CRIMES CIBERNÉTICOS CONTRA CRIANÇAS E ADOLESCENTES: OS DESAFIOS DO PRIMEIRO GRAU DE JURISDIÇÃO

Cybercrimes Against Children And Adolescents: The Challenges Of The First-Instance Jurisdiction

GABRIELA PASSOS ANDRADE - Assessora de Pós-graduação na Unidade Especial de Atuação no Primeiro Grau de Jurisdição (UEA) e Mestranda em Direito das Relações Sociais pela Universidade Federal do Paraná. E-mail: gabriela.p.andrade@tjpr.jus.br.

LUCAS DE SOUZA PATARO - Estagiário de Graduação na Unidade Especial de Atuação no Primeiro Grau de Jurisdição (UEA), Acadêmico de direito pelo Centro Universitário do Paraná Uniensino. E-mail: lucas.pataro@tjpr.jus.br.

MARCELE CAROLINE MOREIRA MEDEIROS - Assessora de Pós-graduação na Unidade Especial de Atuação no Primeiro Grau de Jurisdição (UEA) e Pós-Graduanda em Direito e Processo Penal pela Academia Brasileira de Direito Constitucional. E-mail: marcele.medeiros@tjpr.jus.br.

O artigo trata dos crimes cibernéticos praticados contra crianças e adolescentes, analisando sua vulnerabilidade no ambiente digital e os desafios enfrentados pelo primeiro grau de jurisdição na apuração e responsabilização dos autores. O objetivo é compreender os entraves jurídicos e técnicos decorrentes da anonimização e propor soluções que assegurem a efetividade da proteção integral da criança e do adolescente. Para isto, utilizou-se pesquisa bibliográfica e análise normativa, abordando dispositivos como a Constituição, o ECA, o Marco Civil da Internet e a LGPD, além de estudos doutrinários sobre o tema. Conclui-se que a complexidade tecnológica exige uma resposta multidisciplinar e técnica, bem como a cooperação institucional para garantir celeridade processual e proteção efetiva às vítimas.
Palavras-Chave: Crimes cibernéticos; Anonimização; Crianças e adolescentes; Proteção integral.

The present article addresses cybercrimes committed against children and adolescents, analyzing their vulnerability in the digital environment and the challenges faced by the first instance jurisdiction in the process of investigation and holding perpetrators accountable. The goal is to understand the legal and technical obstacles arising from the anonymization as well as propose solutions that ensure the effectiveness of the integral protection of children and adolescents. To achieve this, the study employed bibliographic research and normative analysis, covering devices such as The Constitution, The Child and Adolescent's Statute (ECA), The Internet Civil Framework, and the General Data Protection Law (LGPD), in addition to the doctrinal studies on the subject. It was concluded that the technological complexity demands a multidisciplinary and technical response, as well as institutional cooperation to guarantee procedural speed and effective protection for the victims.
Keywords: *Cybercrimes; Anonymization; Children and Adolescents; Integral protection.*

INTRODUÇÃO

O *cibercrime* é um termo genérico que se refere aos crimes praticados por meio da utilização de computadores e da internet, trata-se qualquer atividade criminosa que utiliza computadores, rede de computadores ou a internet como meio ou base para o ataque.

A análise dos crimes cibernéticos demanda a identificação precisa dos sujeitos envolvidos, sobretudo quando as condutas ilícitas atingem pessoas em situação de especial vulnerabilidade jurídica. A inserção precoce de crianças e adolescentes no ambiente digital potencializa a incidência de violações a direitos fundamentais, exigindo a aplicação de um regime jurídico protetivo específico. Desse modo, torna-se imprescindível delimitar o conceito legal de criança e adolescente, a fim de compreender a extensão da tutela conferida pelo ordenamento jurídico, nos termos do Estatuto da Criança e do Adolescente.

Nos termos do artigo 2º do ECA, considera-se c*riança a pessoa até 12 anos de idade incompletos*, enquanto adolescente é *aquela entre 12 e 18 anos de idade*. Excepcionalmente, o Estatuto admite a aplicação de suas disposições a pessoas entre 18 e 21 anos, nos casos expressamente previstos em lei, especialmente para fins de responsabilização por atos praticados durante a adolescência.

A intensificação do uso das tecnologias digitais e da internet transformou profundamente as formas de interação social, ampliando o acesso à informação e à comunicação, mas também criando espaços para a prática de condutas ilícitas. Assim, crianças e adolescentes apresentam um dos grupos mais vulneráveis aos crimes cibernéticos, em razão de sua condição peculiar de desenvolvimento.

Além da acentuada vulnerabilidade das vítimas infantojuvenis, os crimes cibernéticos apresentam desafios próprios quanto à identificação e responsabilização de seus autores. O uso de perfis falsos, técnicas de ocultação e criptografia de endereço dificultam a atuação estatal, especialmente no âmbito do primeiro grau de jurisdição, onde se concentram a instrução probatória e as decisões iniciais do

processo penal. Tais obstáculos exigem do Judiciário e dos demais órgãos de persecução penal uma atuação técnica e célere, capaz de conciliar a complexidade tecnológica com a efetiva proteção dos direitos fundamentais das vítimas para o fim de precisar acerca de quem devidamente responderá pelo delito, isto é, a autoria certa do agente.

