termo de modo a construir a definição jurídico-constitucional do termo. Interpretação teleológica e sistêmica da Constituição Federal, conjugando fatores e circunstâncias históricas, políticas e sociais que regeram sua formação e aplicação, a fim de obter-se o real sentido e alcance da norma. 7. A Constituição Federal de 1988 impôs aos agentes de delitos dessa natureza, pela gravidade e repulsividade da ofensa, a cláusula de imprescritibilidade, para que fique, ad perpetuam rei memoriam,

9. Direito comparado. A exemplo do Brasil as legislações de países organizados sob a égide do estado moderno de direito democrático igualmente adotam em seu ordenamento legal punições para delitos que estimulem e propaguem segregação racial. Manifestações da Suprema Corte Norte-Americana, da Câmara dos Lordes da Inglaterra e da Corte de Apelação da Califórnia nos Estados Unidos que consagraram entendimento que aplicam sanções àqueles que transgridam as regras de boa convivência social com grupos humanos que simbolizem a prática de racismo.

[...]

11. Explícita conduta do agente responsável pelo agravo revelador de manifesto dolo, baseada na equivocada premissa de que os judeus não só são uma raça, mas, mais do que isso, um segmento racial atávica e geneticamente menor e pernicioso.

12. Discriminação que, no caso, se evidencia como deliberada e dirigida especificamente aos judeus, que configura ato ilícito de prática de racismo, com as consequências gravosas que o acompanham.

13. Liberdade de expressão. Garantia constitucional que não se tem como absoluta. Limites morais e jurídicos. O direito à livre expressão não pode abrigar, em sua abrangência, manifestações de conteúdo imoral que implicam ilicitude penal.

14. As liberdades públicas não são incondicionais, por isso devem ser exercidas de maneira harmônica, observados os limites definidos na própria Constituição Federal (CF, artigo 5º, § 2º, primeira parte). O preceito fundamental de liberdade de expressão não consagra o "direito à incitação ao racismo", dado que um direito individual não pode constituir-se em salvaguarda de condutas ilícitas, como sucede com os delitos contra a honra. Prevalência dos princípios da dignidade da pessoa humana e da igualdade jurídica.

[...]

Ordem denegada.

(STF. HC 82424, Relator(a): MOREIRA ALVES, Relator(a) p/ Acórdão: MAURÍCIO CORRÊA, Tribunal Pleno, julgado em 17/09/2003, DJ 19-03-2004 PP-00024 EMENT VOL-02144-03 PP-00524)

fake news visando garantir e prestigiar o princípio da liberdade de expressão, *in verbis*[27]*.*

Assim, para que uma ação seja caracterizada de fato como uma *fake news* é exigido, pois, que se atente a sua finalidade. No que concerne à intenção de manipular o entendimento geral por meio de alegação manifestamente falsa, tem-se, pois, que não há mais que se falar em liberdade de expressão. Logo, da mesma maneira, finalidade de intimidação, humilhação ou de discriminação da vítima possibilita sua caracterização como prática criminosa de cyberbullying.

[27] [...] para que a liberdade de expressão seja devidamente assegurada, em princípio, não devem ser caracterizados como "fake news": os juízos de valor e opiniões; as informações falsas que resultam de meros equívocos honestos ou incorreções imateriais; as sátiras e paródias; e as notícias veiculadas em tom exaltado e até sensacionalista. Deve-se usar o conceito de "fake news" para o conteúdo manifestamente falso que é intencionalmente criado e divulgado para o fim de enganar e prejudicar terceiros, causar dano, ou para lucro.
(TSE. Recurso Especial Eleitoral Nº 97229, Acórdão, Min. Luís Roberto Barroso, Publicação: DJE - Diário de Justiça Eletrônico, 26/08/2019)

CONSIDERAÇÕES FINAIS

A internet, que começou como um projeto militar na década de 1960, transformou-se em uma ferramenta essencial para a vida cotidiana, transformando profundamente a sociedade com a criação de novas formas de interação e comunicação. Todavia, este avanço tecnológico também suscitou novas realidades que impactam diretamente o Direito Penal com o surgimento de novos tipos de crimes e bens jurídicos nesse ambiente virtual. Ademais, a internet também se tornou um meio para a prática de delitos já existentes que quando cometidos virtualmente se apresentam como mais danosos, em razão da capacidade de anonimato e rápida disseminação de informações que o ambiente virtual proporciona a exemplo do cyberbullying.

