# 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 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.

# A INFLUÊNCIA DO DIREITO DIGITAL NO DIREITO PENAL

# THE INFLUENCE OF DIGITAL LAW ON CRIMINAL LAW

**Breno Carvalho Lopes de figueiredo**
**Gabriela Rodrigues Pazelli**

**Resumo**

O avanço digital transformou o Direito Penal, impondo novos desafios como fake news, crimes cibernéticos, uso ilícito de criptomoedas e a responsabilidade das plataformas digitais. O Direito Digital busca responder a essas questões por meio de legislações, jurisprudência e doutrina. O projeto analisa esses impactos, destacando a necessidade de atualização legislativa, equilíbrio entre repressão e direitos fundamentais, e cooperação internacional. A pesquisa adota método dedutivo, abordando casos concretos e propondo soluções jurídicas que integrem tecnologia, ética e regulação, visando um sistema penal eficaz e adaptado à era digital.

**Palavras-chave:** Crimes cibernéticos, Fake news, Criptomoedas

**Abstract/Resumen/Résumé**

Digital advances have transformed Criminal Law, posing new challenges such as fake news, cybercrimes, illicit use of cryptocurrencies and the liability of digital platforms. Digital Law seeks to respond to these issues through legislation, case law and doctrine. The project analyzes these impacts, highlighting the need for legislative updates, a balance between repression and fundamental rights, and international cooperation. The research adopts a deductive method, addressing specific cases and proposing legal solutions that integrate technology, ethics and regulation, aiming at an effective criminal system adapted to the digital age.

**Keywords/Palabras-claves/Mots-clés:** Cybercrimes, Fake news, Cryptocurrencies

## Introdução

O avanço das tecnologias digitais transformou as relações sociais, econômicas e jurídicas, trazendo novos desafios ao Direito Penal. O Direito Digital, como ramo emergente, busca regulamentar as interações no ambiente virtual, enquanto o Direito Penal enfrenta a necessidade de adaptar seus conceitos tradicionais para lidar com fenômenos como fake news, crimes cibernéticos, o uso de criptomoedas e blockchain em práticas ilícitas e a responsabilidade das plataformas digitais. Este resumo expansivo, baseado no projeto de pesquisa da Faculdade de Direito de Franca, analisa como o Direito Digital influencia o Direito Penal, examinando os problemas de pesquisa propostos: o impacto das fake news em casos criminais, os desafios das novas tecnologias, a tipificação de crimes cibernéticos e a responsabilidade jurídica das plataformas. A análise utiliza o método dedutivo, com base em legislação, jurisprudência, casos concretos e doutrina, visando oferecer uma reflexão crítica sobre esses temas.

Assim a revolução digital trouxe benefícios, mas também desafios jurídicos significativos. A disseminação de fake news compromete a integridade de processos criminais, manipulando a opinião pública e influenciando julgamentos. Tecnologias como criptomoedas e blockchain, por sua natureza descentralizada e anônima, são usadas em crimes como lavagem de dinheiro e fraudes, desafiando a rastreabilidade penal. Os crimes cibernéticos, como invasão de dispositivos e estelionato digital, exigem atualizações no Código Penal, que, apesar de avanços como a Lei Carolina Dieckmann (Lei nº 12.737/2012), ainda apresenta lacunas. Por fim, a responsabilidade das plataformas digitais gera debates sobre o equilíbrio entre liberdade de expressão, privacidade e prevenção de crimes. Este resumo aborda esses quatro eixos, detalhando suas implicações penais.