Diante desse contexto, o presente artigo tem como objetivo central analisar os crimes cibernéticos praticados contra crianças e adolescentes, destacando os principais entraves enfrentados pelo primeiro grau de jurisdição na apuração, identificação dos criminosos e aplicação das normas protetivas. A relevância do tema reside não apenas no crescimento exponencial dessas práticas delitivas, mas também na necessidade de fortalecer a tutela jurídica conferida ao público infantojuvenil, assegurando a efetividade do Estatuto da Criança e do Adolescente e dos princípios constitucionais da proteção integral e da prioridade absoluta.

O Código Penal não fornece um conceito de crime, somente dizendo, em sua Lei de Introdução, que ao *crime é reservada uma pena de reclusão ou de detenção, quer alternativa ou cumulativamente com a pena de multa*. No entanto, o Código Penal adota implicitamente o conceito analítico de crime, o qual define o crime como *fato típico, antijurídico e culpável.* Sobre o tema Rogério Greco dispõe que:

> A função do conceito analítico é a de analisar todos os elementos ou características que integram o conceito de infração penal sem que com isso se queira fragmentá-lo. O crime é, certamente, um todo unitário e indivisível. Ou o agente comete o delito (fato típico, ilícito e culpável), ou o fato por ele praticado será considerado um indiferente penal. O estudo estratificado ou analítico permite-nos, com clareza, verificar a existência ou não da infração penal (Rogério Greco, 2025, pág. 160).

Diante do exposto, conclui-se que, embora o Código Penal brasileiro não apresente um conceito expresso de crime, limitando-se a diferenciá-lo das contravenções a partir da espécie de sanção cominada, a estrutura normativa e sistemática do diploma penal revela a adoção implícita do *conceito analítico de crime*.

A compreensão do crime como fato típico, antijurídico e culpável, conforme leciona Rogério Greco, permite uma análise racional, metódica e escalonada da infração penal, sem que se perca a noção de sua unidade conceitual. Tal construção dogmática mostra-se essencial para a correta identificação da relevância penal da conduta humana, assegurando coerência interpretativa, segurança jurídica e rigor científico na aplicação do Direito Penal.

1 CRIMES CIBERNÉTICOS CONTRA CRIANÇAS E ADOLESCENTES E O MARCO JURÍDICO DE PROTEÇÃO

A consolidação das tecnologias da informação e comunicação transformou profundamente as relações sociais, ampliando o acesso ao conhecimento, à interação e ao entretenimento no ambiente virtual. Todavia, esse avanço tecnológico também trouxe novos riscos e desafios, sobretudo no que se refere à segurança e à proteção de direitos fundamentais no meio digital. A ausência de barreiras físicas, o anonimato e a rápida disseminação de conteúdos ilícitos tornam a internet um espaço propício à

prática de condutas criminosas, exigindo especial atenção do ordenamento jurídico e das políticas públicas de proteção.

Logo, a incidência dos crimes cibernéticos torna-se especialmente significativa quando envolve crianças e adolescentes, cuja crescente inserção no ambiente digital os expõe de forma acentuada a práticas ilícitas.

A expansão de crianças e adolescentes no ambiente digital inovou as formas de interação social, comunicação e acesso à informação. Plataformas digitais como redes sociais, jogos online e aplicativos de mensagens estão presentes no cotidiano infantojuvenil, o que potencializa à prática de crimes cibernéticos e outras formas de violação de direitos fundamentais.

Assim, se faz necessário analisar a vulnerabilidade infantojuvenil no ambiente digital à luz da Constituição da República Federativa do Brasil, do Estatuto da Criança e do Adolescente e da tutela penal como instrumentos de proteção integral.

1.1. Vulnerabilidade Infantojuvenil no Ambiente Digital

A vulnerabilidade de crianças e adolescentes no meio digital decorre de fatores biológicos, psicológicos e sociais advindos da fase do desenvolvimento. A restrita capacidade de análise crítica, bem como a imaturidade emocional, faz com que o público infantojuvenil seja mais suscetível a manipulações, aliciamentos e exposições indevidas.

No ambiente virtual, tais fragilidades são potencializadas por características próprias de tecnologia, como: anonimato dos usuários, facilidade de acesso a inúmeros conteúdos, rapidez na disseminação de informações, dificuldade de percepção de riscos, ausência de barreiras físicas ou temporais. Esses elementos favorecem a prática de condutas ilícitas e a violação da dignidade de crianças e adolescentes.

Na concepção de Andrea Sant'ana:

> Os próprios adolescentes na Internet conseguem acesso ao submundo do crime sem sair de casa, conectando-se com criminosos de qualquer parte, mediante compras de produtos ilícitos, assim como alguns já praticam crimes digitais (*cybercrimes*), agindo como hackers, violando dispositivos informáticos, em infração ao disposto na Lei Carolina Dieckmann (Lei nº 12.727/2012), além de estelionatos, crimes de ódio e intolerância, isso quando não figuram eles mesmos como líderes e partícipes de organizações criminosas (Andrea Sant' ana Leone Souza, 2022, pág. 63).

