

**III CONGRESSO INTERNACIONAL  
DE DIREITO, POLÍTICAS PÚBLICAS,  
TECNOLOGIA E INTERNET**

**DIREITO PENAL E CIBERCRIMES II**

---

D598

Direito penal e cibercrimes II [Recurso eletrônico on-line] organização III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet: Faculdade de Direito de Franca – Franca;

Coordenadores: Renan Posella Mandarino, Fábio Cantizani Gomes e Ana Carolina de Sá Juzo – Franca: Faculdade de Direito de Franca, 2025.

Inclui bibliografia

ISBN: 978-65-5274-364-0

Modo de acesso: [www.conpedi.org.br](http://www.conpedi.org.br) em publicações

Tema: Governança, regulação e o futuro da inteligência artificial.

1. Direito. 2. Políticas Públicas. 3. Tecnologia. 4. Internet. I. III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet (1:2025 : Franca, SP).

CDU: 34

---

# **III CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET**

## **DIREITO PENAL E CIBERCRIMES II**

---

### **Apresentação**

Entre os dias 30 de setembro e 3 de outubro de 2025, a Faculdade de Direito de Franca recebeu o III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet. O evento reuniu acadêmicos, profissionais, pesquisadores e estudantes, promovendo o debate interdisciplinar sobre o impacto das inovações tecnológicas no campo jurídico e nas políticas públicas. A programação envolveu Grupos de Trabalho (GTs) organizados para aprofundar temas específicos, abordando desde o acesso à justiça até as complexidades da regulação tecnológica, com ênfase na adaptação do sistema jurídico aos avanços da inteligência artificial e da automação.

O GT 9 foca nos crimes digitais e na responsabilização penal de condutas praticadas em ambiente virtual. As pesquisas discutem pornografia não consentida, cyberbullying, discursos de ódio e a eficácia das investigações digitais. O grupo ressalta a necessidade de adequação legislativa e de políticas públicas voltadas à prevenção e repressão dos cibercrimes.

## **ATUAÇÃO DO DIREITO PENAL EM CIBERCRIMES CONTRA CRIANÇAS E ADOLESCENTES: REDES SOCIAIS, DEEP WEB E DARK WEB**

### **CRIMINAL LAW AND THE FIGHT AGAINST CYBERCRIMES TARGETING CHILDREN AND ADOLESCENTS: THE CONTEXT OF SOCIAL MEDIA, THE DEEP WEB, AND THE DARK WEB**

**Rubens Chioratto Junior <sup>1</sup>**  
**Marjorie Luana Aquino Alonso <sup>2</sup>**

#### **Resumo**

O artigo busca esclarecer o que são cibercrimes contra crianças e adolescentes e analisar a atuação do Direito Penal frente aos cibercrimes cometidos contra esse público infantojuvenil, com ênfase nos crimes praticados por meio das redes sociais, da deep web e da dark web. Diante da vulnerabilidade desse público no ambiente digital, discute-se a eficácia das normas penais e das políticas públicas de proteção, bem como os desafios tecnológicos enfrentados pelas autoridades, famílias e sociedade. Conclui-se que a atuação estatal, somada à responsabilidade das plataformas digitais e à educação digital preventiva, é essencial para garantir a segurança infantojuvenil online.

**Palavras-chave:** Palavras-chave: cibercrimes, Direito penal, Criança e adolescente, Proteção digital, Social media, Dark web

#### **Abstract/Resumen/Résumé**

This article aims to clarify the nature of cybercrimes committed against children and adolescents and to analyze the role of Criminal Law in addressing such offenses, with particular emphasis on crimes perpetrated through social media. Given the increased vulnerability of this age group in digital environments, the study discusses the effectiveness of criminal norms and public protection policies, as well as the technological challenges faced by authorities, families, and society. The research concludes that effective state intervention, combined with the accountability of digital platforms and preventive digital education, is essential to ensuring the online safety of children and adolescents.

**Keywords/Palabras-claves/Mots-clés:** Keywords: cybercrime, Criminal law, Children and adolescents, Digital protection, Social media, Dark web

---

<sup>1</sup> Psicólogo e aluno do curso de Direito da UNESP - Franca

<sup>2</sup> aluna do curso de Direito da UNESP de Franca

## **1. INTRODUÇÃO**

A crescente digitalização da vida cotidiana trouxe inúmeros benefícios, mas também elevou consideravelmente os riscos de exposição de crianças e adolescentes a crimes virtuais. Nesse cenário, destaca-se a importância de se compreender a atuação do Direito Penal como instrumento de proteção contra condutas criminosas praticadas no meio digital, notadamente nas redes sociais, deep web e dark web.

Atualmente, crianças e adolescentes utilizam o ambiente digital como entretenimento, estudo e busca de informações. Contudo, esse ambiente também traz consigo uma série de desafios e riscos específicos, aos quais esse público é particularmente vulnerável, de forma especial, no que se refere a cibercrimes. Assim, torna-se fundamental compreender como o Direito Penal atua para protegê-los e quais são as principais ameaças existentes neste contexto.