## Análise dos Problemas

### Como o Direito Digital Pode Influenciar as Fake News em Casos Criminais?

As fake news, ou notícias falsas, são informações fabricadas ou distorcidas, disseminadas intencionalmente para manipular opiniões ou causar prejuízos. No contexto penal, elas afetam diretamente o devido processo legal, comprometendo investigações, influenciando jurados e criando julgamentos paralelos nas redes sociais. O Direito Digital busca mitigar esses impactos por meio de regulamentações e ferramentas tecnológicas que são:

Impactos no Processo Penal por meio das seguintes formas: 1. Comprometimento de Investigações: Fake news podem desviar o foco de inquéritos policiais, como em casos de linchamentos virtuais baseados em boatos; 2. Influência em Julgamentos: A exposição de informações falsas nas redes sociais pode pressionar juízes ou jurados, violando a imparcialidade (ex.: caso Marielle Franco, com desinformação sobre os acusados); e 3. Dano à Reputação: Vítimas ou réus podem sofrer difamação ou calúnia amplificada pelo alcance digital.

Resposta do Direito Digital por meio de: 1. Legislação Aplicável: No Brasil, fake news em casos criminais podem ser enquadradas como calúnia (art. 138, CP), difamação (art. 139, CP) ou injúria (art. 140, CP). A disseminação de desinformação com fins

discriminatórios pode configurar crime previsto na Lei nº 7.716/1989 (art. 20, §2º); 2. Marco Civil da Internet (Lei nº 12.965/2014): Determina que plataformas digitais removam conteúdos ilícitos após ordem judicial (art. 19), mas não impõe monitoramento proativo; e 3. Propostas Legislativas: O PL das Fake News (PL 2.630/2020, ainda em tramitação em 2025) propõe maior responsabilidade das plataformas na moderação de desinformação, com sanções administrativas.

Porém essas alternativas trazem desafios como: A liberdade de expressão (art. 5º, IX, CF) limita a criminalização de fake news, exigindo um equilíbrio com a proteção contra danos e A identificação de autores é dificultada pelo anonimato digital.

Assim trazemos um exemplo prático para melhor entendimento: Em 2023, a disseminação de fake news sobre um suposto crime em uma cidade do interior de São Paulo levou a ataques virtuais contra um inocente, configurando difamação (art. 139, CP) e constrangimento ilegal (art. 146, CP).

**Qual o Impacto das Novas Tecnologias, como Criptomoedas e Blockchain, no Direito Penal?**

As criptomoedas (ex.: Bitcoin, Ethereum) e a tecnologia blockchain (um registro descentralizado e imutável) revolucionaram transações financeiras, mas também facilitaram crimes como lavagem de dinheiro, evasão de divisas e fraudes. O anonimato e a ausência de regulação centralizada desafiam o Direito Penal.

No uso em Práticas Ilícitas temos os seguintes exemplos: Lavagem de Dinheiro (Lei nº 9.613/1998): Criptomoedas são usadas para ocultar a origem de recursos ilícitos, como em esquemas de ransomware (ex.: criminosos exigem pagamento em Bitcoin); Evasão de Divisas (Lei nº 7.492/1986, art. 22): Transferências internacionais via blockchain burlam controles fiscais; e Fraudes Financeiras (art. 171, CP): Esquemas de pirâmide com criptomoedas (ex.: “pump and dump”) enganam investidores.

O que traz desafios penais para as autoridades como: Rastreabilidade: A descentralização do blockchain dificulta identificar transações ilícitas, exigindo cooperação internacional (ex.: Convenção de Budapeste); Tipificação: O CP não possui tipos penais específicos para crimes com criptomoedas, enquadrando-os em crimes tradicionais (ex.: estelionato, art. 171); e Prova Digital: A coleta de evidências em blockchain exige expertise técnica, como análise de carteiras digitais.

A melhor solução é a criação de respostas jurídicas como: Regulamentação: A Receita Federal (Instrução Normativa nº 1.888/2019) exige declaração de transações com criptomoedas, auxiliando no combate à lavagem de dinheiro; Cooperação Internacional: O Brasil, signatário da Convenção de Budapeste, troca informações com outros países para rastrear transações ilícitas; e Jurisprudência: Casos como a Operação Kryptos (2021) demonstram condenações por lavagem de dinheiro com Bitcoin, usando o art. 1º da Lei nº 9.613/1998.