Desse modo, verifica-se que a vulnerabilidade de crianças e adolescentes no ambiente digital não é circunstancial, mas estrutural, decorrendo tanto das características próprias do estágio de desenvolvimento quanto das especificidades do meio tecnológico. A conjugação desses fatores amplia significativamente os riscos de violação a direitos fundamentais, seja na condição de vítimas, seja na de envolvidos em práticas ilícitas.

Nesse contexto, impõe-se a adoção de uma tutela jurídica reforçada, pautada nos princípios da proteção integral e da prioridade absoluta, que contemple ações preventivas, educativas e repressivas, bem como a corresponsabilização do Estado, da família, da sociedade e das plataformas digitais, a fim de mitigar os impactos nocivos do ambiente virtual e assegurar o pleno desenvolvimento da população infantojuvenil em consonância com a dignidade da pessoa humana.

1.2. Diretrizes Constitucionais da Proteção Infantojuvenil

A Constituição da República Federativa do Brasil consagra em seu art. 227, a proteção integral da criança e do adolescente como dever prioritário do Estado, da família e da sociedade.

Este dispositivo fundamenta a adoção do princípio da proteção integral, que impõe uma atuação positiva e contínua do Poder Público na formulação de políticas públicas, na edição de normas infraconstitucionais e na atuação jurisdicional. No contexto do ambiente digital, a norma constitucional assume especial relevância, pois legitima e exige a implementação de mecanismos preventivos e repressivos aptos a enfrentar os riscos decorrentes do uso das tecnologias da informação, garantindo que o desenvolvimento tecnológico não se sobreponha à tutela da dignidade humana e aos direitos fundamentais de crianças e adolescentes. Nesse sentido, Tavares, destaca que:

> A Constituição, expressamente, ainda se ocupa em criar o dever de todos de colocar a criança, o adolescente e o jovem a salvo de toda forma de negligência, exploração, violência, crueldade e opressão, cujos conteúdos só podem ser bem compreendidos a partir do pressuposto de que o cuidado a ser dispensado está em direta relação com sua especial condição de vulnerabilidade (André Ramos Tavares, 2025, pág. 366).

Diante disso, evidencia-se que a proteção integral prevista no art. 227 da Constituição Federal não se limita a uma diretriz programática, mas configura verdadeiro mandamento constitucional de eficácia plena, impondo ao Estado e à coletividade o dever de adaptação permanente das estruturas normativas e institucionais às novas realidades sociais.

No ambiente digital, tal dever revela-se ainda mais imperativo, uma vez que a vulnerabilidade de crianças e adolescentes é potencializada pela amplitude, velocidade e alcance das tecnologias da informação. Assim, a tutela constitucional exige uma atuação preventiva, educativa e repressiva articulada, capaz de assegurar que a inovação tecnológica se desenvolva em consonância com a dignidade da pessoa humana e com a efetiva salvaguarda dos direitos fundamentais da população infantojuvenil.

1.3. Estatuto da Criança e do Adolescente e a Proteção no Meio Digital

O Estatuto da Criança e do Adolescente (Lei n.º 8.069/1990) representa a consolidação dos princípios constitucionais da proteção integral e da prioridade absoluta, estruturando um

ordenamento jurídico destinado à efetivação dos direitos fundamentais da criança e do adolescente. Embora elaborado em contexto histórico anterior à ampla disseminação da internet e das tecnologias digitais, o ECA tem sido interpretado de maneira sistemática, teleológica e evolutiva, permitindo sua plena aplicação às violações de direitos ocorridas no ambiente virtual, em consonância com as transformações sociais e tecnológicas.

Assim, merecem destaque os direitos à dignidade, ao respeito e à inviolabilidade da integridade física, psíquica e moral da criança e do adolescente, previstos nos arts. 15 a 17 do Estatuto, os quais devem ser preservados também nas interações digitais.

O ECA também estabelece proteção expressa contra a exploração sexual e qualquer forma de violência, nos termos dos arts. 70 e seguintes, impondo o dever de adoção de políticas públicas e medidas de prevenção capazes de reduzir fatores de risco. Tais dispositivos revelam-se plenamente aplicáveis às práticas ilícitas ocorridas no ciberespaço, como o aliciamento virtual (*grooming*), a exposição indevida de imagens íntimas e o compartilhamento de material pornográfico infantil, condutas que frequentemente se iniciam em plataformas digitais, redes sociais e jogos online.

No âmbito da tutela penal, os arts. 240 a 241-*E* do Estatuto tipificam condutas relacionadas à *produção, posse, divulgação e comercialização de material pornográfico envolvendo crianças e adolescentes*, bem como o *aliciamento e a exploração sexual praticados, inclusive, por meios eletrônicos*. A previsão desses tipos penais evidencia a opção do legislador por uma proteção penal reforçada, reconhecendo a especial vulnerabilidade desse grupo etário e a gravidade das lesões aos bens jurídicos tutelados, notadamente a dignidade sexual e o desenvolvimento psíquico.

