XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO III

MAIQUEL ÂNGELO DEZORDI WERMUTH

DENISE NEVES ABADE

D597

Direito penal, processo penal e constituição III[Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Maiquel Ângelo Dezordi Wermuth, Denise Neves Abade – Florianópolis: CONPEDI, 2025.

Inclui bibliografia
ISBN: 978-65-5274-318-3
Modo de acesso: www.conpedi.org.br em publicações
Tema: Os Caminhos Da Internacionalização E O Futuro Do Direito

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito penal. 3. Processo penal. XXXII Congresso Nacional do CONPEDI São Paulo - SP (4: 2025: Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO III

Apresentação

A presente obra reúne a produção científica apresentada no Grupo de Trabalho Direito Penal, Processo Penal e Constituição III, realizado no âmbito do XXXII Congresso Nacional do CONPEDI, em São Paulo, no dia 27 de novembro. Inseridos em um espaço de reflexão crítico-acadêmica de alta densidade teórica, os textos aqui compilados evidenciam o vigor das discussões contemporâneas sobre o sistema penal brasileiro, articulando análises dogmáticas, constitucionais e político-criminológicas. Ao congregar pesquisas que dialogam com metodologias diversas e com a literatura especializada nacional e internacional, a coletânea reafirma o papel do CONPEDI como locus de produção de conhecimento avançado e de circulação de debates capazes de tensionar paradigmas tradicionais, fomentar perspectivas inovadoras e contribuir para a consolidação de um pensamento jurídico comprometido com os direitos fundamentais e com o aprimoramento das instituições democráticas.

O estudo de Idir Canzi, Yonatan Carlos Maier e Lucas Stobe oferece uma leitura tecnicamente consistente do problema das condenações de inocentes, articulando a análise empírica dos erros judiciais com a Teoria do Ordenamento Jurídico de Norberto Bobbio. A principal contribuição reside na demonstração de que a incoerência sistêmica é estrutural, decorrente tanto do uso inadequado dos procedimentos de reconhecimento quanto da persistência de traços inquisitórios. A interação entre coerência normativa, presunção de inocência e limites epistemológicos do processo penal reforça a necessidade de abordagens sistêmicas para enfrentar injustiças penais.

O trabalho de Paulo Hideki Ito Takayasu e Sérgio Tibiriçá Amaral, ao examinar a constitucionalidade e a eficácia do Cadastro Nacional de Predadores Sexuais, situa-se na interface entre política criminal simbólica e tutela de direitos fundamentais. A comparação com a Lei de Megan evidencia a fragilidade de soluções baseadas em exposição pública, revelando déficits de eficiência e riscos de violação à presunção de inocência. A análise qualitativa e quantitativa demonstra baixa operacionalização da medida e potencial de gerar condenações sociais irreversíveis, indicando a urgência de políticas baseadas em evidências.

Já o estudo de Dierik Fernando de Souza, Danilo Rinaldi dos Santos Jr. e Dêivid Barbosa dos Santos Neves retoma a tensão entre verdade e legalidade no processo penal, aprofundando a aplicação da Teoria dos Frutos da Árvore Envenenada. A discussão das exceções

jurisprudenciais evidencia que a teoria só se mantém como garantia efetiva se forem evitadas flexibilizações que subordinem a legalidade à busca pela verdade. O trabalho contribui ao debate sobre limites epistêmicos da prova e racionalidade do modelo garantista.

A análise crítica realizada por Antonio Henrique da Silva sobre as condenações proferidas pelo Supremo Tribunal Federal nos eventos de 8 de janeiro de 2023 introduz o conceito de humildade judicial como ferramenta hermenêutica e de autocontenção. O exame das dosimetrias demonstra que, embora não haja exacerbação punitiva evidente, persistem inconsistências decorrentes da ausência de critérios objetivos na pena-base. O estudo oferece contribuição relevante ao debate sobre proporcionalidade sancionatória e transparência decisória no âmbito das cortes constitucionais.

No trabalho de André Giovane de Castro, o monitoramento eletrônico é analisado a partir de uma perspectiva que reconhece o caráter jurídico-político das decisões judiciais. A pesquisa, apoiada em método quali-quantitativo, evidencia a coexistência de feições autoritárias e democráticas nas decisões do Tribunal de Justiça do Rio Grande do Sul, destacando a necessidade de que os direitos humanos funcionem como bússola interpretativa para a formação da decisão judicial em um Estado Democrático de Direito.

O estudo de Tamíris Rosa Monteiro de Castro sobre a Teoria da Co-culpabilidade revisita um dos debates mais complexos da dogmática penal: a possibilidade de considerar a omissão estatal como fator redutor de culpabilidade. A análise constitucional e dogmática demonstra como variáveis estruturais – desigualdade, marginalização e exclusão social – ainda encontram resistência jurisprudencial para ingressar na teoria do delito, indicando a urgência de uma leitura material do princípio da igualdade.

A pesquisa de Lucas Guedes Ferreira de Brito e Fausy Vieira Salomão sobre o sistema prisional de Frutal-MG articula investigação documental, bibliográfica e empírica in loco. A análise da superlotação, das deficiências estruturais e da localização inadequada do presídio evidencia os impactos diretos sobre a dignidade dos presos, a segurança da comunidade e a eficácia das políticas de ressocialização. A perspectiva de um novo presídio surge como alternativa, mas também como convite a reflexões sobre planejamento carcerário e direitos fundamentais.

O artigo de Fabrício Veiga Costa, Karoliny de Cássia Faria e Matheus Castro de Paula enfatiza a indispensabilidade do contraditório técnico na prova pericial, inclusive na fase investigativa. Ao evidenciar a assimetria entre acusação e defesa no inquérito policial, o trabalho consolida a importância de um modelo garantista de produção probatória, no qual a

formulação de quesitos, o acompanhamento técnico e a crítica ao laudo são condições para a concretização do devido processo legal.

Por fim, a investigação de Antonio Carlos da Ponte e Eduardo Luiz Michelan Campana sobre regulação das redes sociais e crimes cibernéticos contra crianças e adolescentes apresenta uma leitura abrangente da arquitetura digital contemporânea, dos tipos penais aplicáveis e dos possíveis modelos regulatórios. A proposta de critérios objetivos para orientar tanto a legislação quanto a jurisdição constitucional e a autorregulação das plataformas contribui de modo inovador ao debate sobre proteção integral em ambientes digitais.

O trabalho de Rodrigo Gomes Teixeira introduz uma discussão sobre a interculturalidade e seus impactos na teoria do delito, ao defender a possibilidade de ausência de ação penalmente relevante em casos de descontextualização cultural absoluta. Fundamentado em uma concepção significativa da ação e em um paradigma discursivo inclusivo, o estudo evidencia a necessidade de um direito penal intercultural que reconheça projetos de vida diversos e experiências etnoculturais historicamente condicionadas. A abordagem sobre performatividade, ação significativa e diversidade cultural explicita que a dogmática penal deve dialogar com parâmetros constitucionais pluralistas, permitindo a identificação de situações nas quais a imputação penal não se justifica diante da ruptura completa entre o ato praticado e o horizonte cultural do agente. Trata-se de uma contribuição de elevada densidade teórica ao debate sobre pluralismo, limites da culpabilidade e reconhecimento das diferenças em um Estado Democrático de Direito.

O texto de Gustavo Ribeiro Gomes Brito enfrenta com precisão analítica o debate sobre o princípio da insignificância na lavagem de capitais, campo marcado por forte expansão legislativa e por tensões conceituais em torno do bem jurídico protegido. Seu estudo historiciza o fenômeno, reconstrói as narrativas de legitimação penal e problematiza a pertinência de juízos de tipicidade material em crimes econômicos, especialmente em sociedades de risco. A investigação, ancorada na literatura especializada nacional e estrangeira, ilumina a complexidade do tema e demonstra que a discussão sobre a insignificância, longe de trivial, demanda compreensão sofisticada da função político-criminal da lavagem de capitais.

O artigo de Alan Stafforti, Juliana Oliveira Sobieski e Rômulo Moreira da Silva projeta um debate essencial sobre tecnologia, liberdade e justiça, ao examinar criticamente a proposta de utilização de NFTs no sistema prisional. Fundamentado na Lei Geral de Proteção de Dados e na teoria das capacidades de Amartya Sen, o estudo evidencia que a introdução acrítica de inovações digitais em ambientes de vulnerabilidade pode produzir reforço de estigmas, riscos

discriminatórios e violações estruturais de direitos fundamentais. O histórico comparado e as referências a experiências distópicas indicam a necessidade de prudência regulatória e de um olhar ético-humanista acerca das finalidades do sistema penal, cujo horizonte constitucional é a ampliação de liberdades, e não o aprofundamento de desigualdades.