## **2. METODOLOGIA**

Este estudo tem por objetivo compreender as ameaças enfrentadas por crianças e adolescentes no ambiente digital, analisar os principais desafios da repressão penal aos cibercrimes e discutir medidas legislativas e estratégias de aprimoramento da proteção infantojuvenil online.

Para tanto, utilizou-se a pesquisa bibliográfica, com base na legislação brasileira vigente e nas obras de Diego Canabarro (2021) e Fabrício B. de Oliveira (2022), que são referências no tema em questão e, que abordam, respectivamente, os aspectos substantivos e processuais dos crimes cibernéticos.

Canabarro (2021), aborda de forma atualizada e crítica os desafios do Direito Penal diante das novas formas de criminalidade no ambiente digital. Examina os tipos penais relacionados aos cibercrimes, destacando questões como tipicidade, bem jurídico tutelado e adequação normativa. O autor também discute a evolução legislativa brasileira e internacional no enfrentamento dos crimes cibernéticos, incluindo temas como invasão de dispositivos informáticos, fraudes digitais e delitos contra a honra na internet.

Já, Fabrício Oliveira (2022) oferece uma análise abrangente dos crimes cometidos no ambiente virtual, com foco não só na parte penal, mas também nos aspectos processuais. A obra se destaca pela abordagem prática e detalhada de temas como a produção de provas digitais, cooperação internacional, competência jurisdicional e medidas cautelares no processo penal. A 4ª edição atualiza o conteúdo frente às mudanças legislativas e jurisprudenciais recentes, serve como referência para quem atua na investigação, acusação ou defesa em casos de crimes cibernéticos.

### **3. O DIREITO PENAL E A PROTEÇÃO INFANTOJUVENIL NO AMBIENTE DIGITAL**

O Direito Penal tem buscado se adaptar à realidade digital com o objetivo de coibir crimes que afetam crianças e adolescentes na internet. A legislação brasileira conta com dispositivos no Código Penal, no Estatuto da Criança e do Adolescente (Lei nº 8.069/1990), na Lei nº 12.965/2014 (Marco Civil da Internet) e na Lei nº 13.709/2018 (LGPD), que estabelecem bases para a responsabilização penal e civil de condutas lesivas.

Além disso, a Resolução nº 245/2024 do Ministério dos Direitos Humanos e da Cidadania reforça a responsabilidade de autoridades públicas, famílias, escolas e empresas na promoção de um ambiente digital seguro. Entre os crimes combatidos estão: produção e divulgação de material de abuso sexual infantil (CSAM), aliciamento (grooming), sextorsão, cyberbullying, entre outros.

### **4. A DARK WEB E A EXPLORAÇÃO INFANTIL**

A dark web é uma parte da internet inacessível por navegadores convencionais e utilizada para práticas criminosas devido ao seu alto grau de anonimato. Através de softwares como o Tor, criminosos encontram um ambiente propício para compartilhar conteúdos ilegais e explorar sexualmente crianças e adolescentes. E, é principalmente, a *dark web* que os criminosos utilizam para cometer hediondos crimes contra crianças e adolescentes.

Reconhecendo a vulnerabilidade de crianças e adolescentes nesse contexto. A legislação é instrumentalizada para punir os atos de violência física e outras formas de exploração e abuso que ocorrem através da internet. Entre os principais crimes praticados nesse espaço destacam-se a produção, posse e divulgação de material de abuso sexual infantil, o aliciamento (*grooming*), o assédio e a extorsão; condutas essas que esclarecemos o que é abaixo.

A produção e compartilhamento de material de abuso sexual infantil (CSAM) na *dark web* é um centro para a criação e disseminação desse tipo de conteúdo, permitindo que agressores troquem informações e materiais de forma "oculta".

O aliciamento e tráfico de pessoas é facilitado na *dark web* pelo anonimato e, é usada por criminosos para aliciar crianças e adolescentes, seja para exploração sexual, trabalho forçado ou outras formas de abuso. Ainda, no ambiente da dark web, pode ser feita a negociação e o "comércio" das vítimas.

Os fóruns e comunidades para pedófilos, podem ser entendidos, como grupos e fóruns na dark web onde criminosos e agressores se reúnem para discutir estratégias de exploração, compartilhar experiências e incentivar a prática de crimes.

O Conteúdo perigoso e extremista, normalmente vão além dos crimes sexuais, a dark web também pode expor crianças e adolescentes a conteúdo violento, extremista ou que promova automutilação e suicídio, o que pode ter impactos psicológicos graves em todos os envolvidos.

Essas práticas não apenas violam direitos fundamentais, como também causam danos psicológicos e físicos irreparáveis. A dificuldade de rastreamento dos agressores representa um obstáculo à efetividade das ações repressivas, exigindo cooperação internacional e uso de técnicas avançadas de investigação forense digital.

## **5. REDES SOCIAIS COMO MEIO DE PRÁTICA DE CIBERCRIMES**

As redes sociais, apesar de suas potencialidades pedagógicas e comunicacionais, têm sido palco de diversas formas de violência digital. A facilidade de interação e o número massivo de usuários tornam essas plataformas vulneráveis a práticas como *cyberbullying* e assédio online; aliciamento (*grooming*); sextorsão sexual ou sextorsão financeira; disseminação de conteúdo impróprio; desafios perigosos e jogos online; vazamento de dados e fraudes.