As quais podemos ver através do seguinte exemplo prático: Um grupo criminoso usa Bitcoin para receber resgates de ransomware, configurando lavagem de dinheiro (art. 1º, Lei nº 9.613/1998) e extorsão (art. 158, CP).

**Quais São os Principais Crimes Cibernéticos Enquadrados no Código Penal?**

Os crimes cibernéticos são condutas ilícitas praticadas no ambiente digital, divididas em crimes próprios (exclusivos do meio virtual) e crimes comuns (praticados via internet). O CP foi atualizado por leis como a Lei nº 12.737/2012 e a Lei nº 14.155/2021, mas lacunas persistem. Como:

Crimes Próprios: Invasão de Dispositivo Informático (art. 154-A, CP): Acessar dispositivo sem autorização para obter ou adulterar dados. Pena: 1 a 4 anos; qualificado (ex.: obtenção de dados sensíveis), 2 a 5 anos. Exemplo: Hackear um celular para roubar fotos pessoais. Crimes Comuns no Ambiente Digital: 1. Estelionato Eletrônico (art. 171, §2º-A, CP): Fraudar via internet para obter vantagem ilícita. Pena: 4 a 8 anos, com aumento para vítimas vulneráveis; 2. Calúnia, Difamação e Injúria (arts. 138, 139, 140, CP): Ofensas à honra em redes sociais. Penas variam de 6 meses a 3 anos; 3. Induzimento a Suicídio/Automutilação (art. 122, CP): Incentivar suicídio ou automutilação via plataformas digitais. Pena: 6 meses a 6 anos, dependendo do resultado; 4. Ameaça (art. 147, CP): Ameaçar via WhatsApp ou e-mail. Pena: 1 a 6 meses; 5. Extorsão (art. 158, CP): Chantagear com dados roubados. Pena: 4 a 7 anos e Falsidade Ideológica (art. 299, CP): Criar perfis falsos. Pena: 1 a 5 anos.

Legislações Especiais: Lei nº 12.737/2012: Introduziu o art. 154-A, tipificando invasão de dispositivos; Lei nº 14.155/2021: Agravou penas para crimes digitais, como estelionato eletrônico e ECA (art. 241): Criminaliza pornografia infantil no ambiente digital.

Ainda possui lacunas como: Crimes como deepfakes ou ataques de ransomware ainda carecem de tipificação específica, sendo enquadrados em tipos genéricos (ex.: art. 171 ou 158, CP).

Como o exemplo a seguir: Um golpista clona um site de banco e induz vítimas a transferir dinheiro, configurando estelionato eletrônico (art. 171, §2º-A).

**Como o Direito Penal Trata a Responsabilidade de Plataformas Digitais?**

A responsabilidade penal das plataformas digitais (ex.: redes sociais, aplicativos de mensagens) é um tema controverso, pois o Direito Penal brasileiro foca na responsabilização de pessoas físicas e, excepcionalmente, pessoas jurídicas (art. 225, §3º, CF, para crimes ambientais).

Marco Civil da Internet (Lei nº 12.965/2014): Regra Geral: Plataformas (provedores de aplicação) não respondem por conteúdos de usuários, salvo se descumprirem ordens judiciais para remoção (art. 19). Exceções: Pornografia Infantil: Dever de notificar autoridades (art. 241-D, ECA) e Conivência: Gestores podem responder penalmente por omissão ou dolo (ex.: facilitar crimes). Como o exemplo a seguir: O Facebook não é penalmente responsável por uma injúria racial postada por um usuário, a menos que ignore ordem judicial para removê-la.

Responsabilidade Penal: Pessoas Jurídicas: Não há responsabilidade penal direta para crimes cibernéticos, mas representantes podem responder por crimes como receptação (art. 180, CP) ou associação criminosa (art. 288, CP) se facilitarem ilícitos. Conforme

exemplo: Um marketplace que permite venda de produtos falsificados, sabendo da ilicitude, pode implicar seus administradores em receptação qualificada. Já a Convenção de Budapeste: Exige que plataformas preservem dados para investigações, mas a não cooperação gera sanções administrativas, não penais com a seguinte jurisprudência: O STJ (REsp 1.692.023/SP) exige proatividade apenas em casos graves, como pornografia infantil.