O fenômeno do bullying, caracterizado pela intimidação sistemática e persistente de uma vítima através de agressões físicas, verbais ou psicológicas, é um problema amplamente reconhecido, especialmente em ambientes escolares. O cyberbullying, por sua vez, emerge como uma forma mais grave dessa violência, pois transcende as barreiras físicas e temporais, expondo a vítima a ataques constantes e muitas vezes anônimos, com a permanência dos registros online e a possibilidade de viralização do conteúdo ofensivo intensificando os danos psicológicos e emocionais das vítimas.

Ao longo das últimas décadas, o aumento das denúncias e a maior visibilidade desses problemas levaram à criação de normas específicas para a sua prevenção e combate; como a instituição do Programa de Combate à Intimidação Sistemática (*Bullying*), por meio da Lei Nº 13.185/2015, e a inclusão, pela Lei Nº 13.663/2018, da promoção de medidas de conscientização, prevenção e combate ao bullying entre as incumbências dos estabelecimentos de ensino.

Por sua vez, o reconhecimento dos efeitos danosos do bullying e, inobstante a adoção destas medidas preventivas, da reticência por parte de uma quantidade significativa de indivíduos em sua prática; levou a tipificação da prática do bullying no ordenamento jurídico brasileiro com a introdução do crime de Intimidação Sistemática ao Código Penal pela Lei Nº 14.811/2024.

Neste contexto, como decorrência da gravidade exacerbada dos danos advindos da prática do bullying na internet, a previsão de punição substancialmente mais severa para a prática da intimidação sistemática virtual, ou seja, do cyberbullying,

representa um avanço significativo na proteção das vítimas. Contudo, a legislação atual ainda enfrenta desafios consideráveis em sua aplicação prática.

A responsabilização penal dos pais por sua omissão em obstar a prática do bullying virtual por seus filhos menores mostra-se um mecanismo viável e necessário para a prevenção e repressão do cyberbullying. A atuação dos pais, ao exercerem controle sobre o uso de dispositivos de comunicação no ambiente doméstico é crucial para a mitigação desse problema e se apresenta como medida perfeitamente exigível frente aos deveres de proteção, vigilância e educação impostos aos mesmos em decorrência do poder familiar.

A investigação de crimes cibernéticos esbarra na defasagem tecnológica dos órgãos de segurança pública e nas barreiras impostas pela criptografia de ponta a ponta utilizada em muitos aplicativos de comunicação. Estes obstáculos tornam a coleta de provas mais complexa e dificultam a identificação e responsabilização dos agressores, esbarrando em questões atinentes à proteção de dados pessoais e à privacidade.

Além disso, é fundamental a atuação conjunta de diversas áreas do conhecimento para compreender e combater eficazmente o cyberbullying. Psicólogos, educadores, juristas e profissionais de tecnologia precisam trabalhar em conjunto para desenvolver estratégias de prevenção, conscientização e intervenção que possam ser aplicadas de maneira eficaz em diferentes contextos sociais e educacionais de maneira a sedimentar doutrinária e jurisprudencialmente uma distinção clara entre as práticas em ambientes virtuais que caracterizam o bullying daquelas que constituem manifestações opinativas e críticas emanadas no exercício do direito fundamental à liberdade de expressão.

REFERÊNCIAS

ABREU, Karen Cristina Kraemer**.** História e usos da Internet. **Biblioteca On-line de Ciências da Comunicação**, v. 2009, p. 01-09, 2009.Disponível em: <http://www.bocc.ubi.pt/pag/abreu-karen-historia-e-usos-da-internet.pdf>. Acesso em: 18/05/2024.