Itzhak Zeitune Oliveira e Silva, por sua vez, oferece uma reflexão aprofundada sobre o estado de coisas inconstitucional reconhecido pelo Supremo Tribunal Federal na ADPF 347, conectando-o a teorias de políticas públicas estruturais e a experiências estrangeiras, especialmente a colombiana. O autor demonstra como a crise prisional brasileira exige soluções sistêmicas, superando a lógica casuística e convocando o Judiciário, o Executivo, o Legislativo e a sociedade civil para um processo colaborativo de reconstrução institucional. Ao situar medidas como as audiências de custódia, a Súmula Vinculante 56 e o HC coletivo 143.641 no contexto de transformações estruturais, o trabalho revela a urgência de políticas de desencarceramento e de afirmação dos direitos humanos como vetores de contorno do punitivismo.

O artigo de Thiago Allisson Cardoso de Jesus, Igor Costa Gomes e Guilherme da Silveira Botega analisa a proposta de tipificação do ecocídio no PL n. 2933/2023, destacando sua relevância como resposta penal à destruição ambiental em larga escala. Ao examinar os fundamentos jurídicos e político-criminais da criação de um tipo penal específico, o estudo evidencia a necessidade de instrumentos normativos capazes de enfrentar danos ambientais graves e irreversíveis, reforçando a centralidade da tutela ambiental no Estado Democrático de Direito.

No campo da epistemologia jurídica, a contribuição de Ana Clara Vasques Gimenez e Vitor Rorato analisa com rigor científico a fragilidade da prova testemunhal diante dos limites cognitivos da memória humana. A partir de aportes da psicologia do testemunho, expõem como processos de esquecimento, reconsolidação e sugestibilidade alteram a confiabilidade dos relatos, especialmente quando colhidos tardiamente. O trabalho situa-se em sintonia com a literatura internacional que critica práticas forenses baseadas em intuições não científicas e propõe reformas procedimentais capazes de qualificar a valoração probatória e oferecer maior racionalidade às decisões judiciais.

Por fim, o estudo de Maiza Silva Santos sobre advocacia e lavagem de dinheiro apresenta um panorama internacional robusto, mapeando tensões entre sigilo profissional e deveres de colaboração na prevenção a crimes financeiros. Seu exame comparado — que envolve sistemas jurídicos como o norte-americano, britânico, francês, alemão, italiano e espanhol — permite compreender diferentes modelos de regulação e seus impactos sobre a função

essencial da advocacia. A análise do caso Michaud versus França, articulada à atuação do GAFI/FATF e da Rede Egmont, demonstra que o equilíbrio entre proteção do direito de defesa e mecanismos de compliance é tema central da política criminal contemporânea, exigindo parâmetros de proporcionalidade e garantias institucionais para evitar a erosão de direitos fundamentais.

Os trabalhos, em conjunto, evidenciam uma agenda de pesquisa comprometida com a racionalidade penal, com a centralidade dos direitos fundamentais e com o aperfeiçoamento das instituições do sistema de justiça a partir de metodologias robustas e sensibilidade democrática.

Desejamos uma ótima leitura a todos e todas que tiverem o privilégio de acessar estes anais!

São Paulo, 27 de novembro de 2025.

Maiquel Ângelo Dezordi Wermuth

Denise Neves Abade

REGULAÇÃO DAS REDES SOCIAIS E CRIMES CIBERNÉTICOS CONTRA CRIANÇAS E ADOLESCENTES

REGULATION OF SOCIAL NETWORKS AND CYBERCRIMES AGAINST CHILDREN AND ADOLESCENTS

Antonio Carlos da Ponte
Eduardo Luiz Michelan Campana

Resumo

Resumo. A presente investigação se inicia com a constatação de o surgimento e a expansão da internet democratizaram a veiculação de ideias, reduziu os custos de transmissão, apropriação e modificação de informação, sendo que as redes sociais se destacam, oferecendo ferramentas tais que facilitam e incentivam ainda mais a publicação e o compartilhamento de conteúdo, permitindo que os usuários construam conexões sociais com outros grupos ou indivíduos. Após esclarecimentos terminológicos, necessários para a compreensão de determinados fenômenos socialmente danosos e criminosos que encontram terreno fértil para a sua propagação através das redes sociais, atingindo principalmente crianças e adolescentes anos, discutem-se os modelos e critérios de sua regulação. Identificam-se os crimes cibernéticos contra menores de 18 anos previstos na Lei n. 8.069 /1990 e no Código Penal. Propõe-se a eleição de um parâmetro seguro e objetivamente sindicável no contexto de uma regulação normativa, de uma interpretação através do exercício da jurisdição constitucional, ou por meio de uma autorregulamentação pelas próprias plataformas digitais.

Palavras-chave: Redes sociais, Regulação, Crimes cibernéticos, Tutela penal da criança e do adolescente, Internet

Abstract/Resumen/Résumé

Abstract. This investigation begins by observing that the emergence and expansion of the Internet have democratized the dissemination of ideas while reducing the costs associated with transmitting, appropriating, and modifying information. Social networks stand out for providing tools that facilitate and further stimulate the publication and sharing of content, allowing users to build social connections with groups or individuals. The paper proceeds by clarifying key terminology to understand certain socially harmful and criminal phenomena that proliferate on social networks - primarily impacting children and adolescents. It then examines the models and criteria for regulating these phenomena. Furthermore, the study aims to identify cybercrimes committed against minors, as provided for in Law No. 8,069 /1990 and the Penal Code. Ultimately, the objective is to propose a safe and objectively reviewable parameter within the context of normative regulation, an interpretation through constitutional jurisdiction, or self-regulation by the digital platforms themselves.

Keywords/Palabras-claves/Mots-clés: Social networks, Regulation, Cybercrimes, Criminal protection of children and adolescents, Internet

1 Introdução

Um dos temas mais cadentes atualmente é a regulação das redes sociais. O presente trabalho visa inicialmente estudar o uso ilícito da internet como fator desencadeante de comportamentos criminosos nos meios digitais. Para tanto, debruça-se sobre as particularidades da rede mundial de computadores e acerca da distinção entre os provedores de serviço em provedores de conexão e de aplicação. Após esclarecimentos terminológicos, necessários para a compreensão de determinados fenômenos socialmente danosos e criminosos que encontram terreno fértil para a sua propagação através das redes sociais, atingindo principalmente vítimas menores de 18 anos, discutem-se os modelos e critérios de sua regulamentação, definindo-se os crimes cibernéticos. Em seguida, são identificados os delitos desta natureza, contra crianças e adolescentes, que estão previstos na Lei n. 8.069/1990 e no Código Penal, dentro da proposta de eleição de um parâmetro seguro e objetivamente sindicável no contexto de uma regulação normativa, de interpretação através do exercício da jurisdição constitucional, ou por meio de uma autorregulamentação pelas próprias plataformas digitais.

2 Redes Sociais e a criminalidade na internet

2.1 O uso ilícito da internet como fator criminógeno

A internet tornou-se, na década de 1990, mais acessível e popular, ao mesmo tempo em que a digitalização se difundiu rapidamente no mundo privado e profissional, sendo que, hodiernamente, são os próprios usuários que geram conteúdos e os divulgam na rede mundial de computadores, fenômeno conhecido como “Web 2.0”, relevando-se como particularmente populares as “redes sociais”, através das quais pessoas com os mesmos interesses podem se comunicar e trocar dados acerca de qualquer assunto entre si (Hilgendorf, 2020, p. 133-134).

Com efeito, o surgimento e a expansão da internet deram azo a toda uma infraestrutura que democratizou a veiculação de ideias, reduziu os custos de transmissão, apropriação e modificação de informação, acarretando uma descentralização do controle dos meios de comunicação, para além de permitir que o conteúdo produzido pelos usuários transpusesse fronteiras geográficas e culturais, possibilitando “uma quantidade muito maior de interações entre indivíduos e grupos espalhados ao redor do mundo” (Salvador, 2023, p. 56).

Conforme ainda observa João Pedro Favaretto Salvador, as plataformas de redes sociais se destacam, nesse cenário, entre outros intermediários da comunicação digital, eis que

oferecem ferramentas tais que facilitam e incentivam ainda mais a publicação e o compartilhamento de conteúdo, constituindo o seu principal objetivo permitir que os usuários construam conexões sociais com outros grupos ou indivíduos, de tal forma que elas "são plataformas porque propagam a voz de seus usuários e são redes sociais porque mediam, promovem e geram interações sociais" (2023, p. 56-57).