Dessa forma, o Estatuto consagra um dever geral de prevenção, atribuindo à família, à sociedade e ao Poder Público responsabilidade compartilhada na adoção de medidas destinadas a evitar a ocorrência de violações de direitos, inclusive no ambiente digital. Tal dever preventivo impõe a necessidade de ações educativas, acompanhamento responsável do uso das tecnologias, mecanismos de controle e moderação de conteúdo, bem como atuação eficiente do sistema de justiça.

Por fim, o ECA reafirma seu papel central na proteção integral da criança e do adolescente frente aos riscos decorrentes da expansão do ciberespaço, exigindo respostas jurídicas compatíveis com as transformações tecnológicas da sociedade contemporânea.

2 A ANONIMIZAÇÃO DE ENDEREÇOS ELETRÔNICOS

Para a adequada compreensão do problema da anonimização, faz-se necessário o esclarecimento prévio de alguns conceitos e princípios fundamentais. Nesse contexto, destaca-se o recorrente debate acerca do direito ao anonimato no ambiente digital, especialmente no que se refere à proteção de dados pessoais sensíveis assegurada pela Lei Geral de Proteção de Dados desde 2018, em contraposição ao art. 5º, inciso IV, da Constituição Federal de 1988, que garante a liberdade de manifestação do pensamento, vedando o anonimato. Todavia, apesar de vedar, o referido dispositivo constitucional não estabelece sanção ou tipificação específica para o uso do anonimato, o

que contribui para a ambiguidade quanto à sua utilização nas redes sociais (MACHADO DONEDA, 2020).

Desta feita, verificado o cenário de insegurança jurídica no meio digital, houve uma tentativa de regular e tornar a internet em um ambiente mais seguro por meio da Lei Nº 12.965/2014. Também conhecida como O Marco Civil da Internet, o regulamento prevê um conjunto de regras que norteiam e servem de auxílio para estabelecer direitos e deveres relativos à utilização da internet no Brasil. Veja-se:

> Art. 5º Para os efeitos desta Lei, considera-se:
> I - Internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;
> II - Terminal: o computador ou qualquer dispositivo que se conecte à internet;
> III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;
> (...)
> V - Conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;
> VI - Registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados; (...).

Com estes parâmetros, é possível compreender como é realizada a localização de endereço por meio do acesso de um dispositivo/terminal à internet ou algum aplicativo que à utilize, visto que todo acesso de rede necessita de um registro de conexão para se comunicar com uma rede.

A Lei Geral de Proteção de Dados (LGPD) surge como uma complementação ao Marco Civil da Internet e consigo traz uma série de novos parâmetros, sendo um deles a definição de anonimização. Leia-se:

> Art. 5º Para os fins desta Lei, considera-se:
> (...)
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento
> (...)
> XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;(...).

Compreende-se desta forma que a anonimização se dá quando da utilização de algum artifício para que a imagem da pessoa se desvincule, direta ou indiretamente, da forma com que esta se apresenta a outrem em um ambiente virtual.

É importante ressaltar que o anonimato, por si só, não possui caráter positivo ou negativo, pois seu valor depende do uso que o indivíduo faz dele; assim, pode ser empregado de ambas as formas. Deste modo uma denúncia anônima de um crime contribui positivamente para a manutenção da ordem, enquanto a não identificação de um indivíduo que pratica

phishing[120] e causa danos a um negócio contribui de forma negativa. A dificuldade reside em estabelecer um balanço entre até onde o anonimato deve ser relativizado e até onde deve ser protegido (SIEPIERSKI SILVA, 2016).

Contudo, por mais que existam meios para a localização e identificação do perpetrador, as dificuldades para tal feito se intensificam com o uso de tecnologias específicas, VPNs e navegadores anônimos. Há também a criação de perfis falsos e temporários, que são excluídos logo após a prática de um crime para apagar rastros. Vale ressaltar que a criação de perfis falsos por si só não configura crime, restando caracterizado apenas quando o perfil for utilizado para alguma conduta delitiva, isto é, servir como meio para a concretização de um crime (TEIXEIRA; SANTOS; ÉRICA, 2023).

Outro fator de impedimento para a localização de criminosos é a utilização de Virtual Private Network - Redes Privadas Virtuais (VPN's), esta tecnologia mascara o endereço IP de um terminal e o criptografa constantemente, tornando o terminal virtualmente indetectável, vide a desvirtuação dos dados originais. Esta técnica de ocultação do IP dificulta a identificação da autoria, restando a materialidade do crime, mas sem o seu genitor (SILVA; CARVALHO, 2025).

Pode-se utilizar como um grande exemplo de navegação anônima em nossa sociedade contemporânea, o próprio navegador TOR - popularmente chamado de *The Onion Router*, por seu logotipo remontar uma 'cebola', reforçando a ideia de camadas - o maior navegador não rastreável devido ao seu elevado nível de criptografia e complexidade, sendo comumente utilizado para acessar sites não disponíveis por meio de navegadores convencionais (como o Google ou Firefox, for exemplo) e, principalmente, para acessar a Deep Web, uma camada mais profunda e nociva da internet (TEIXEIRA; DE LUCENA, 2016). Esta ferramenta, embora legítima, frequentemente é utilizada para acessar conteúdos ilícitos, inclusive conteúdos relacionados à exploração e tráfico de pornografia infantil, motivado exatamente pela dificuldade de rastreio do usuário.