ALEXY, Robert. **Teoria dos direitos fundamentais**. Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros, 2008.

ALMEIDA, Juliana Evangelista de. **Testamento Digital**: como se dá a sucessão dos bens digitais [recurso eletrônico]. Porto Alegre: Editora Fi, 2019.

ALVES, Andreia Filipa de Melo. **Cyberbullying**: a linguagem como expressão de fenómeno. Dissertação (Mestrado em Psicologia). Universidade de Lisboa. Lisboa, 2017. Disponível em: < https://repositorio.ul.pt/bitstream/10451/33562/1/ulfpie052914_tm.pdf> Acesso em: 18/05/2024.

BACCIOTTI. Karina Joelma. **Direitos humanos e novas tecnologias da informação e comunicação**: o acesso à internet como direito humano. Dissertação (mestrado em direito). São Paulo: Pontifícia Universidade Católica de São Paulo, 2014. Disponível em: <https://repositorio.pucsp.br/jspui/bitstream/handle/6578/1/Karina%20Joelma%20Bacciotti.pdf> Acesso em: 18/05/2024.

BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de investigação cibernética**: à luz do marco civil da internet. Rio de Janeiro: Brasport, 2016.

BAUMAN, Sheri. **Cyberbullying**: a Virtual Menace. Paper to be presented at the National Coalition Against Bullying National Conference Melbourne, Australia November 2 – 4, 2007. Disponível em: < https://www.researchgate.net/publication/265937264_Cyberbullying_a_Virtual_Menace> Acesso em: 18/05/2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 18/05/2024.

BRASIL. **Decreto-Lei Nº 2.848**, de 7 de dezembro de 1940.Código Penal. Disponível em: < https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm> Acesso em: 18/05/2024.

BRASIL. **Lei Nº 8.069,** de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em: < https://www.planalto.gov.br/ccivil_03/leis/l8069.htm> Acesso em: 18/05/2024.

BRASIL. **Lei Nº 12.737**, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em: 18/05/2024.

BRASIL. **Lei Nº 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 18/05/2024.

BRASIL. **Lei Nº 13.185**, de 6 de novembro de 2015. Institui o Programa de Combate à Intimidação Sistemática (Bullying). Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13185.htm> Acesso em: 18/05/2024.

BRASIL **Lei Nº 13.663**, de 14 de maio de 2018. Altera o art. 12 da Lei nº 9.394, de 20 de dezembro de 1996, para incluir a promoção de medidas de conscientização, de prevenção e de combate a todos os tipos de violência e a promoção da cultura de paz entre as incumbências dos estabelecimentos de ensino. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13663.htm#:~:text=LEI%20N%C2%BA%2013.663%2C%20DE%2014,incumb%C3%AAncias%20dos%20estabelecimentos%20de%20ensino.> Acesso em: 18/05/2024.

BRASIL. **Lei Nº 14.811**, de 12 de janeiro de 2024. Institui medidas de proteção à criança e ao adolescente contra a violência nos estabelecimentos educacionais ou similares, prevê a Política Nacional de Prevenção e Combate ao Abuso e Exploração Sexual da Criança e do Adolescente e altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), e as Leis nºs 8.072, de 25 de julho de 1990 (Lei dos Crimes Hediondos), e 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente). Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/lei/l14811.htm> Acesso em: 18/05/2024.

BRASIL, Câmara dos Deputados. **Projeto de Lei Nº 4.224/2021**. Institui medidas de proteção à criança e ao adolescente contra violências. Autor: Osmar Terra - MDB/RS. Apresentação: 01/12/2021. Disponível em: < https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2115456&filename=PL%204224/2021> Acesso em: 18/05/2024.

