# II CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

## DIREITO PENAL E CIBERCRIMES

D598
Direito penal e cibercrimes [Recurso eletrônico on-line] organização II Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet: Faculdade de Direito de Franca – Franca;

Coordenadores: Ana Carolina de Sá Juzo, Lucas Gonçalves da Silva e Helen Cristina de Almeida Silva – Franca: Faculdade de Direito de Franca, 2024.

Inclui bibliografia
ISBN: 978-65-5274-015-1
Modo de acesso: www.conpedi.org.br em publicações
Tema: Regulação do Ciberespaço.
1. Cibercrimes. 2. Fraudes Virtuais. 3. Deep Web. 4. Políticas Públicas de Desenvolvimento. 5. Efetividade do Direito. I. II Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet (1:2024 : Franca, SP).

CDU: 34

# II CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

## DIREITO PENAL E CIBERCRIMES

---

## Apresentação

Entre os dias 27 e 30 de agosto de 2024, a Faculdade de Direito de Franca recebeu o 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 – Direito Penal e Cibercrimes tratou dos desafios do direito penal no contexto dos cibercrimes, destacando as transformações tecnológicas e os novos tipos de crimes virtuais que demandam respostas inovadoras do sistema jurídico. As discussões exploraram as tecnologias aplicadas à investigação criminal e os desafios jurisdicionais associados a crimes eletrônicos, incluindo fraudes virtuais, ataques realizados por hackers e crackers, e os riscos associados à Deep Web e à Dark Web. O uso das redes sociais como meio para atividades criminosas e a aplicação de reconhecimento facial na persecução penal também foram amplamente debatidos, evidenciando a necessidade de regulamentações específicas e de ferramentas tecnológicas para a segurança e a justiça no ambiente digital.

# COMBATE AO CRIME CIBERNÉTICO NO CONTEXTO NACIONAL E INTERNACIONAL

# FIGHTING CYBERCRIME IN THE NATIONAL AND INTERNATIONAL CONTEXT

**Priscila de Castro Busnello** [1]
**Flavia Valeria Nava Silva** [2]
**Bruno Emanuel Setubal Learte** [3]

**Resumo**

O estudo explora o enfrentamento aos Crimes cibernéticos, com foco na adesão do Brasil à Convenção sobre o Crime Cibernético. O estudo exploratório mapeia as estratégias adotadas pelo Brasil tendo como ponto de partida a pergunta de pesquisa: “Quais são as iniciativas e estratégias adotadas pelo Brasil desde sua adesão à Convenção sobre o Crime Cibernético, com foco na cooperação internacional e eficácia da Rede 24/7, e como essas medidas têm impactado o combate aos crimes cibernéticos transnacionais? Os resultados apresentam as iniciativas implementadas pelo Brasil desde a adesão à Convenção, enfatizando a eficácia da Rede 24/7.

**Palavras-chave:** Crimes cibernéticos, Convenção sobre o crime cibernético, Cooperação internacional, Rede 24/7, Estratégias de combate

**Abstract/Resumen/Résumé**

The study explores the fight against cybercrime, focusing on Brazil's accession to the Convention on Cybercrime. The exploratory study maps the strategies adopted by Brazil, taking as its starting point the research question: "What are the initiatives and strategies adopted by Brazil since its accession to the Convention on Cybercrime, with a focus on international cooperation and the effectiveness of the 24/7 Network, and how have these measures impacted the fight against transnational cybercrime?". The results present the initiatives implemented by Brazil since joining the Convention, emphasizing the effectiveness of the 24/7 Network.

---

[1] Mestrado e doutorado em direito processual penal (PUC/SP), Mestrado em direito econômico (Universidade de Genebra/Suíça), Mestrado em Relações Internacionais (Paris 1 Pantheon-Sorbonne/França), Diploma de Administração Pública (INSP-ENA/ França)

[2] Mestranda pela University of Nicosia. Pós-graduada em Direitos Difusos, Coletivos e Gestão Fiscal pela ESMP/MPMA e em Neurociencia, Psicologia Positiva pela PUC/PR. Promotora de Justiça.