Alerta Eric Hilgendorf que, com as redes sociais, os mundos *online* e *offline* se fundem, e, por essa razão, "surgem muitos comportamentos socialmente danosos e criminosos", ao que se acrescentam significativos problemas para a tipificação de condutas e de aplicação do direito penal causados pelo contínuo desenvolvimento da internet, quais sejam, a ubiquidade de publicações, a velocidade de transferência de informações, a permanência de conteúdos, a interculturalidade da rede, sua uniformidade técnica e a fusão com nossa vida cotidiana (2020, p 134-137).

A ubiquidade dos conteúdos é fruto da internacionalidade sem precedentes das publicações de tal forma que o que é publicado na internet está, pelo menos em tese, disponível para o mundo todo, sendo que a superação de fronteiras é a regra e não a exceção. A velocidade de transferência de informação possibilita que o conteúdo inserido na internet se torne disponível, de maneira quase instantânea, no lugar mais longínquo do planeta, desde que ali haja uma conexão com a rede mundial de computadores. A conjugação dessas duas primeiras particularidades acarreta uma velocidade de comunicação que cria a ilusão de uma intimidade, com enorme potencial para ser explorada por criminosos contra vítimas em situações de vulnerabilidade. Por fim, "a rede global de informações não esquece quase nada", pois uma vez registrados os conteúdos na internet, somente de lá são excluídos com muito esforço, uma vez que são rapidamente copiados e reiteradamente guardados, daí porque se fala de uma terceira particularidade consistente numa "especial permanência de informações", o que se intensifica com novas formas de armazenamento em "nuvem" (Hilgendorf, 2020, p. 136-137).

Ademais, prossegue o autor, a inédita disponibilidade de informações e conteúdo em todo o mundo, propiciada pela internet, faz com que um número crescente de indivíduos se conecte com comunidades das mais diversas características culturais, fenômeno esse conhecido como "interculturalidade da internet", sendo que essa pluralidade cultural da rede é, por sua vez, confrontada com uma universidade técnica da internet, pois a tecnologia nela empregada é idêntica em todo o mundo e, para além, os *softwares* e *hardwares* utilizados são produzidos por poucas empresas, no mais das vezes sediadas nos EUA (*Big Techs*), cuja influência ultrapassa as fronteiras nacionais. Por fim, a internet se funde com os objetos de nosso mundo privado e profissional, resultado de trânsito de dados não somente entre computadores

controlados pelo usuário, mas também entre objetos de uso cotidiano dotados de sensores e microchips (2020, p. 137-138).

Para o enfrentamento dos desafios que se impõem para o direito penal de *lege lata* e de *lege ferenda*, a internet deve ser pensada levando em conta os intermediários que compõem o seu ecossistema de comunicação, pois a sua infraestrutura exerce somente a função de transmitir informações, enquanto as tarefas mais complexas são exercidas pelos dispositivos conectados, controlados por agentes privados, os denominados provedores de serviço, e, assim, "dificilmente haverá informação circulando na internet que não passe pela infraestrutura de um agente intermediário, controlado por uma pessoa jurídica ou física, pública ou privada" (Salvador, 2023, p. 52).

A Lei n. 12.965/2014, o Marco Civil da Internet, em seu artigo 5º, faz a distinção dos provedores de serviço em provedores de conexão à internet e de aplicações da internet. Nos termos do inciso V do referido dispositivo, os provedores de conexão têm como objeto a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP (*Internet Protocol*), ao passo que o inciso VII considera que os provedores de aplicações consistem no conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet.

Em outras palavras, os provedores de conexão são as empresas de telecomunicações (servidores) que, em escala mundial, nacional ou regional, fornecem o acesso à internet, fixa ou móvel, conectando seus clientes à infraestrutura da rede global, com a atribuição de um endereço de protocolo de controle de transmissão de dados aos seus dispositivos (TCP/IP). Na verdade, a "Web" (*Word Wide Web*) consiste numa forma de acesso às informações através da infraestrutura da internet, utilizando-se dos protocolos HTTP (*Hypertext Transfer Protocol*) ou HTTPS (*Hypertext Transfer Protocol Secure*) para que se possa visualizar as páginas, vinculadas por hyperlinks consistentes em textos, imagens, sons ou multimídias, ou seja, é um dos serviços que funcionam no interior da rede mundial de computadores (Masini Neto, 2025, p. 6-7).

Lado outro, os provedores de aplicação da internet são empresas, indivíduos e organizações do terceiro setor que ofertam variados serviços e funcionalidades, permitindo que usuários recebam e enviem dados para seus servidores, como se verifica com os mecanismos de busca (Google, Bing, Safari, Yahoo), serviços de hospedagem que alugam espaços em seus servidores para aqueles que desejam ter o seu próprio site (Locaweb), sistemas de pagamento (Paypal, PagSeguro, GooglePay), aplicativos de mensageria (Whatsapp, Telegram), portais de

notícias, blogs, fóruns de discussão e as plataformas de redes sociais (Salvador, p. 53). Há ainda plataformas híbridas, que funcionam como rede social e serviço de mensageria (Discord).

No Brasil, conforme o artigo 2º, parágrafo único, da Resolução n. 305/2019 do CNJ, consideram-se como rede social todos os sítios da internet, plataformas digitais e aplicativos de computador ou dispositivo eletrônico móvel voltados à interação pública e social, que possibilitem a comunicação, a criação ou o compartilhamento de mensagens, de arquivos ou de informações de qualquer natureza. As plataformas Facebook, Instagram, X (ex-Twitter), LinkedIn, Tik Tok e Youtube, dentre outras semelhantes, são, portanto, redes sociais, ao permitirem a interação entre os usuários, a criação de perfis, conteúdos e de comunidade de seguidores, possuindo algoritmos que recomendam conteúdos com base nas preferências das pessoas que delas se utilizam, para além de a maioria remunerar os produtores de conteúdo que granjeiam anunciantes, característica essa conhecida por monetização.

Esclarecimentos terminológicos e definições sobre mecanismos da internet, e seu eventual emprego ilícito, são necessários para a real compreensão de fenômenos criminógenos que as plataformas de redes sociais podem acarretar.

Adriana Shimabukuro e Melissa Garcia Blagitz de Abreu e Silva definem a internet profunda (*Deep Web, Deep Net, UnderNet ou Free Net*) como a parte da rede cujo conteúdo não está disponível ou indexado aos principais mecanismos de busca e pesquisa, possuindo "dimensão inimaginável e com crescimento similar ao da Internet Visível", sendo que várias razões fazem com que um determinado conteúdo não seja indexado ou localizado por um mecanismo tradicional de busca e pesquisa, como Google, Bing ou Yahoo, entre as quais a necessidade de senha ou de software específico para acesso, ou ainda bloqueio pelo criador da página (2018, p. 255).

Observam ainda as autoras que, para além das páginas desindexadas, embora acessíveis, a *Deep Web* abarca uma rede mais privativa e anônima, que é denominada *Dark Web*, acessada com softwares específicos destinados para navegação em ambientes criptografados, dentre os quais se destaca o P2P ou i2p (*peer-to-peer*), siglas que designam o Projeto de Internet Invisível, assinalando que parte considerável das publicações na *Dark Web* envolve alguma modalidade de atividade ilícita, citando exemplos de auxílio à produção de material pornográfico infanto-juvenil (2018, p. 255-261). Bem destaca Carla Albuquerque que os criminosos digitais encontram na *Dark Web* o ambiente propício para a proliferação de suas infrações penais, abarcando fóruns de discussão onde o delito é exaltado e crianças e adolescentes são até treinados para o cometimento de atividades ilegais (2025, p. 84-85). Por

óbvio, o conteúdo produzido na *Dark Web* pode, posteriormente, ser introduzido e veiculado nas redes sociais, ou seja, vir à tona na superfície visível da internet.

Claro está que nem todo o instrumental da internet e, mais especificamente, das plataformas de redes sociais, foi criado para propósitos ilícitos, muito pelo contrário, mas é inegável que também incrementou a propagação de conteúdos nocivos, parte considerável deles criminosos, cujo alcance, impacto e lesão a bens jurídicos é assaz potencializado pela quantidade inimaginável de interações entre indivíduos e grupos, principalmente pela replicação das publicações, que podem "viralizar", ainda que inicialmente não fosse essa a intenção do seu autor (Salvador, 2023, p. 58-59).