BRASIL, Câmara dos Deputados. **Substitutivo da Comissão de Previdência, Assistência Social, Infância, Adolescência e Família ao Projeto de Lei Nº 4.224/2021.** Relator: Deputado Dr. Zacharias Calil (União/GO). Sala das Comissões, 19 de maio de 2023. Disponível em: < https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2275886&filename=SBT%201%20CPASF%20=%3E%20PL%204224/2021> Acesso em: 18/05/2024.

BRASIL, Comissão de Constituição e Justiça e de Cidadania (CCJC). **Parecer da Comissão**: Proposta de Emenda à Constituição Nº 47, de 2021. Brasília, 20 de junho de 2023. Disponível em: < https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2292846&filename=PAR+1+CCJC+%3D%3E+PEC+47/2021+%28Fase+1+-+CD%29> Acesso em: 18/05/2024.

BRASIL, Comitê Gestor da Internet no Brasil. **Nota conjunta do Ministério da Ciência e Tecnologia e Ministério das Comunicações (maio de 1995)**. 15 de maio de 2015.Disponível em: < https://www.cgi.br/legislacao/notas/nota-conjunta-mct-mc-maio-1995> Acesso em: 18/05/2024.

BRASIL, Senado Federal. **Proposta de Emenda à Constituição Nº 47/2021**. Acrescenta o inciso LXXX ao art. 5º da Constituição Federal para introduzir a inclusão digital no rol de direitos fundamentais. Disponível em: < https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2183047&filename=PEC%2047/2021%20(Fase%201%20-%20CD)> Acesso em: 18/05/2024.

CARVALHO, Juliano Maurício de. A política de implantação da Internet no Brasil. **Revista de Comunicação Social Publicidade e Propaganda**, Valinhos-SP, v. III, p. 74-97, 2000. Disponível em: < https://www.academia.edu/12865060/A_pol%C3%ADtica_de_implanta%C3%A7%C3%A3o_da_Internet_no_Brasil> Acesso em: 18/05/2024.

CASTELLS, Manuel. **A Sociedade em Rede.** Volume I. São Paulo: Paz e Terra, 1999.

CNJ. **Bullying Cartilha 2016**: Projeto Justiça nas Escolas.3ª ed. Brasília/DF, 2016. Disponível em: < https://bibliotecadigital.cnj.jus.br/jspui/bitstream/123456789/362/1/Bullying%20-%20Projeto%20Justi%C3%A7a%20nas%20Escolas.pdf> Acesso em: 18/05/2024.

CUCCI, Gisele Paschoal; CUCCI, Fábio Augusto. A Proteção Integral de Crianças e Adolescentes Como Dever Social da Família, da Sociedade e do Estado. **Revista de Ciências Jurídicas e Empresariais**, *[S. l.]*, v. 12, n. 2, 2015. Disponível em: <https://revistajuridicas.pgsscogna.com.br/juridicas/article/view/910> Acesso em: 18/05/2024.

CURY, Munir. **Estatuto da criança e do adolescente comentado**: Comentários jurídicos e sociais. 7ª ed. São Paulo: Malheiros, 2005.

GARCIA, Jardel Lucas. **Ressignificando o conceito de presencialidade**: o conceito de metaverso e suas potencialidades. In: GARCIA et. al. COMBINE: Pessoas, Virtualidade e Finanças. Porto Alegre: Faculdade CMB, 2021.

GARCIA, Rebeca. Marco civil da internet no Brasil: repercussões e perspectivas. **Revista dos Tribunais**. São Paulo, n. 964, fev. 2016. Disponível em: < https://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RTrib_n.964.06.PDF>. Acesso em: 18/05/2024.

GODOY, Fernando. **Metaverso**. São Paulo: Buzz, 2022.

ISTO É DINHEIRO. Número de usuários de Internet no mundo chega aos 4,66 bilhões. **Isto é Dinheiro**. Publicado em:03/03/2021. Disponível em: https://www.istoedinheiro.com.br/numero-de-usuarios-de-internet-no-mundo-chega-aos-466-bilhoes/ . Acesso em: 18/05/2024.