[3] Pós-Graduado em Direito, Cibersegurança e Ciberdefesa pela Verbo Jurídico, Pós-Graduado em Ethical Hacking e CyberSecurity, Especialista em Computação Forense e Perícia Digital, Graduando em Direito. Servidor Público (MPMA).

**Keywords/Palabras-claves/Mots-clés:** Cybercrime, Convention on cybercrime, International cooperation, 24/7 network, Combat strategies

## 1 Introdução

O combate ao crime cibernético tornou-se uma prioridade crucial, tanto no contexto nacional, quanto internacional, impulsionado pelo crescente uso da tecnologia e da internet. A transição para um ambiente digitalizado, no final do século XX proporcionou novas oportunidades para atividades ilícitas, com a exploração das vastas possibilidades oferecidas pelo mundo digital. Dessa forma, o Direito deve se adequar à nova realidade, pois embora alguns tipos penais tradicionais se apliquem aos crimes praticados no ciberespaço, há ainda um grande vácuo em termos de leis específicas que abordem comportamentos ilegítimos e abusos na era digital. A cooperação internacional, essencial para o combate a esses crimes transnacionais por excelência, é um mecanismo que também necessita de atualização, facilitando assim a produção de provas em diferentes jurisdições.

## 2 Crime cibernético no mundo e no Brasil

Com o avanço da transformação digital e a migração de diversos serviços cotidianos, como comunicação entre pessoas, e-commerce, educação, serviços públicos prestados por plataformas governamentais e atividades financeiras, para o ambiente online, surgiram também os riscos associados aos crimes cibernéticos. Essa transição para a rede mundial de computadores trouxe não apenas benefícios em termos de velocidade e comodidade, mas também expôs novos desafios, especialmente relacionados à prática de crimes digitais. Essa atividade criminosa, que abrange desde fraudes fiscais, roubo de identidade, até ataques cibernéticos contra infraestruturas críticas, constitui uma ameaça significativa à segurança, à economia e à privacidade ao redor do mundo (VECCHIA, 2019).

Considerando o caráter transnacional do tema, há grande dificuldade na elaboração um conceito definitivo de crime cibernético. Porém, é possível encontrar algumas definições, como a de Bryant (2008), de que “crimes digital ou de alta tecnologia é aquele no qual foi utilizada tecnologia para facilitar a atividade criminosa”; ou a de Reith, Carr e Gunsh (2002):

> Crimes cibernéticos não são, necessariamente, novos crimes, pois podem ser crimes clássicos que exploram o poder proporcionado pelo computador e acessibilidade de informações principalmente através da internet.

Nesse cenário, com novas modalidades de atos ilegítimos e violações de direitos, os Estados soberanos precisam estabelecer estratégias, fundadas no direito internacional,

ante a natureza transnacional de muitas ações delitivas praticadas no ciberespaço. A cooperação internacional é a principal forma de combater esses atos.

Um dos poucos instrumentos internacionais que trata de crimes cibernéticos e de cooperação é a Convenção do Conselho da Europa (CoE) sobre o Cibercrime. Conhecida como Convenção de Budapeste (ETS N°185), ela foi firmada em 2001 e conta atualmente com 75 Partes (em julho de 2024). Trata-se do instrumento internacional vinculante mais relevante sobre esse tema, e foi recentemente promulgado no Brasil, pelo Decreto n° 11.419/2023, em abril de 2023. Importante mencionar que, no âmbito das Nações Unidas, foi criado um Comitê Ad Hoc para elaborar uma Convenção Internacional abrangente sobre o combate ao uso de tecnologias de informação e comunicação para fins criminosos. Os trabalhos do Comitê ainda estão em andamento, sem perspectiva para a conclusão das negociações.

Considerando um marco importante na cooperação internacional, especialmente para investigações criminais de cibercrimes, a Convenção fomenta o esforço conjunto no combate, em escala global, à dificuldade na identificação da autoria e materialidades nos crimes desta natureza (DONZA; ARAUJO; 2023). Essa Convenção também viabiliza a racionalidade do Direito Penal, em cooperação internacional, instando os Estados a tipificarem condutas e, com isso, favorecem a harmonização da legislação penal entre os países-membros, assim, garantindo o enfrentamento dos crimes cometidos pelo computador, por serem infrações que ultrapassam fronteiras internacionais, no qual haverá diálogo entre diversos sistemas jurídicos internacionais (CASTRO, 2018).