2.2 Modelos de Regulação e Crimes Cibernéticos contra crianças e adolescentes

No que tange a crianças e adolescentes, o mundo digital proporciona uma fuga da vida real, sujeitando-os, em razão da sua condição peculiar de desenvolvimento e de se encontrarem num período de difícil transição de faixa etária, a uma vulnerabilidade psicológica (Albuquerque, 2025, p. 83), o que os torna alvo da prática de inúmeras infrações penais, dentre as quais crimes cibernéticos relacionados ao abuso sexual infantil.

Particularmente no âmbito da internet visível, destaca-se o advento e a popularização de algoritmos que, utilizados para fins diversos do originalmente pretendido, passaram a possibilitar a manipulação de vídeos e a inserção artificial de rostos e vozes, o que propiciou o surgimento do fenômeno conhecido como *deppfake*, ou seja, uma "montagem ultrarrealista em que o rosto de uma pessoa é sobreposto ao corpo de outra em um vídeo, podendo ainda ser conjugada com manipulação de voz, por intermédio de sistemas de inteligência artificial", o que induz a uma falsa percepção quanto ao participante desse material, uma vez que, em razão de o algoritmo ter sido treinado com diferentes ângulos e microexpressões do rosto humano, e como ele se movimenta, possui a capacidade de replicar com perfeição e transformar o rosto de uma pessoa no de qualquer outra que se pretenda (Rodrigues, 2023, p. 278).

A fabricação de *deepfakes* reveste-se de gravidade ímpar, pois qualquer pessoa pode extrair fotos e vídeos disponibilizados pela vítima em redes sociais e construir uma montagem através do emprego de inteligência artificial, compartilhando na mesma plataforma ou em aplicativos de mensageria (Rodrigues, 2023, p. 285). E não é só. Existem modalidades mais reprováveis, dada a sua perversidade, dessa montagem digital, que são as *fakes* pornográficas envolvendo pessoas adultas ou crianças e adolescentes. As últimas, também conhecidas como *deepfakes* pornográficas infantis, podem ainda submeter o infante à sextorsão, ou seja, "a

utilização de informações, fotos e vídeos de teor sexual para constranger a vítima a fazer algo mediante a ameaça de divulgação do seu conteúdo" (Massini Neto, 2025, p. 46).

Acresçam-se os fenômenos de igual enormidade que encontram terreno fértil nas redes sociais, como as *Fake News*, os delitos e os discursos de ódio, a apologia ao terrorismo, e a violência contra a mulher.

Nesse quadro, João Pedro Favaretto Salvador obtempera que as plataformas de redes sociais não apenas transmitem informações, sem qualquer interferência, entre os seus usuários, chamando a atenção que, com relação aos discursos de ódio, as empresas provedoras de serviços de internet se tornaram protagonistas na regulação desses conteúdos, por senso de responsabilidade corporativa, por pressão externa de agentes públicos ou até por interesse de tornar mais rentáveis os espaços de comunicação (2023, p. 61-62). Pode-se dizer o mesmo no que tange às publicações de similar ou de maior nocividade, havendo uma preocupação mais intensa dos provedores de aplicação quando o conteúdo abarca abuso sexual infantil (*Child Sexual Abuse Material*), pois a maioria das *Bigh Techs* estão sediadas nos Estados Unidos, ficando sujeitas a uma rigorosa legislação federal e estadual sobre essa temática, cuja aplicação é confiada a uma seção específica do Departamento de Justiça americano (*Child Exploitation and Obscenity Section)*.

Assim, essas empresas decidem sobre o conteúdo que circula em suas plataformas não somente de acordo com o que é determinado por autoridades públicas, mas igualmente conforme regras de elaboração própria, através das quais são removidas postagens e se procede ao banimento de usuários sem a necessidade de ordem judicial, sendo que essa atividade de regulação privada, ou autorregulação, é comumente chamada de moderação de conteúdo, a qual visa a adequação do que é publicado pelos usuários aos objetivos e regramento próprios, que se materializam nos termos de usos, padrões da comunidade ou outros documentos assemelhados e que determinam o que consideram manifestações nocivas, o modo pelo qual são identificadas e as providências a serem tomadas, tais como a limitação ou impedimento da sua circulação e a restrição ou suspensão do acesso ao usuário infrator (Salvador, 2023, p. 64-65).

Contudo, esse modelo de autorregulamentação, para além do ponto de tensão com a liberdade de expressão do usuário, pois passível de ser cerceada por um agente privado, tem se mostrado insuficiente frente à multiplicação de produção e divulgação de conteúdos que atentam contra outros direitos fundamentais e lesam bens jurídicos de inegável magnitude.

No Brasil, conforme expõem Maria Celeste Cordeiro Leite dos Santos e Marilena Araújo, para as complexas questões acerca da regulamentação do ambiente digital e o confronto com a liberdade de expressão, vislumbram-se duas respostas, quais sejam, o Projeto de Lei

2.630/2020, conhecido como “PL das Fake News”, e o julgamento pelo Supremo Tribunal Federal, nos Recursos Extraordinários 1.037.396-SP e 1.057.258-MG, ambos dotados de Repercussão Geral, acerca da constitucionalidade do art. 19 da Lei n. 12.965/2014, que exige ordem judicial específica para a responsabilização civil de provedor de aplicações de internet por danos decorrentes de conteúdo gerado por terceiros (2024, p. 27).

No julgamento finalizado em 27 de junho de 2025, o Supremo Tribunal Federal, por maioria de votos, com emprego da técnica da interpretação conforme, reconheceu a parcial e progressiva inconstitucionalidade do mencionado dispositivo do MCI (Tema 533), fixando tese que estipula a responsabilização civil de provedores de aplicações de internet, enquanto não sobrevier nova legislação, sujeitando-os a um regime que impõe às essas plataformas um dever de cuidado, estabelecendo que estas, dentre várias obrigações, devem promover a indisponibilização imediata de conteúdos que configuram crimes graves previstos em rol taxativo, em que se elencam o induzimento, instigação ou auxílio a suicídio ou a automutilação, a pornografia infantil, e crimes graves contra crianças e adolescentes.

Por outro norte, na redação final do Projeto de Lei 2.630/2020, que leva em mira instituir a “Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet”, e, assim, adotar um modelo de regulação normativa, o segundo capítulo objetiva estabelecer a responsabilização dos provedores, os quais, consoante o artigo 11 do texto, caso promulgado o diploma legal, deverão atuar diligentemente para prevenir e mitigar práticas ilícitas no âmbito de seus serviços, envidando esforços para aprimorar o combate a disseminação de conteúdos ilegais gerados por terceiros, que possam configurar infrações penais que elenca, dentre elas crimes contra criança e adolescentes previstos na Lei n. 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente) e de incitação à prática de delitos contra essas vítimas ou apologia de fato criminoso ou autor de crimes contra infantes tipificados no Código Penal.

O projeto de lei aponta para a fixação de critérios para regulação das redes sociais através do direito penal, o qual, no dizer de Carlos María Romeo Casabona (2011, p. 513), enfrenta, nos meios digitais, uma criminalidade, progressivamente, mais poderosa e perigosa, sob muitos pontos de vista, e que exige uma resposta necessária, alertando que:

> “Não se pode esquecer que, mesmo tendo complexidade técnica e jurídica, há o fato de que as construções jurídico-penais (assim como as de outras disciplinas jurídicas), elaboradas ao longo das últimas décadas, nem sempre podem ser adaptadas às características destas tecnologias, nem às manifestações criminais que proporcionam”.

Dessarte, se o conteúdo disponibilizado e divulgado encerra a prática de um delito, é estreme de dúvida que se impõe ao provedor a sua imediata retirada e a suspensão do usuário infrator, sob pena de responsabilização civil ou até mesmo, como adiante se verá, penal. Cuida-se de parâmetro seguro e objetivamente sindicável no contexto de uma regulação normativa, de uma interpretação através do exercício da jurisdição constitucional, ou por meio de uma autorregulamentação pelas próprias redes sociais.

Conforme assinala Eric Hilgendorf, os avanços da tecnologia, ao invés de simplesmente aumentarem nossas opções de ações e, desse modo, nos ajudarem a configurar o mundo e a nós mesmos segundo nossas compreensões, nos causam também efeitos colaterais e contrários aos nossos desejos e interesses, o que levanta a questão sobre o controle do desenvolvimento tecnológico num Estado Democrático Constitucional. Para o autor, é o parlamento que deveria confrontar com as questões essenciais do desenvolvimento tecnológico, o que levante notáveis problemas no que tange à regulação da internet pelo direito penal. Indaga-se, *verbi gratia*, acerca de quais são exatamente os problemas que, então, demandariam a iniciativa do legislador, sobre o caminho do progresso da tecnologia no futuro, e a respeito dos seus efeitos colaterais, até indesejados, que possam aparecer (2020, p. 128).