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

KUNRATH, Josefa Cristina Tomaz Martins. **A expansão da criminalidade no ciberespaço**: desafios de uma política criminal de prevenção ao cibercrime. Mestrado Profissional em Segurança Pública, Justiça e Cidadania/UFBA. Salvador/BA, 2014. (Dissertação de Mestrado). Disponível em: < http://www.progesp.ufba.br/sites/progesp.ufba.br/files/dissertacao-final-josefa-cristina-tomaz-martins-kunrath-2014.pdf> Acesso em: 18/05/2024.

LINS, Bernardo Felipe Estellita. A evolução da Internet: uma perspectiva histórica. **Cadernos ASLEGIS.** Brasília, n. 48, p. 11-46, jan./abr. 2013. Disponível em: https://www.belins.eng.br/ac01/papers/aslegis48_art01_hist_internet.pdf. Acesso em: 18/05/2024.

MADALENO, Rolf. **Direito de Família**. 10ª ed. Rio de Janeiro: Forense, 2020.

MANDEL, Arnaldo e SIMON, Imre e DELYRA, Jorge Lacerda. **Informação: computação e comunicação**. Revista USP, v. 35, p. 10-45, nov. 1997. Disponível em:< https://revistas.usp.br/revusp/article/view/26865/28646>. Acesso em: 18/05/2024.

MARMELSTEIN, George. **Curso de Direitos Fundamentais**. São Paulo: Atlas, 2008.

MPF. **Crimes cibernéticos**: Manual Prático de Investigação. Procuradoria da República no Estado de São Paulo, Grupo de Combate aos Crimes Cibernéticos. Abril de 2006. Disponível em: <https://www2.mppa.mp.br/sistemas/gcsubsites/upload/60/ManuaL%20Pr%C3%83%C2%A1tico%20de%20Investiga%C3%83%C2%A7%C3%83%C2%A3o%20sobre%20Crimes%20de%20Inform%C3%83%C2%A1tica.PDF> Acesso em: 18/05/2024.

NUCCI, Guilherme de Souza. **Manual de Direito Penal**. 17ª ed. Rio de Janeiro: Grupo GEN, 2021. E-book.

PEREIRA, Ricardo Alexandre. **Como combater o bullying na sua escola**: guia para educadores e gestores. Curitiba: Instituto Federal do Paraná, 2019. Disponível em: < https://educapes.capes.gov.br/bitstream/capes/564663/2/Produto%20Educacional_PROFEPT_Ricardo.pdf> Acesso em: 18/05/2024.

PINHEIRO, Patrícia Peck. **Direito digital**. 7ª ed. São Paulo: Saraiva Educação, 2021.

QATTAN, Mohammed. **Metaverso**: O Futuro da Internet -Tudo o que você precisa saber. E-book. Mohammed Qattan, 2022.

RASSI, João Daniel. **Imputação das ações neutras e o dever de solidariedade no direito penal brasileiro**. 2012. Tese (Doutorado em Direito). Departamento de Direito Penal, medicina forense e criminologia da Faculdade de Direito da Universidade de São Paulo. Disponível em: < https://www.teses.usp.br/teses/disponiveis/2/2136/tde-07062013-152131/publico/Joao_Daniel_Rassi_Doutorado_2012_Versao_completa.pdf> Acesso em: 18/05/2024.

RECEITA FEDERAL DO BRASIL. **Instrução Normativa RFB nº 1888**, de 03 de maio de 2019. Institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil (RFB). Secretaria da Receita Federal do Brasil. Brasília, Diário Oficial da União, 07 de maio de 2019, seção 1, página 14. Disponível em: http://normas.receita.fazenda.gov.br. Acesso em: 18/05/2024.

ROSA, Fabrízio. **Crimes de Informática**. 2ª ed. Campinas: Bookseller, 2005.

SANTOS, Erik. O fenômeno bullying e os direitos humanos. **Revista de Direito Educacional**. Vol. 3, p. 51-108, Jan/Jun 2011. São Paulo: Revista dos Tribunais, 2011.