O *cyberbullying* e assédio online são ofensas reiteradas que provocam sérios problemas sociais e emocionais, que podem levar ao abandono da escola, isolamento social, ansiedade, depressão e até suicídio. Ocorre quando crianças e adolescentes são frequentemente vítimas de intimidação, humilhação e ameaças por meio de mensagens, comentários ou publicações em redes sociais.

O aliciamento ou *Grooming*, visa a manipulação de menores para obtenção de favores sexuais. Os predadores se utilizam das redes sociais para se aproximar de crianças e adolescentes, construindo uma relação de confiança para, posteriormente, abusá-los ou explorá-los sexualmente. Eles podem se passar por amigos ou pessoas da mesma idade, usando táticas de manipulação.

A sextorsão pode se caracterizar de duas formas, a tradicional e a financeira, ambas feitas por ameaças de divulgação de imagens íntimas para obter novos conteúdos íntimos ou dinheiro. A tradicional é quando o criminoso quer obter novos conteúdos íntimos e a sextorsão financeira ele exige recursos financeiros para não divulgar as imagens. Dessas formas, crianças e adolescentes podem ser coagidos a produzir ou enviar esse tipo de conteúdo ou dinheiro.

Os desafios perigosos são atividades que incentivam automutilação e condutas de risco. São caracterizados por jogos online usados por grupos criminosos que podem se organizar em plataformas criptografadas para promover desafios e competições com conteúdo de ódio e extremismo, levando crianças e adolescentes a práticas perigosas que podem levar a acidentes graves, ou mesmo, a condutas como assassinato ou o suicídio.

O vazamento de dados se caracteriza pela utilização de informações pessoais para fraudes. Ocorre quando informações pessoais de crianças e adolescentes podem ser obtidas e utilizadas para fins maliciosos, como roubo de identidade ou fraudes financeiras.

Esses crimes exigem medidas repressivas eficazes e políticas públicas que promovam a educação digital, a fiscalização parental, o monitoramento das plataformas e o fortalecimento de mecanismos de denúncia e resposta rápida.

## **6. A IMPORTÂNCIA DA ATUAÇÃO MULTISSETORIAL**

A repressão aos crimes digitais contra crianças e adolescentes não deve se limitar à atuação penal. É imprescindível que o Estado, por meio do Poder Legislativo, atualize constantemente a legislação, tornando-a eficaz e adequada à dinamicidade do ambiente virtual.

Ademais, a educação digital nas escolas, a conscientização dos pais e responsáveis, a regulamentação das plataformas e a participação da sociedade civil são pilares fundamentais de uma política ampla de proteção. As próprias empresas de tecnologia devem adotar mecanismos robustos de moderação de conteúdo e ferramentas de segurança voltadas ao público infantojuvenil.

## **7. CONSIDERAÇÕES FINAIS**

Portanto, a atuação do Direito Penal nos casos de cibercrimes contra crianças e adolescentes é um instrumento essencial, mas que, isoladamente, não resolve a complexidade do problema. Diante da crescente exposição dos menores ao ambiente digital, faz-se necessária uma abordagem integrada, que envolva não apenas repressão penal, mas também prevenção, educação e responsabilização de todos os atores envolvidos.

E, a proteção da infância e adolescência no ciberespaço deve ser compreendida como uma responsabilidade coletiva, contínua e permanente, que exige atualização legislativa, investimento em tecnologia, políticas públicas eficazes e o comprometimento ético das plataformas digitais.



Além disso, o tema é de grande relevância social, considerando, inclusive a ascensão das redes sociais e a manutenção do bem-estar e da saúde mental e social das crianças e adolescentes.

## 8. REFERÊNCIAS

- BRASIL. **Código Penal**. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Disponível em: <https://www.planalto.gov.br>. Acesso em: 3 jul. 2025.
- BRASIL. **Estatuto da Criança e do Adolescente**. Lei nº 8.069, de 13 de julho de 1990. Disponível em: <https://www.planalto.gov.br>. Acesso em: 30 jun. 2025.
- BRASIL. **Lei Geral de Proteção de Dados Pessoais – LGPD**. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: <https://www.planalto.gov.br>. Acesso em: 2 jul. 2025.
- BRASIL. **Marco Civil da Internet**. Lei nº 12.965, de 23 de abril de 2014. Disponível em: <https://www.planalto.gov.br>. Acesso em: 2 jul. 2025.
- BRASIL. **Resolução nº 245, de 16 de janeiro de 2024**. Ministério dos Direitos Humanos e da Cidadania. Dispõe sobre medidas de proteção digital para crianças e adolescentes. Disponível em: <https://www.planalto.gov.br>. Acesso em: 30 jun. 2025.
- CANABARRO, Diego. **Cibercrimes e Direito Penal**. São Paulo: Revista dos Tribunais, 2021.
- OLIVEIRA, Fabrício B. de. **Crimes na Internet: aspectos penais e processuais**. 4. ed. São Paulo: Saraiva, 2022.