Dentre esses problemas que se descortinam para o direito penal e o seu papel norteador para a regulação da internet e das redes sociais, encontra-se a necessidade da compreensão dos crimes cibernéticos (*cybercrimes*).

Para Carlos María Romeo Casabona, eles se diferenciam dos delitos informáticos, assim entendidos como as infrações penais que constituiriam, na fenomenologia das tecnologias de informação e comunicação, uma primeira geração que agrupa cinco modalidades principais de conduta típicas, quais sejam manipulação de dados e ou programas (fraude informática); cópia ilegal de programas (pirataria informática); obtenção ou utilização ilícita de dados (espionagem informática), produzindo dano à capacidade competitiva da empresa; destruição ou inutilização de dados ou sistemas de informática (sabotagem informática); e agressões ao *hardware* ou ao suporte material de informática, principalmente "furto de tempo em um sistema de informática (2011, p. 515-516). O sistema de informática seria, portanto, o objeto material desses crimes.

Para o autor, os crimes cibernéticos integram uma geração posterior, que incorpora a antecedente, preferindo-se a nova terminologia, pois resultante da evolução das comunicações telemáticas abertas, especialmente a internet, que permitem possibilidades ilimitadas de transferência, fluxo e comunicação de informações, de tal forma que essas seriam o conjunto de condutas referentes ao acesso, apropriação, troca e disponibilização de informações em redes

telemáticas, praticadas sem consentimento ou autorização exigidos, podendo afetar bens jurídicos individuais ou supra individuais, elencando, dentre as condutas mais comuns as seguintes: divulgação de conteúdos ilícitos; acesso, alteração ou obstrução de sistemas e bases de dados alheios, independentemente de sua estrutura ou conteúdo; ataques a diversos objetos da propriedade intelectual; e "delitos convencionais, nos quais a rede seja o fator mais relevante para possibilitar a prática e a reiteração instantânea e sucessiva do fato" (2011, p 517-518).

Como se vê, os delitos cibernéticos, pelas suas características, podem ser praticados com maior facilidade através das plataformas de redes sociais, ostentando maior potencial lesivo a bens jurídico-penais. Segundo Ametelo Masini Neto, os cibercrimes próprios ou puros são as condutas que não existiam antes do advento da tecnologia digital, cuidando-se de infrações penais que não podem ser pensadas em outro contexto senão pelo atentado aos sistemas informáticos, sendo cometidos, em sua maioria, pela rede mundial de computadores (2025, p. 23), como, por exemplo, no Brasil, o delito de invasão de dispositivo informático (art. 154-A do CP); o crime de furto mediante fraude cometido por meio de dispositivo informático (art. 155, § 4º-B, do CP), o delito de estelionato eletrônico (artigo 171, § 2ª-A, do CP); o crime de inserção de dados falsos em sistema de informações (art. 313-A do CP); e o delito de modificação ou alteração não autorizada de sistema de informações (art. 313-A do CP). Em suma, são crimes que apenas podem ser praticados através do emprego de tecnologias digitais.

Por sua vez, os crimes cibernéticos impróprios ou impuros são as infrações penais tradicionais que já existiam na legislação antes da era digital, mas que, atualmente, podem ser perpetradas pela internet, tais como os delitos contra a honra e a ameaça (Masini Neto, 2025, p. 23-24). Acrescentamos a essa definição as condutas que foram criminalizadas após o advento da rede mundial de computadores e que também podem ser praticados, ainda que não exclusiva ou necessariamente, através de meios digitais.

A tutela penal de crianças e adolescentes encontra sua legitimidade notadamente no princípio da prioridade absoluta, consagrado no artigo 227 da Constituição Federal e no artigo 4º da Lei n. 8.069/1990, que deve ser observado pelo Estado, pela família e pela sociedade, significando a primazia em favor dos menores de 18 anos, tendo como objetivo concretizar a proteção integral, que se assenta em três pilares: o reconhecimento do infante como pessoa em peculiar condição de desenvolvimento, titular de proteção especial e do direito à convivência familiar.

Ademais, o artigo 227, § 4º, da nossa Lei Maior, encerra um mandado expresso de criminalização, ao prever que a "lei punirá severamente o abuso, a violência e a exploração sexual da criança e do adolescente", contendo inequívoca determinação ao legislador ordinário

para que se valha do direito penal para a tutela de bens jurídicos de inegável magnitude e que são atingidos por essas condutas de extrema gravidade.

Os crimes contra crianças e adolescentes não estão previstos somente na Lei n. 8.069/1990, mas também no Código Penal e em outras leis penais especiais, contemplando delitos em que o infante é sujeito passivo imediato ou tipos derivados, nos quais a condição de menor de 18 anos de idade é uma qualificadora ou causa de aumento de pena, isso sem falar da agravante genérica do crime perpetrado contra criança prevista no art. 61, II, alínea h, do Código Penal.

Nesse panorama, os crimes cibernéticos, próprios ou impróprios, contra crianças e adolescente assomem em importância, justamente pelas peculiaridades do contínuo desenvolvimento da internet, como se viu acima, quais sejam a velocidade de transferência de informações, a permanência de conteúdos e a fusão com a vida cotidiana, o que incrementa o potencial de prática de delitos com a utilização da rede mundial de computadores e, particularmente das redes sociais, contra vítimas vulneráveis, o que reclama a sua regulação, notadamente normativa e através do direito penal.

É o que se tem verificado nos últimos anos com diversas alterações legislativas de tipos penais já existentes e na criminalização de condutas que atinjam bens jurídicos cujos titulares são pessoas menores de 18 anos. É o que adiante se verá.

3 Crimes cibernéticos previstos na Lei n. 8.069/1990

Atualmente, o Estatuto da Criança e do Adolescente (ECA), no Título VII, da sua Parte Especial, em seu Capítulo I, prevê vinte e dois tipos penais, sem qualquer rubrica lateral e uma sistematização que, embora não isenta de críticas, permite divisar crimes relacionados ao atendimento à gestante e ao neonato em estabelecimentos de saúde (artigos 228 e 229); ao procedimento de apuração de atos infracionais (artigos 230, 231, 234 e 235); um crime contra a Administração da Justiça (artigo 236); delitos que protegem o direito à convivência familiar e comunitária, no seio da família natural ou, segundo os ditames legais, em família substituta (artigos 237 a 239); crimes que tutelam a integridade física, psíquica, a saúde e a formação moral (artigos 232, 242, 243, 244, 244-B e 244-C); e, aqui merecendo especial atenção, os crimes que, tendo por objeto material um conteúdo pornográfico infanto-juvenil, tutelam a integridade física, psíquica, moral, a honra objetiva e a dignidade sexual da pessoa menor de 18 anos.

Os delitos que envolvem material pornográfico infanto-juvenil, desde a promulgação do Estatuto, foram objeto de sucessivas alterações e inovações, através da Lei n. 10.764, de 12 de novembro de 2003; da Lei n. 11.829, de 25 de novembro de 2008; e, mais recentemente, da Lei n. 14.811, de 12 de janeiro de 2024. Em todos esses diplomas, procurou-se atualizar o Estatuto para o enfrentamento do abuso sexual infantil propiciado pela produção, comercialização, divulgação de conteúdo pornográfico, condutas potencializadas pelo emprego da internet para tais finalidades.

Certamente, a grande reforma deu-se com a Lei n. 11.829, de 25 de novembro de 2008, a qual, em consonância com a Convenção Sobre os Direitos da Criança e seu Protocolo Facultativo referente à Venda de Crianças, à Prostituição e à Pornografia Infantis, ratificados pelo Brasil, alterou os artigos 240 e 241 e acrescentou os artigos 241-A a 241-E do Estatuto.

Marcos Tupinambá M. A. Pereira classifica essas infrações penais em crimes de criação de conteúdo, de comercialização, de distribuição, de posse, de criação e distribuição de conteúdo por simulação e de aliciamento (2024, p. 53-54).

A norma penal explicativa (artigo 241-E do ECA) não distingue cena de sexo explícito da cena pornográfica, estabelecendo que ambas compreendem qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição de órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais. Mesmo com a explicitação pelo referido dispositivo, a expressão empregada é um elemento normativo do tipo, dependendo de uma valoração pelo intérprete (Campana, 2010, p. 1.097).

Nos referidos tipos penais, todos eles dolosos, é possível identificar crimes cibernéticos próprios e impróprios.