O problema da anonimização é multifacetado e merece uma resposta interdisciplinar e técnica

3 OS IMPACTOS DA ANONIMIZAÇÃO E A INCERTEZA DA AUTORIA NO PRIMEIRO GRAU DE JURISDIÇÃO

A crescente incidência de crimes praticados em ambientes digitais, especialmente aqueles cometidos mediante o uso de ferramentas de anonimização, como redes privadas virtuais (VPNs), aplicações de navegação anônima e perfis falsos, tem imposto desafios relevantes à persecução penal, particularmente no âmbito do primeiro grau de

[120] Modalidade de ataque cibernético que se vale de comunicações falsas como e-mails, mensagens de texto, ligações telefônicas ou páginas eletrônicas fraudulentas, com o objetivo de induzir as vítimas a revelarem informações sigilosas.

jurisdição. A dificuldade de identificação da autoria delitiva repercute diretamente sobre institutos centrais do processo penal, como a justa causa, o recebimento da denúncia e a valoração da prova, exigindo respostas institucionais do Poder Judiciário compatíveis com a complexidade tecnológica desses ilícitos.

No plano institucional, a verificação da justa causa, prevista no art. 395, III, do Código de Processo Penal, não se restringe ao momento decisório, mas envolve um conjunto de atividades desempenhadas pelas unidades judiciárias e pelos setores de apoio responsáveis pela adequada instrução e tramitação dos feitos criminais. A existência de lastro probatório mínimo quanto à materialidade e à autoria delitiva depende, em certa medida, da organização dos autos, da correta classificação das peças, da conferência dos elementos informativos e da gestão documental realizada pelas equipes técnicas que integram a estrutura do Judiciário.

Ainda, no contexto dos crimes cibernéticos, a atuação institucional enfrenta obstáculos específicos decorrentes da natureza da prova digital. Isso pois, a fragmentação dos dados e a volatilidade impõem desafios à padronização de procedimentos, ao controle de prazos e à preservação da cadeia de custódia. Nesse cenário, a eficiência da resposta jurisdicional está diretamente vinculada à capacidade institucional do Judiciário de articular seus setores técnicos, promover a adequada tramitação das requisições judiciais e assegurar a integridade dos elementos probatórios incorporados aos autos.

Tais dificuldades repercutem, por exemplo, no exame de admissibilidade da acusação, especialmente no recebimento da denúncia. Isso porque, ainda que não se exija prova exauriente da autoria ou da materialidade, a análise institucional dessa fase pressupõe que a peça acusatória esteja devidamente instruída e formalmente adequada. Assim, a atuação coordenada das secretarias, cartórios e assessorias técnicas revela-se essencial para evitar a instauração de ações penais fundadas em imputações genéricas ou em elementos informativos insuficientemente organizados, preservando a racionalidade do fluxo processual.

A valoração da prova, por sua vez, também se insere em uma lógica institucional que transcende a decisão judicial em sentido estrito. O sistema do livre convencimento motivado exige que as provas estejam regularmente produzidas e acessíveis ao contraditório, o que depende da correta gestão processual dos autos. Em crimes marcados pela anonimização, o Judiciário é chamado a estruturar rotinas administrativas e técnicas capazes de assegurar a transparência, a rastreabilidade e a confiabilidade desses elementos, evitando sua supervalorização ou uso acrítico.

Dessa forma, a anonimização e a consequente incerteza quanto à autoria delitiva produzem impactos institucionais relevantes no primeiro grau de jurisdição, afetando não apenas a análise dos pressupostos da ação penal, mas também a organização interna e a eficiência do aparelho judicial. A justa causa, o recebimento da denúncia e a valoração da prova devem ser compreendidos de maneira integrada e à luz do modelo constitucional de processo penal, no qual o Poder Judiciário, enquanto instituição, assume papel central na contenção do poder punitivo estatal, por meio de práticas organizacionais,

técnicas e procedimentos compatíveis com as exigências do devido processo legal.

3.1 Morosidade Processual e Proteção Integral da Vítima

A análise da morosidade processual exige, inicialmente, a consideração do expressivo aumento da judicialização no Brasil. Dados divulgados pelo Conselho Nacional de Justiça indicam que, em 2023, o número de novos processos alcançou a marca de 35,3 milhões, o que representa um crescimento de 9,4% em relação ao ano de 2022[121].

O incremento contínuo do volume de demandas judiciais levou à edição do Provimento nº 193/2025, por meio do qual a Corregedoria Nacional de Justiça estabeleceu o prazo de 120 dias corridos para a aferição de eventual morosidade do juízo, decorrente de excesso de prazo nos processos judiciais. A medida tem como finalidade identificar paralisações indevidas em qualquer fase da tramitação processual, reforçando a preocupação institucional com a duração razoável do processo.