## 3 Cooperação internacional: breve introdução

A globalização impulsionou o surgimento e a consolidação de estruturas criminosas transnacionais; no entanto, o combate à criminalidade enfrenta desafios relacionados aos limites territoriais dos Estados. Não é raro que as provas de crimes tenham que ser produzidas no território de outro Estado, com a colaboração de autoridades estrangeiras. Nesse cenário, a cooperação internacional tem se tornado um mecanismo indispensável para assegurar a efetiva aplicação da lei penal.

As bases para a colaboração entre Estados são os tratados ou convenções (multilaterais ou bilaterais) ou as promessas de reciprocidade (manifestadas por via diplomática). Algumas jurisdições também contam com um arcabouço jurídico interno que disciplina a cooperação internacional. Os tratados internacionais, depois de

internalizados no Brasil, por meio de Decreto Presidencial, têm força de lei e proporcionam segurança e estabilidade às relações internacionais.

A falta de tratado não impede a cooperação, que pode ocorrer no contexto da cooperação técnica, da troca de informações ou encaminhamento de dados. No entanto, a despeito do funcionamento da cooperação "informal", baseada no bom relacionamento entre as partes, é importante que existam formalidades e respaldo jurídico, sobretudo quando as provas produzidas com a cooperação instruirão processos judiciais, que podem resultar em condenações penais. Neste caso, o caminho que garante a validade da prova é o da **cooperação internacional**, que basicamente inclui a cooperação **policial** internacional e cooperação **jurídica** internacional.

A cooperação *jurídica* internacional é necessária para a prática de atos que estão sob reserva de jurisdição, ou seja, sempre que demandar representação e autorização judicial. Nos outros casos, quando o ato puder ser realizado diretamente pela autoridade policial, a cooperação *policial* será possível. São muitas as possibilidades de cooperação policial, incluindo: o esclarecimento sobre a lei estrangeira, a identificação de pessoas, o fornecimento de dados cadastrais, pesquisas em sistemas e fontes abertas etc. A assistência internacional pode ser na modalidade **ativa**, quando a autoridade brasileira solicita o auxílio à autoridade estrangeira, ou **passiva**, quando a autoridade estrangeira solicita o auxílio à autoridade brasileira.

Além dessas formas tradicionais de cooperação, a Convenção sobre o crime Cibernético trouxe uma inovação para o sistema jurídico brasileiro. Prevista no artigo 35 da Convenção, a Rede 24/7 é uma rede de cooperação internacional, formada por Pontos de Contato indicados pelos países que fazem parte da convenção. Esses Pontos de Contato devem estar disponíveis 24 horas por dia, 7 dias por semana, a fim de assegurar assistência imediata para investigações ou procedimentos relacionados a crimes de computador e de dados, ou para a obtenção de provas eletrônicas de uma infração penal. Essa nova forma de cooperação internacional, mais célere e efetiva, é implementada por Pontos de Contato (PoC).

## 4. Rede 24/7

A Convenção de Budapeste diminui a vulnerabilidade à cibercriminalidade, pois fornece às autoridades recursos adicionais em investigações desses crimes e dos crimes que demandam a obtenção de provas eletrônicas ou digitais armazenadas em outras

jurisdições. Ela favorece a coleta e preservação de provas digitais. Na prática, as autoridades brasileiras contam com novos mecanismos, o que proporciona uma melhoria em termos de segurança jurídica, efetividade e celeridade na obtenção de provas.

Conforme mencionado, uma importante inovação está no artigo 35, que prevê a criação de uma **REDE 24/7**, cujo objetivo é de funcionar como Ponto de Contato, a fim de assegurar a assistência **imediata** para investigações ou procedimentos relacionados a dados e sistemas informáticos, ou para obtenção de provas eletrônicas. A assistência inclui a facilitação e a adoção direta das seguintes medidas: aconselhamento técnico; conservação de dados; coleta de provas, informações de caráter jurídico e localização de suspeitos.