Com efeito, no artigo 240 de Lei n. 8.069/1990, denominado crime de produção ou de criação de material pornográfico infanto juvenil, foi acrescentado, pela Lei n. 14.811, de 12 de janeiro de 2024, o inciso II ao seu § 1º, que contém a previsão de condutas equiparadas, sancionando, com pena de reclusão de quatro a oito anos, quem exibe, transmite, auxilia ou facilita a exibição ou transmissão, em tempo real, pela internet, por aplicativos, por meio de dispositivo informático ou qualquer meio ou ambiente digital, de cena de sexo explícito ou pornográfica com a participação de criança ou adolescente. Aliás, por força do mesmo diploma legal, tais condutas constituem crimes hediondos.

Segundo Guilherme de Souza Nucci no mencionado inciso, as condutas típicas se relacionam a uma mostra realizada ao vivo, pela rede mundial de computadores, valendo-se de softwares ou programas feitos para servir a dispositivos informáticos, e cujo instrumento é um dispositivo informático, como um hardware apto a armazenar dados, ou qualquer outro meio

ou ambiente digital, abrangendo "possíveis novas tecnologias capazes de transmitir dados por caminhos digitais inéditos" (2025b, p. 92),

Cuida-se de crime que agora pode ser chamado de transmissão em tempo real de material pornográfico infanto-juvenil, classificado como crime cibernético próprio, pois somente pode ser cometido através de meios digitais, inclusive através de aplicativos de mensageria e plataformas de redes sociais, as últimas em razão de o legislador claramente utilizar-se de interpretação analógica.

Por sua vez, o artigo 241-A, *caput*, do Estatuto, prevê a punição de condutas de divulgação gratuita do conteúdo encerrando cena de sexo explícito ou pornográfica envolvendo criança ou adolescente, inclusive por meio de sistema de informática ou telemático, o que inclui, especialmente, a internet. Trata-se de delito cibernético impróprio, pois também pode ser praticado por outro meio, que não empregue tecnologia digital.

Dentre as condutas equiparadas no § 1º do referido dispositivo, nos seus incisos I e II, pune-se, com reclusão de três a seis anos, quem assegura os meios ou serviços para o armazenamento do material pornográfico infanto-juvenil de que trata o *caput*, e, que proporciona, por qualquer meio, o acesso por rede de computadores a este conteúdo, incluindo, portanto, como sujeito ativo, o provedor de acesso à internet e o provedor de aplicação. Está-se diante de outro crime cibernético próprio.

Tanto assim que, no § 2º do artigo 241-A do ECA, dispõe-se sobre uma condição objetiva de punibilidade, pois condutas do § 1º somente são puníveis caso haja omissão do responsável legal pela prestação do serviço, ou seja, quando esse agente, possuindo capacidade técnica para tanto e poder de mando, deixa de desabilitar o acesso ao conteúdo ilícito quando oficialmente notificado para tanto. Embora não haja prazo fixado na lei, reputa-se razoável o período de 24 a 48 horas (Nucci, 2025b, p. 101).

Deve-se, ademais, atentar que o crime de distribuição gratuita de material pornográfico-infanto-juvenil previsto no Estatuto da Criança e do Adolescente prevalece sobre o crime de divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia (art. 218-C do Código Penal), o qual foi incluído pela Lei n. 13.718/2018 e que também prevê como modo de execução o emprego de sistema de telemática ou informática. De fato, o referido tipo penal cede por força da subsidiariedade expressa no seu preceito secundário e em razão de o primeiro ser mais severamente apenado.

No que tange ao crime de aquisição e guarda de conteúdo de pornografia infantil (art. 241-B da Lei n. 8.069/1990), que foi acrescentado ao rol dos hediondos pela Lei n. 14.811/2024, há previsão de causa excludente de ilicitude se a posse e o armazenamento têm a finalidade de

denunciar às autoridades competentes a ocorrência dos delitos previstos nos artigos 240, 241, 241-A e 241-C do Estatuto, quando a comunicação, a qual, por óbvio, deve ser breve, for levada a efeito pelo representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio da rede de computadores, até o recebimento do material pela Autoridade Policial, pelo Ministério Público e Poder Judiciário (art. 241-B, § 2º, inciso III, do ECA), o que, juntamente com a condição objetiva de punibilidade inserta no dispositivo anterior, também mostra que deve existir, por parte dessas plataformas, controle acerca do conteúdo nocivo que trafega pela internet.

O tipo penal de montagem de material pornográfico infanto-juvenil ou de criação e distribuição de conteúdo por simulação, descrito no art. 241-C, *caput*, do ECA é outro crime cibernético impróprio, pois não é cometido exclusivamente por meio digital. Busca-se a punição do agente que, não possuindo conteúdo verdadeiro, quais sejam fotos, vídeos ou outros registros contendo imagens de crianças e adolescentes em cenas pornográficas ou de sexo explícito, produz um simulacro, "alterando cenas, por meio de programas específicos, com o fim de criar imagens dissimuladas" (Nucci, 2025b, p. 106). Os verbos nucleares são adulterar (falsificar), montar (construir) e modificar (alterar), os objetos materiais já mencionados, alcançando qualquer forma de representação visual, empregando mais uma vez o legislador a interpretação analógica (Ishida, 2024, p. 958). No parágrafo único, pune-se, com a mesma sanção (reclusão de um a três anos), a divulgação, venda, aquisição, posse e armazenamento da contrafação.

Frise-se que o Brasil promulgou, através do Decreto n. 11.491, de 12 de abril de 2023, a Convenção de Budapeste sobre o Crime Cibernético, o qual estabelece a criminalização da produção, disponibilização, distribuição, aquisição e posse de pornografia infantil através de um sistema de computador, bem como que o material pornográfico inclui a representação visual de imagens realísticas retratando um menor envolvido em conduta sexual explícita, o que se enquadra na simulação de participação de criança e adolescente em cena desta natureza.

O *caput* do artigo 241-C do ECA amolda o fenômeno do *deepfake* pornográfico infantil, a pseudopornografia, sendo que, conforme bem observado por Ameleto Masini Neto, o uso da inteligência artificial para a prática da infração penal ganha destaque (2025, p.78), pois o algoritmo permite, por exemplo, uma montagem que consista no aproveitamento da imagem real do rosto de uma criança ou adolescente, nela se inserindo um corpo *fake*, nu, de pessoa adulta, material esse que posteriormente será transmitido e divulgado por meios digitais.

Paulo Gustavo Lima e Silva Rodrigues atenta que o compartilhamento desse conteúdo pelas redes sociais e *sites* pornográficos é, efetivamente, a conduta mais lesiva dentre aquelas envolvidas no *deepfake* (2023, p. 287).

Por sua vez, o crime de aliciamento de criança (art. 241-D do ECA), sancionado com a pena de reclusão de um a três anos, é crime formal, de perigo abstrato, exigindo o dolo específico consistente na finalidade do agente de praticar ato libidinoso com o menor de 12 anos. Cuida-se de um crime cibernético impróprio, pois todas as condutas típicas descritas no *caput*, quais sejam, aliciar, assediar, instigar ou constranger, podem ser praticadas por qualquer meio de comunicação, inclusive pela internet e pelas ferramentas por ela disponibilizadas, como salas de bate-papo, e-mails, e redes sociais como Facebook (Masini Neto, 2025, p. 80). No mesmo sentido, o entendimento de Guilherme de Souza Nucci, ao afirmar que o tipo incriminador se dirige, primordialmente, ao agente que se comunica, através da internet, por intermédio de sites, dentre outros instrumentos, com crianças, "buscando atraí-las para a mantença de relacionamento sexual" (2025b, p. 108).

Aliás, a proliferação de redes sociais permite também que através delas sejam cometidas as condutas equiparadas no § 1º, inciso I, do artigo 241-D do ECA, quais sejam, facilitar ou induzir o acesso da criança ao material pornográfico infanto-juvenil, com o propósito do agente em satisfazer a própria lascívia, ou ainda atrair a criança, por meio dessas plataformas, com o fim de persuadi-la a mostrar-se de forma pornográfica ou sexualmente explícita, agindo o agente, portanto, com o elemento subjetivo específico, pois "almeja conseguir fotos, vídeos ou outros registros" (Nucci, 2025b, p. 109), o que configura o delito previsto no § 1º, inciso II, do referido dispositivo.

Por fim, o crime de corrupção de criança ou adolescente, definido no artigo 244-B da Lei n. 8.069/1990 é um delito formal, que prevê, no parágrafo 1º, uma modalidade eletrônica ou virtual (Masini Neto, 2025, p. 81), ao punir a conduta de perverter ou facilitar a perversão do menor de 18 anos, com ele praticando infração penal, ou induzindo a praticá-la, empregando-se quaisquer meios eletrônicos, inclusive salas de bate-papo na internet, e, igualmente, através de e-mails e redes sociais. É um crime cibernético próprio, majorado se a infração penal cometida ou induzida encontra-se no rol dos hediondos, consoante dispõe o seu § 2º.