Embora a doutrina apresente diversas teorias voltadas à explicação do fenômeno da judicialização no contexto brasileiro, a presente análise, em atenção aos limites e objetivos deste trabalho, concentra-se em examinar os impactos da demora processual sobre as vítimas de crimes cibernéticos, especialmente crianças e adolescentes, cuja proteção integral demanda respostas jurisdicionais céleres e eficazes. Nesses casos, a morosidade assume contornos ainda mais gravosos, uma vez que a proteção integral, princípio estruturante do Estatuto da Criança e do Adolescente[122], exige respostas estatais rápidas e sensíveis à condição peculiar de desenvolvimento dessas vítimas.

Conforme abordado em tópicos anteriores, a utilização de técnicas de anonimização no ambiente digital impacta diretamente o trâmite processual, na medida em que dificulta a identificação do autor da infração penal. Essa dificuldade técnica prolonga a fase investigativa, retarda o oferecimento da denúncia e compromete a efetividade da persecução penal, contribuindo para a sensação de impunidade e para a revitimização daqueles que já se encontram em situação de especial vulnerabilidade.

Além disso, o tratamento dos processos que envolvem crimes cibernéticos, sobretudo quando praticados contra crianças e adolescentes, exige atenção redobrada quanto à preservação da confidencialidade dos dados das partes[123]. A necessidade de sigilo, embora

[121] Informações publicadas em maio de 2025 no site oficial do Conselho Nacional de Justiça.

[122] Lei Nº 8.069/1990: Art. 1º Esta Lei dispõe sobre a proteção integral à criança e ao adolescente.

[123] A tutela do sigilo nos processos que envolvem crianças e adolescentes configura garantia abrangente, fundada na condição especial de pessoas em desenvolvimento, reconhecida pelo art. 227 da Constituição Federal. Tal proteção é concretizada por meio de disposições específicas previstas no Estatuto da Criança e do Adolescente, especialmente no art. 143, bem como no Código de Processo Civil, no art. 189, inciso II, que impõem a restrição da publicidade processual com o objetivo de resguardar a imagem, a intimidade e a honra do menor, sempre à luz do

essencial para a proteção da vítima, frequentemente impõe cautelas procedimentais adicionais que, se não acompanhadas de adequada gestão processual, podem contribuir para a lentidão da tramitação.

A ausência de impulso processual adequado ou a demora excessiva na prática de atos essenciais pode, inclusive, resultar na prescrição da pretensão punitiva estatal, frustrando o direito à justiça das vítimas. Nesse sentido, André Estefam e Victor Eduardo Rios Gonçalves conceituam a prescrição como:

> A prescrição é a perda do direito de punir decorrente do decurso de determinado prazo sem que a ação penal tenha sido proposta por seu titular ou sem que se consiga conclui-la (prescrição da pretensão punitiva), ou, ainda, a perda do direito de executar a pena por não conseguir o Estado dar início ou prosseguimento a seu cumprimento dentro do prazo legalmente estabelecido (prescrição da pretensão executória).

Diante desse cenário, cumpre destacar o relevante trabalho desempenhado pela Unidade Especial de Atuação no Primeiro Grau de Jurisdição (UEA), cuja atuação tem por objetivo minimizar a morosidade processual, seja por meio da padronização de procedimentos, seja pela atuação em forças-tarefa, contribuindo para o aumento da eficiência e da efetividade da prestação jurisdicional.

Todavia, embora os esforços já implementados revelem avanços significativos, permanece evidente a necessidade de adoção de novas políticas judiciárias voltadas ao aprimoramento da gestão processual, à racionalização dos fluxos procedimentais e ao fortalecimento da atuação institucional do Judiciário, especialmente no enfrentamento dos crimes cibernéticos. Apenas por meio de uma atuação coordenada, que leve em consideração as especificidades técnicas desses delitos e a condição peculiar de desenvolvimento das vítimas, será possível reduzir a morosidade, evitar a prescrição e assegurar uma tutela jurisdicional célere, efetiva e compatível com os ditames da proteção integral.

Nesse contexto, ressalta-se que a UEA se mantém firme no compromisso de prestar um serviço jurisdicional de qualidade, atento às demandas contemporâneas e às vulnerabilidades identificadas, atuando de forma estratégica e contínua para mitigar os entraves existentes e promover o aperfeiçoamento da atuação judicial no primeiro grau de jurisdição.

4 DA PREVENÇÃO

No âmbito da política de prevenção prevista pelo Estatuto da Criança e do Adolescente, o artigo 70 estabelece o *dever compartilhado da família, da sociedade e do Estado na proteção integral de crianças e adolescentes contra qualquer forma de violação de direitos*. Deste modo, o artigo 71 do ECA

princípio do melhor interesse da criança e do adolescente.

assume especial relevância ao assegurar o direito ao respeito e à dignidade, reforçado pelas diretrizes do artigo 4, que consagra a prioridade absoluta na efetivação de políticas públicas voltadas ao desenvolvimento saudável do público infantojuvenil.

De forma mais específica, o *art. 71, inc. V*, ao garantir o acesso de crianças e adolescentes a espaços comunitários, culturais, esportivos e de lazer, evidencia a importância desses locais como ambientes seguros de convivência social, capazes de promover o desenvolvimento físico, emocional e social. A ocupação do tempo livre em espaços supervisionados e voltados à interação saudável reduz a exposição excessiva ao ambiente virtual, diminuindo, consequentemente, situações de vulnerabilidade que podem resultar em aliciamento, exploração ou outras modalidades de crimes cibernéticos.