Com os seguintes desafios: Anonimato: Dificulta identificar usuários criminosos e liberdade de expressão: Moderação excessiva pode violar direitos constitucionais. Exemplo Prático: Um aplicativo de mensagens que não fornece logs de acesso em um caso de tráfico de drogas enfrenta multas, mas não responsabilidade penal direta.

**Metodologia do Projeto**

O projeto adota o método dedutivo, partindo de normas gerais (CP, Marco Civil, LGPD) para analisar casos específicos. Os procedimentos incluem:

Análise Legislativa: Estudo do CP, Lei nº 12.737/2012, Lei nº 14.155/2021, Marco Civil da Internet e LGPD.

Jurisprudência: Exame de decisões do STF e STJ sobre fake news, criptomoedas e plataformas.

Casos Concretos: Análise de casos notórios, como a Operação Kryptos (criptomoedas) ou linchamentos virtuais por fake news.

Revisão Doutrinária: Consulta a autores como Renan Nascimento, Paula Cristina de Oliveira, Andreas Schmidt e Danilo Doneda.

**Referências Preliminares Comentadas**

- **Nascimento (2021)**: Analisa a insuficiência do CP para criminalizar fake news, sugerindo enquadramento em crimes contra a honra.
- **Oliveira (2020)**: Discute a evolução dos crimes cibernéticos e a necessidade de tipificações específicas.
- **Schmidt (2021)**: Explora o uso de blockchain em crimes financeiros, destacando desafios de rastreamento.
- **Allen (2021)**: Debate a responsabilidade de plataformas, criticando a imunidade excessiva.
- **Doneda (2019)**: Contextualiza a LGPD e sua interface com crimes digitais, como roubo de dados.

**Análise Crítica**

Fake News: A ausência de um tipo penal específico dificulta a repressão, mas a aplicação de crimes contra a honra é limitada pelo alcance viral da desinformação.

Criptomoedas/Blockchain: A regulação incipiente e o anonimato exigem maior cooperação internacional e capacitação técnica.

Crimes Cibernéticos: As Leis nº 12.737/2012 e 14.155/2021 foram avanços, mas crimes emergentes (ex.: deepfakes) demandam novas tipificações.

Plataformas: O Marco Civil protege plataformas, mas a falta de proatividade na moderação pode perpetuar ilícitos. O PL das Fake News pode mudar esse cenário.

Perspectiva Crítica: O Direito Penal enfrenta um conflito entre repressão eficaz e proteção de direitos fundamentais, exigindo um equilíbrio delicado.

**Conclusão**

A influência do Direito Digital no Direito Penal é profunda, exigindo uma reestruturação de paradigmas para enfrentar os desafios do ambiente virtual. Este projeto de pesquisa, ao abordar fake news, criptomoedas/blockchain, crimes cibernéticos e responsabilidade das plataformas digitais, revela a complexidade de adaptar o sistema penal a uma realidade tecnológica em constante evolução.

Este estudo, ao adotar o método dedutivo, oferece uma análise crítica das interseções entre Direito Digital e Penal, contribuindo para o debate acadêmico e legislativo. A análise de casos concretos, jurisprudência e doutrina revela que o Brasil avançou, mas precisa de maior agilidade regulatória. O projeto destaca a importância de um Direito Penal adaptado ao século XXI, que proteja a sociedade sem comprometer a democracia digital.

Assim a influência do Direito Digital no Direito Penal é um processo em construção, marcado por avanços (ex.: Leis nº 12.737/2012, 14.155/2021) e desafios. A integração de tecnologia, legislação e ética é essencial para enfrentar fake news, crimes cibernéticos, criptomoedas e a responsabilidade das plataformas. Este projeto reforça a necessidade de um diálogo interdisciplinar, envolvendo juristas, tecnólogos e policymakers, para construir um sistema penal justo e eficaz no ambiente virtual.

**Franca 2025**