Como bem assevera Marcos Tupinambá M. A. Pereira, a tutela de crianças e adolescentes deve ser prioridade e o meio digital não pode ser uma forma de proteção aos predadores sexuais ou a outros criminosos de qualquer espécie (2024, p. 55).

Os crimes cibernéticos previstos no ECA mostram que já existe um desenho punitivo que alcança a criminalidade praticada através da internet e, particularmente, pelas redes sociais, possibilitando em algumas hipóteses a punição de pessoas físicas que representam provedores de internet, de conexão e de aplicação, evidentemente se agirem com dolo, fornecendo-se,

assim, um alicerce para a autorregulamentação ou para a regulação normativa das plataformas digitais.

Conforme tese fixada pelo STF no julgamento do RE 1.037.396-SP, de relatoria do Ministro Dias Toffoli, enquanto não sobrevier nova legislação, os provedores de aplicação são obrigados a promover a indisponibilização imediata de conteúdos que configurem os crimes dos artigos 240, 241-A, 241-C, 241-D do Estatuto da Criança e do Adolescente.

4 Código Penal e crimes cibernéticos contra crianças e adolescentes

A Lei n. 14.811/2024, que instituiu medidas de proteção aos menores de 18 anos contra a violência nos estabelecimentos educacionais ou similares, para além de prever a Política Nacional de Prevenção e Combate ao Abuso e Exploração Sexual da Criança e do Adolescente, introduziu dispositivos no Código Penal que encerram crimes cibernéticos.

Com efeito, além das alterações no Estatuto da Criança e Adolescente, como acima se viu, o diploma legal acrescentou o § 5º ao art. 122 do CP, que descreve o crime de induzimento, instigação ou auxílio ao suicídio e à automutilação, e estatuiu os tipos incriminadores do *bullying* e *cyberbullying* ao inserir o art. 146-A e seu parágrafo único ao Estatuto Repressivo.

É bem verdade que a Lei n. 13.185/2015 estabeleceu o Programa de Combate de Intimidação Sistemática (*bullying)* e a conceituou como todo ato de violência física ou psicológica, intencional e repetitivo que ocorre sem motivação evidente, praticado por indivíduo ou grupo, contra uma ou mais pessoas, com o objetivo de intimidá-la ou agredi-la, causando dor e angústia à vítima, em uma relação de desequilíbrio de poder entre as partes envolvidas, ao mesmo tempo mencionando que se considera *cyberbullying* a intimidação sistemática na rede mundial de computadores, quando se usam os instrumentos que lhe são próprios para depreciar, incitar a violência, adulterar fotos e dados pessoais com o intuito de criar meios de constrangimento psicossocial. Contudo, não tipificou essas condutas.

Ana Paula Canto de Lima e Valéria Cheque Granato asseveram que o *bullying* e *cyberbullying* são fenômenos sociais que não possuem o tratamento e relevância que deveriam, tendo em vista o seu potencial lesivo, sendo que o *cyberbullying* surge com o advento da internet, utilizando recursos tecnológicos com o mesmo objeto do *bullying*, mas devido ao seu alcance e da disponibilidade do anonimato no ambiente digital, se tornou um problema mais grave (2024, p. 85-86).

Embora o *bullying* possa ocorrer em praticamente qualquer local, independentemente da idade, o fenômeno é mais comum no ambiente e idade escolar, sendo que as ofensas e

agressões disseminadas através da internet provocam resultados mais gravosos para as vítimas (Röder e Silva, 2018, p. 30), atingindo notadamente crianças e adolescentes, causando-lhes um sofrimento capaz de se prologar até a vida adulta. Destaque-se que a Lei n. 14.811/2024 foi promulgada após alguns casos de ataques a escolas ocorridos em 2023 e que vitimaram professores e alunos (Lima e Granato, 2024, p. 91).

Acrescente-se que, no RE 1.037.396-SP, o STF estipulou o dever dos provedores de aplicação de tornar indisponíveis imediatamente também os conteúdos que configurem crimes cometidos contra mulheres em razão da condição do sexo feminino, entre os quais o previsto no art. 146-A do CP, figurando igualmente como vítimas crianças e adolescentes.

Consoante a nova definição típica, o crime de *cyberbullying* consiste na realização de todos os elementos descritos no *caput* do artigo 146-A quais sejam a intimidação sistemática, individual ou em grupo, mediante violência física ou psicológica, de uma ou mais pessoas, de modo intencional e repetido, sem motivação evidente, por meio de atos de humilhação ou de discriminação ou de ações verbais, morais, sexuais, sociais, psicológicas, físicas materiais ou virtuais) através da internet, de rede social, de aplicativos, de jogos on-line ou por qualquer outro meio ou ambiente digital, ou transmitida em tempo real. Trata-se, evidentemente, de um crime cibernético próprio, habitual, tendo o legislado lançado mão, mais uma vez, da interpretação analógica.

Ameleto Masini Neto elenca como exemplos concretos da intimidação sistemática virtual o assédio *online*, que se verifica como o envio de mensagens ameaçadoras ou ofensivas por intermédio das plataformas digitais; a difamação ou a injúria, inclusive com o compartilhamento de informações falsas ou humilhantes nas redes sociais e o monitoramento contante da vida online da vítima, “causando-lhe desconforto, sofrimento e medo” (2025, p. 69).

Por seu turno, Ana Paula Canto de Lima e Valéria Cheque Granato chamam a atenção para as gravíssimas consequências causadas pelo *cyberbullying* às suas vítimas, principalmente a automutilação, inúmeros transtornos, ansiedade, depressão, podendo chegar ao suicídio (2024, p. 96). Com razão, Tiago Misael de Jesus Martins assinala que os atos de intimidação sistemática andam lado a lado com um outro tipo penal que é cada vez mais comum entre adolescentes: o induzimento, instigação ou auxílio ao suicídio ou a automutilação (2025, p. 71).

Os crimes de participação em suicídio e de participação em automutilação estão previstos no artigo 122 do Estatuto Repressivo. O suicídio é a deliberada eliminação da própria vida, enquanto a automutilação é a autolesão voluntária direta. A última consiste em ferir a si

mesmo, consistindo no ato de causar dor ou lesão em seu próprio corpo, sem intenção de chegar à morte.

O tipo penal incrimina condutas de colaboração no suicídio ou na automutilação de outrem, com a nota que a automutilação pode ser considerada um comportamento imitável, isso porque algumas pessoas ferem-se vendo outras assim agindo, ou ainda, ao tomarem ciência, notadamente pelas redes sociais, de comportamentos dessa ordem.

Guilherme Souza Nucci assinala que a inclusão, pela Lei n. 13.968/2019, do crime de participação em automutilação deita suas raízes num jogo mórbido denominado Baleia Azul, que levava os envolvidos, dentre eles um número considerável de adolescentes, a cortar-se ou até mesmo tirar a própria vida, citando ainda o Desafio do Apagão, que surgiu na internet, por intermédio da rede social Tik Tok, acolhido principalmente por crianças e adolescentes, consistente em apertar o pescoço até perder a consciência (2025a, p. 625-626).

Daí porque, as consequências desses delitos são, evidentemente mais gravosas, quando as vítimas são crianças ou adolescentes. Sendo assim, nos termos do § 3º do dispositivo, a pena é duplicada se a vítima é menor ou tem diminuída, por qualquer causa, a capacidade de resistência. Essa causa de aumento de pena incide quando a vítima é menos de 18 anos e maior de 14 anos, por interpretação sistemática com os §§ 6º e 7º do artigo 122 do CP, os quais estipulam que, se os crimes forem praticados contra menor de 14 anos ou contra quem não tenha necessário discernimento para a prática do ato ou que não possa, por qualquer outra causa oferecer resistência, o agente pode responder, dependendo do resultado, pelo delito de lesão corporal gravíssima ou por homicídio.

Demais disso, a Lei 14.811/2024 tornou hedionda a participação cibernética em suicídio e automutilação prevista no § 4º do art. 122 do Estatuto Repressivo, que prevê o aumento de pena até o dobro se a conduta do agente é praticada por meio da rede mundial de computadores (internet), rede social ou transmitida em tempo real, por meio de plataformas digitais *online*. O referido diploma legal também alterou o § 5 do art. 122 do CP, passando a estipular que a pena ainda se aplica em dobro se o autor das condutas típicas é líder, coordenador ou administrador de grupo, de comunidade ou de rede virtual, ou por estes é responsável.