Por sua vez, o *inc. IX* do mesmo dispositivo, reforça a necessidade de políticas públicas e ações educativas voltadas à orientação, formação e conscientização de crianças e adolescentes, inclusive quanto ao uso responsável e seguro de tecnologias. Tais medidas contribuem para o fortalecimento da autonomia crítica, permitindo que o público infantojuvenil reconheça riscos, identifique condutas ilícitas no meio digital e saiba como buscar ajuda diante de situações de ameaça ou violação de direitos.

Logo, a valorização e o incentivo a esses espaços de interação social aliados a ações educativas permanentes, funcionam como instrumentos eficazes de prevenção aos crimes cibernéticos. Ao promover vínculos sociais reais, acompanhamento institucional e educação digital, reduz-se o isolamento social e a dependência exclusiva das relações virtuais, fatores frequentemente explorados por agentes criminosos no ambiente online. As diretrizes previstas no Estatuto da Criança e do Adolescente constituem instrumentos fundamentais para a consolidação de uma política preventiva eficaz, apta a reduzir a incidência de crimes cibernéticos contra crianças e adolescentes, em consonância com o princípio da proteção integral.

CONSIDERAÇÕES FINAIS

A análise desenvolvida ao longo deste artigo evidenciou que os crimes cibernéticos praticados contra crianças e adolescentes configuram um dos mais complexos desafios contemporâneos para o sistema de justiça, em razão da conjugação entre a especial vulnerabilidade das vítimas infantojuvenis e as dificuldades técnicas inerentes ao ambiente digital. A ampliação do uso das tecnologias da informação, embora represente inegáveis avanços sociais, potencializa riscos relevantes à dignidade, à integridade psíquica e ao pleno desenvolvimento de crianças e adolescentes, exigindo respostas jurídicas compatíveis com essa realidade.

Verificou-se que o ordenamento jurídico brasileiro dispõe de um arcabouço normativo robusto, alicerçado na Constituição Federal, no Estatuto da Criança e do Adolescente, no Marco Civil da Internet e na Lei Geral de Proteção de Dados, capaz de assegurar a tutela integral no ambiente digital. Todavia, a efetividade dessa proteção encontra limites práticos relevantes, sobretudo diante do uso de técnicas de anonimização, como VPNs, navegadores anônimos e perfis falsos, que dificultam a identificação da autoria delitiva e impactam diretamente a persecução penal.

Nesse contexto, destacou-se o papel central do primeiro grau de jurisdição, onde se concentram a instrução probatória, a análise da justa causa, o recebimento da denúncia e a valoração da prova. A incerteza quanto à autoria, aliada à volatilidade da prova digital, impõe não apenas desafios decisórios ao magistrado, mas também demandas institucionais relacionadas à gestão processual, à organização dos autos e à articulação entre setores técnicos do Judiciário. A morosidade processual, quando presente, assume contornos ainda mais gravosos nos crimes envolvendo vítimas infantojuvenis, pois pode gerar revitimização, sensação de impunidade e até a frustração da pretensão punitiva estatal pela prescrição.

Diante desse cenário, a atuação institucional do Judiciário revela-se elemento indispensável para a concretização do princípio da proteção integral. Iniciativas voltadas à padronização de procedimentos, à racionalização dos fluxos processuais e ao fortalecimento da gestão judiciária mostram-se fundamentais para enfrentar os entraves decorrentes da complexidade tecnológica desses delitos. Nesse sentido, merece especial destaque o trabalho desenvolvido pela Unidade Especial de Atuação no Primeiro Grau de Jurisdição (UEA), que se mantém firme no compromisso de prestar um serviço jurisdicional de qualidade, atuando de forma estratégica para minimizar a morosidade processual, aprimorar a eficiência institucional e mitigar os problemas identificados na tramitação dos feitos.

Por fim, conclui-se que o enfrentamento dos crimes cibernéticos contra crianças e adolescentes exige uma atuação integrada e multidimensional, que articule repressão penal eficaz, gestão judiciária eficiente e políticas preventivas contínuas, conforme preconiza o Estatuto da Criança e do Adolescente. Somente por meio de uma resposta coordenada entre Estado, sociedade, família e instituições do sistema de justiça será possível assegurar uma tutela jurisdicional célere, efetiva e sensível à condição peculiar de desenvolvimento das vítimas, reafirmando, no ambiente digital, os princípios constitucionais da dignidade da pessoa humana, da proteção integral e da prioridade absoluta.

REFERÊNCIAS BIBLIOGRÁFICAS

ALENCAR, Mariana. *Crimes cibernéticos e meios de prova.* JusBrasil, 26 nov. 2016. Disponível em: https://www.jusbrasil.com.br/artigos/crimes-ciberneticos-e-meios-de-prova/643636447. Acesso em: 15 dez. 2025.

BRASIL. CONSELHO NACIONAL DE JUSTIÇA - CNJ. *Relatório Analítico*: justiça em números. Brasília, DF: CNJ, 2025. Disponível em: justica-em-numeros-2025.pdf. Acesso em: 17 dez. 2025.