SILVA, Ana Beatriz Barbosa. **Bullying**: mentes perigosas nas escolas. 2ª ed. São Paulo: Globo, 2015.

SLONJE, Robert; SMITH, Peter K. Cyberbullying: Another main type of bullying? **Scandinavian Journal of Psychology**, V.49; Abril, 2008. 147-154. Disponível em: <https://www.researchgate.net/publication/5499414_Cyberbullying_Another_main_type_of_bullying> Acesso em: 18/05/2024.

SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Marco civil da internet**: construção e aplicação. Juiz de Fora: Editar Editora Associada Ltda., 2016.

TSE. **Recurso Especial Eleitoral nº 972-29/MG**. Relator: Min. Luís Roberto Barroso. Julgado em: 28/05/2019. Publicado em: DJe 26/08/2019. Disponível em: <

https://inter03.tse.jus.br/sjur-pesquisa/pesquisa/actionBRSSearchServers.do?tribunal=TSE&livre=97229. Acesso em: 18/05/2024.

STF. **Habeas Corpus 82424**. Relator: Moreira Alves, Relator p/ Acórdão: Maurício Corrêa, Tribunal Pleno. Julgado em 17/09/2003, DJ 19-03-2004 PP-00024 EMENT VOL-02144-03 PP-00524. Disponível em: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=79052> Acesso em: 18/05/2024.

STJ. **Recurso Ordinário em Habeas Corpus 77.232/SC**. Relator: Ministro Felix Fischer, Quinta Turma. Julgado em: 03/10/2017. Publicado em: DJe de 16/10/2017. Disponível em: <https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201602706592&dt_publicacao=16/10/2017> Acesso em: 18/05/2024.

TJ-DF. **Acórdão 946381, Apelação Civil 20150610117859**. Relator: Gilberto Pereira de Oliveira. Relator Designado: Fátima Rafael, 3ª Turma Cível. Julgado em: 01/06/2016. Publicado em: DJE Pág. 272/287, 10/06/2016. Disponível em: <https://pesquisajuris.tjdft.jus.br/IndexadorAcordaos-web/sistj?visaoId=tjdf.sistj.acordaoeletronico.buscaindexada.apresentacao.VisaoBuscaAcordao&controladorId=tjdf.sistj.acordaoeletronico.buscaindexada.apresentacao.ControladorBuscaAcordao&visaoAnterior=tjdf.sistj.acordaoeletronico.buscaindexada.apresentacao.VisaoBuscaAcordao&nomeDaPagina=resultado&comando=abrirDadosDoAcordao&enderecoDoServlet=sistj&historicoDePaginas=buscaLivre&quantidadeDeRegistros=20&baseSelecionada=BASE_ACORDAOS&numeroDaUltimaPagina=1&buscaIndexada=1&mostrarPaginaSelecaoTipoResultado=false&totalHits=1&internet=1&numeroDoDocumento=946381> Acesso em: 18/05/2024.

TJ-RO. **Apelação Cível, Processo nº 1011349-66.2006.822.0007**. Relator: Juiz Edenir Sebastião A. da Rosa, 2ª Câmara Cível. Julgado em: 20/08/2008. Publicado em: Diário Oficial, 19/09/2008. Disponível em: <https://webapp.tjro.jus.br/juris/consulta/detalhesJuris.jsf?cid=2> Acesso em: 18/05/2024.

TURNER, David; MUÑOZ, Jesus. **Para os filhos dos filhos de nossos filhos:** uma visão da sociedade internet. 2ª ed. São Paulo: Summus Editorial, 1999.

UNESCO. **Violência escolar e bullying**: relatório sobre a situação mundial. Título original: School violence and bullying: global status report. Brasília: UNESCO, 2019. Disponível em: < https://unesdoc.unesco.org/ark:/48223/pf0000368092> Acesso em: 18/05/2024.

VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos.** Belo Horizonte: Fórum, 2013.