Portanto, o Código Penal encerra crimes cibernéticos específicos contra crianças e adolescentes e que servem de balizas para uma regulação das redes sociais que imponha aos provedores de aplicação o dever de retirada de conteúdos que possam estimular e desencadear o cometimento desses delitos, na linha do relatório da redação final do Projeto de Lei 2.630/2020 e no âmbito do julgamento da constitucionalidade do artigo 19 da Lei n. 12.965/2014 (Marco Civil da Internet).

5 Conclusões

O surgimento e a expansão da internet trouxeram inúmeros benefícios, ao mesmo tempo que propiciou, notadamente através dos denominados provedores de aplicação, com destaque para as redes sociais, um incremento de comportamentos socialmente danosos e criminosos, de tal forma que o uso ilícito da rede mundial de computadores traz a lume significativos problemas para a tipificação de condutas e a aplicação do direito penal.

Embora nem todo o instrumental da internet e, mais especificamente, das plataformas de redes sociais, tenha sido criado para propósitos ilícitos, é inegável que elas intensificaram a propagação de conteúdos nocivos, cujo alcance, impacto e lesão a bens jurídicos é potencializado pela quantidade inimaginável de interações entre indivíduos e grupos.

Com relação às crianças e adolescentes, o mundo digital proporciona uma fuga da vida real, sujeitando-os a uma vulnerabilidade psicológica que os torna alvo da prática de inúmeras infrações penais, dentre as quais crimes cibernéticos, os quais, pelas suas características, podem ser praticados com maior facilidade através das plataformas de redes sociais, ostentando maior potencial lesivo.

Os crimes cibernéticos previstos na Lei n. 8.069/1990 e no Código Penal mostram que já existe um desenho punitivo que alcança a criminalidade praticada através da internet e, particularmente, pelas redes sociais, possibilitando, em algumas hipóteses, a punição de pessoas físicas que representam provedores, de conexão e de aplicação, quando agirem com dolo, fornecendo-se, assim, um alicerce para a autorregulamentação ou regulação de *lege ferenda* das plataformas digitais, bem como balizas que, através de interpretação conforme, como se verificou em recente julgamento pelo Supremo Tribunal Federal, imponham à plataformas digitais o dever de retirada de conteúdos que configuram o cometimento desses delitos.

6 Referências bibliográficas

ALBUQUERQUE, Carla. Os labirintos do crime digital: jovens e a cibercriminalidade. *Crimes Digitais*. Francini Imene Días Ibrahin e Joaquin Leitão Junior (organizadores). Leme: Mizuno, 2025.

CAMPANA, Eduardo Luiz Michelan. *Estatuto da Criança e do Adolescente Comentado: Comentários Jurídicos e Sociais*. Coordenador Munir Cury. 11ª ed. São Paulo: Malheiros, 2010, p. 1.097.

BRASIL. Decreto nº 99.710, de 21 de novembro de 1990. Promulga a Convenção sobre os Direitos da Criança. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d99710.htm. Acesso em: 25 jun. 2025.

BRASIL. Decreto nº 5.007, de 08 de março de 2004. Promulga o Protocolo Facultativo à Convenção sobre os Direitos da Criança referente à venda de crianças, à prostituição infantil e à pornografia infantil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/decreto/d5007.htm. Acesso em: 25 jun. 2025.

BRASIL. Decreto nº 11.491, de 12 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm. Acesso em: 25 jun. 2025.

BRASIL. Projeto de Lei 2630/2020. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Brasília-DF: Câmara dos Deputados. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256735. Acesso em: 14 jun. 2025.

BRASIL. Supremo Tribunal Federal. Recurso Extraordinário 1.037.396-SP; Relator: Min. Dias Toffoli. Disponível em:https://portal.stf.jus.br/processos/detalhe.asp?incidente=5160549. Acesso em: 30 jun. 2025.

BRASIL. Supremo Tribunal Federal. Recurso Extraordinário RE 1.057.258-MG; Relator: Min. Luiz Fux. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5217273. Acesso em: 30 jun. 2025.

BRASIL. Resolução nº 305 de 17 de dezembro de 2019. Estabelece os parâmetros para o uso das redes sociais pelos membros do Poder Judiciário. Brasília-DF: Conselho Nacional de Justiça. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3124. Acesso em: 14 jun. 2025.

HILGENDORF, Eric. A regulação jurídico-penal da internet como tarefa de um moderno direito da tecnologia. *Digitalização e Direito*. Organizador e tradutor Orlandino Gleizer. São Paulo: Marcial Pons, 2020.

ISHIDA, Valter Kenji. *Estatuto da criança e do adolescente: doutrina e jurisprudência*. 24ª ed. São Paulo: JusPODIVM, 2024.

LIMA, Ana Paula Canto de, GRANATO, Valéria Cheque. Inovação legal: bullying e cyberbullying. *Crimes Digitais*. Ana Paula Canto de Lima e Marcelo Crespo (Coordenadores). São Paulo: Thomson Reuters, 2024.

MARTINS, Tiago Misael de Jesus. Partidas Nocentes- Investigação de Crimes em jogos Eletrônicos Online. *Crimes Digitais*. Francini Imene Días Ibrahin e Joaquin Leitão Junior (organizadores). Leme: Mizuno, 2025.

MASINI NETO, Ameleto. *Crimes cibernéticos*. Indaiatuba: Editora Foco, 2025.

NUCCI, Guilherme de Souza. *Código penal comentado*. 25ª ed. Rio de Janeiro: Forense, 2025a.

_____. *Leis penais e processuais penais comentadas*. Vol. 2. 16ª ed. Rio de Janeiro: Forense, 2025b.

PEREIRA, Marcos Tupinambá M. A. Crimes por meios digitais – desafios e modalidades atuais. *Crimes Digitais*. Ana Paula Canto de Lima e Marcelo Crespo (Coordenadores). São Paulo: Thomson Reuters, 2024.

RÖDER, Priscila Costa Schreiner, SILVA, Helder Magno da. Cyberbullying: uma agressão virtual com consequências reais para a vítima e a sociedade e a |Justiça Restaurativa como forma eficiente de solução. *Crimes cibernéticos: racismo, cyberbullying, deep web, pedofilia e pornografia infantojuvenil; infiltração de agentes por meio virtual, obtenção das provas digitais, nova lei antiterrorismo, outros temas*. Ângelo Roberto Ilha da Silva (organizador). 2ª ed. Porto Alegre: Livraria do Advogado Editora, 2018.

RODRIGUES, Paulo Gustavo Lima e Silva. Deepfakes pornográficas não consensuais: a busca por um modelo de criminalização. *Revista Brasileira de Ciências Criminais*, vol. 199 – novembro-dezembro 2023. São Paulo: Thomson Reuters. p. 277-311.

ROMEO CASABONA, Carlos María. Dos delitos informáticos ao crime cibernético: uma aproximação conceitual e político-criminal. *Doutrinas Essenciais de Direito Penal Econômico e da Empresa*. Vol. 6. São Paulo: RT, 2011, p. 509-522.

SALVADOR, João Pedro Favaretto. *Discurso de ódio e redes sociais*. São Paulo: Almedina, 2023.

SANTOS, Maria Celeste Cordeiro Leite dos, ARAÚJO, Marilene. A Inteligência Artificial (IA) e a lei brasileira de responsabilidade e transparência na internet - Humanismo 4.0 - Impactos na cidadania. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Econômico. Ricardo Hasson Sayeg (coord. de tomo). São Paulo: Pontifícia Universidade Católica de São Paulo, março 2024. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/577/edicao-1/a-inteligencia-artificial-%28ia%29-e-a-lei-brasileira-de-responsabilidade-e-transparencia-na-internet---humanismo-4.0---impactos-na-cidadania. Acesso em: 15 jun. 2025.

SHIMABUKURO, Adriana, ABREU E SILVA, Melissa Garcia Blagitz de. Internet, Deep Web e Dark Web. *Crimes cibernéticos: racismo, cyberbullying, deep web, pedofilia e pornografia infantojuvenil; infiltração de agentes por meio virtual, obtenção das provas digitais, nova lei antiterrorismo, outros temas*. Ângelo Roberto Ilha da Silva (organizador). 2ª ed. Porto Alegre: Livraria do Advogado Editora, 2018.

U.S. Department of Justice, Criminal Divison. Child Exploitation and Obscenity Section (CEOS). Disponível em: https://www.justice.gov/criminal/criminal-ceos/subject-areas, acesso em: 17 de junho de 2025.