CONSELHO NACIONAL DE JUSTIÇA – CNJ. *Corregedoria Nacional fixa prazo de 120 dias para avaliar morosidade de unidades judiciais*. Brasília, 22 maio 2025. Disponível em: https://www.cnj.jus.br/corregedoria-nacional-fixa-prazo-de-120-dias-para-avaliar-morosidade-de-unidades-judiciais/. Acesso em: 16 dez. 2025.

COSTA, Aldo de Campos. *A toda prova: a justa causa para o exercício da ação penal*. Consultor Jurídico – ConJur, São Paulo, 29 nov. 2013. Disponível em: https://www.conjur.com.br/2013-nov-29/toda-prova-justa-causa-exercicio-acao-penal/. Acesso em: 15 dez. 2025.

ESTEFAM, André; GONÇALVES, Victor Eduardo Rios; LENZA, Pedro. *Coleção esquematizado – Direito Penal* – Parte Geral. 14ª ed. São Paulo: Saraiva Jur. 2025

GRECO, Rogério. *Curso de Direito Penal*: artigos 1º a 120 do código penal. v.1. Grupo GEN, 2023. E-book.

MACHADO, Diego; DONEDA, Danilo. Direito ao anonimato na internet: fundamentos e contornos

dogmáticos de sua proteção no direito brasileiro (Right to Anonymity on the Internet: Foundations and Legal Outlines for Its Protection in the Brazilian Law). Revista de Direito Civil Contemporâneo, v. 23, ano 7, p. 95-140, 2020. Disponível em: https://ssrn.com/abstract=3698938. Acesso em: 15 dez. 2025

SIEPIERSKI, Ana Luiza; SILVA, Renata Celeste Sales. CRIMES CIBERNÉTICOS: A POSSIBILIDADE DE RELATIVIZAÇÃO DO ANONIMATO. Portal de Trabalhos Acadêmicos, *[S. l.]*, v. 8, n. 2, 2022. Disponível em: https://revistas.faculdadedamas.edu.br/index.php/academico/article/view/2204. Acesso em: 16 dez. 2025.

OLIVEIRA, Anderson Kenet de; FARIA JUNIOR, Valter da Conceição; CRISTALDO, Vander Martins. Anonimização como possível evidência de encerramento do tratamento de dados pessoais: uma análise jurídica, técnica e estratégica. Migalhas – De Peso, 11 ago. 2025. Disponível em: https://www.migalhas.com.br/depeso/436393/anonimizacao-como-evidencia-final-do-tratamento-de-dados-pessoais. Acesso em: 16 dez. 2025.

SILVA, Moacir Antunes; CARVALHO, Urssula Rodrigues. Análise sobre as dificuldades de investigação relacionadas aos crimes cibernéticos de estelionato na rede social whatsapp. Revista Científica UNIFAGOC, v. 7, n. 2, 2022. Disponível em: https://revista.unifagoc.edu.br/juridico/article/view/1120. Acesso em: 16 dez. 2025.

SOUZA, Andrea Sant'ana Leone; FERRARO, Angelo Viglianisi;

TAVARES, André Ramos. *Curso de Direito Constitucional.* 23ª ed. São Paulo: Saraiva Jur,2025.

TEIXEIRA, Daniel Ruiz; DE LUCENA, Sidney Cunha. A REDE TOR: NO LIMITE ENTRE A DESOBEDIÊNCIA CIVIL E A DELINQUENCIA. 2016. Disponível em: https://bsi.uniriotec.br/wp-content/uploads/sites/31/2020/05/201612Daniel Ruiz.pdf. Acesso em: 15 dez. 2025.

TEIXEIRA, Lara Domingos; SANTOS, João Victor de; GONÇALVES, Érica Oliveira santos. PERFIS FALSOS CRIADOS NO CIBERESPAÇO:: análise das hipóteses e enquadramento em falsa identidade, falsidade ideológica ou estelionato. *Revista Multidisciplinar do Nordeste Mineiro, [S. l.]*, v. 7, n. 1, 2023. Disponível em: https://remunom.ojsbr.com/multidisciplinar/article/view/1117. Acesso em: 16 dez. 2025.

THOMÉ, Caio Érik Pereira. *A problemática sobre a apuração da autoria nos crimes cibernéticos e a atuação dos núcleos especializados de investigação. 2023.* Trabalho de Conclusão de Curso (Bacharelado em Direito) – Fundação Universidade Federal de Mato Grosso do Sul (UFMS), Campo Grande, 2023. Disponível em: https://repositorio.ufms.br/handle/123456789/7369. Acesso em: 15 dez. 2025.

TOMASEVICIUS FILHO, Eduardo (coord.). *Estatuto da Criança e do Adolescente: entre a efetividade dos direitos e o impacto das novas tecnologias*. São Paulo: Almedina, 2022.

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS. Ação penal. *Doutrina na Prática.* Disponível em: https://www.tjdft.jus.br/consultas/jurisprudencia/jurisprudencia-em-temas/a-doutrina-na-pratica/acao-penal/acao-penal. Acesso em: 15 dez. 2025.