Em razão dessa previsão específica na Convenção do CoE, a Diretoria de Combate a Crimes Cibernéticos, da Polícia Federal (DCIBER/PF) foi nomeada ponto de contato para esse tipo de cooperação, e implementou a REDE 24/7 para cooperação internacional. Esse ponto de contato possui uma competência transversal, atuando nos pedidos de **cooperação internacional passiva e ativa.** Quanto à cooperação jurídica internacional, a Convenção de Budapeste mantém a regra geral, estabelecendo como autoridade central o Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional do Ministério da Justiça (DRCI/MJ).

A REDE 24/7 exerce atividades diversificadas. Ela realiza o controle e o registro dos pedidos de cooperação internacional; providencia a distribuição às coordenações temáticas; estabelece procedimentos e fluxos internos; produz estatísticas; verifica a conformidade do procedimento; orienta e assiste às coordenações temáticas e demais autoridades competentes sobre a forma adequada de cumprimento; analisa as respostas e verifica se atendem aos questionamentos encaminhados; confere se o pedido pode ser juridicamente cumprido por cooperação internacional; analisa a base jurídica dos pedidos; orienta as autoridades estrangeiras sobre leis e fluxos da cooperação no Brasil; elabora as respostas formais encaminhadas à contraparte estrangeira; seleciona os documentos que devem instruir as respostas; pode pedir esclarecimento às autoridades estrangeiras; além de outras atribuições.

A despeito da cooperação, policial e jurídica, já realizada tradicionalmente, a REDE 24/7 atua de forma mais específica, no contexto dos crimes cibernéticos. Sua atribuição é de zelar pela implementação adequada e pela celeridade da cooperação

internacional prevista pela Convenção de Budapeste, além da implementação de futuros acordos e convenções que o Brasil possa aderir nessa mesma área temática.

## 4 Considerações finais

O estudo destaca a importância da adesão do Brasil à Convenção sobre o Crime Cibernético e a implementação da Rede 24/7 como um marco significativo na cooperação internacional. Desde a adesão, o Brasil tem demonstrado progresso na cooperação internacional e, consequentemente, na obtenção de resultados positivos no combate ao crime cibernético.

No entanto, são necessários aprimoramentos contínuos nas estratégias e nos mecanismos de cooperação para enfrentar os desafios emergentes e uma das principais expectativas é uma possível convenção no âmbito das Nações Unidas sobre o tema.

A eficácia da Rede 24/7 é evidente, mas requer uma adaptação constante às novas formas de criminalidade digital e uma colaboração mais estreita entre as jurisdições internacionais. Assim, é fundamental que o Brasil continue a investir na capacitação das autoridades, na atualização das leis e na ampliação da cooperação internacional para garantir a segurança no ciberespaço e a proteção dos direitos dos cidadãos.

## Referências


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. Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 13 abr. 2023. Acesso em: 8 julho. 2024.

BRYANT, Robin P. ***Investigating Digital Crime***. Wiley, 2008. p. 272.

CASTRO, José Roberto Wanderley. **A tipicidade dos crimes cibernéticos no Direito Penal brasileiro: um estudo sobre o impacto da Lei 12.737/2012 e a (des)construção de uma dogmática penal dos crimes cibernéticos**. 2018. 231 f. Tese (Doutorado em Direito) –Programa de Pós-Graduação em Direito, Universidade Federal de Pernambuco, Recife, 2018. Acesso em: 8 julho. 2024.

DALLA VECCHIA, Evandro. **Perícia digital: da investigação à análise forense**. Campinas: Millenium, 2019. p. 52. (Série Tratado de perícias criminalísticas; 1)

DONZA CORRÊA, I.; ARAÚJO MONTEIRO NETO, J. **A adesão do Brasil à Convenção de Budapeste e o enfrentamento do Cibercrime: entre a Cooperação Internacional e a expansão do Direito Penal**. Revista Eletrônica Direito & TI, [S. l.], v. 1, n. 16, p.32–60, 2023. Disponível em: https://direitoeti.emnuvens.com.br/direitoeti/article/view/155. Acesso em: 8 jul. 2024.

REITH, M.; CARR, C.; GUNSCH, G. **Na examination of digital forensic models**. *International Journal of Digital Evidence*, 1(3): 1-12, 2002.