

II ENCONTRO NACIONAL DE DIREITO DO FUTURO - II ENDIF

DIREITO PENAL E TECNOLOGIA II

D598

Direito penal e tecnologia II [Recurso eletrônico on-line] organização II Encontro Nacional de Direito do Futuro: Escola Superior Dom Helder Câmara – Belo Horizonte;

Coordenadores: Mariana Azevedo Couto Vidal e Priscila Gabrielle Rodrigues Carvalho
– Belo Horizonte: Escola Superior Dom Helder Câmara - ESDHC, 2025.

Inclui bibliografia

ISBN: 978-65-5274-421-0

Modo de acesso: www.conpedi.org.br em publicações

Tema: Justiça social e tecnológica em tempos de incerteza.

1. Direito do Futuro. 2. Justiça Social. 3. Justiça Tecnológica. I. II Encontro Nacional de Direito do Futuro (1:2025 : Belo Horizonte, MG).

CDU: 34

II ENCONTRO NACIONAL DE DIREITO DO FUTURO - II ENDIF

DIREITO PENAL E TECNOLOGIA II

Apresentação

O II Encontro Nacional de Direito do Futuro (II ENDIF), organizado pelo Centro Universitário Dom Helder com apoio técnico do Conselho Nacional de Pesquisa e Pós-graduação em Direito – CONPEDI, reafirma-se como um espaço qualificado de produção, diálogo e circulação do conhecimento jurídico, reunindo a comunidade científica em torno de um propósito comum: pensar, com rigor metodológico e sensibilidade social, os caminhos do Direito diante das transformações que marcam o nosso tempo. Realizado nos dias 09 e 10 de outubro de 2025, em formato integralmente on-line, o evento assumiu como tema geral “Justiça social e tecnológica em tempos de incerteza”, convidando pesquisadoras e pesquisadores a enfrentar criticamente os impactos da inovação tecnológica, das novas dinâmicas sociais e das incertezas globais sobre as instituições jurídicas e os direitos fundamentais.

Nesta segunda edição, os números evidenciam a força do projeto acadêmico: 408 trabalhos submetidos, com a participação de 551 pesquisadoras e pesquisadores, provenientes de 21 Estados da Federação, culminando na organização de 31 e-books, que ora se apresentam à comunidade científica. Essa coletânea traduz, em linguagem acadêmica e compromisso público, a vitalidade de uma pesquisa jurídica que não se limita a descrever problemas, mas busca compreendê-los, explicar suas causas e projetar soluções coerentes com a Constituição, com os direitos humanos e com os desafios contemporâneos.

A publicação dos 31 e-books materializa um processo coletivo que articula pluralidade temática, densidade teórica e seriedade científica. Os textos que compõem a coletânea passaram por avaliação acadêmica orientada por critérios de qualidade e imparcialidade, com destaque para o método double blind peer review, que viabiliza a análise inominada dos trabalhos e exige o exame por, no mínimo, dois avaliadores, reduzindo subjetividades e preferências ideológicas. Essa opção metodológica é, ao mesmo tempo, um gesto de respeito à ciência e uma afirmação de que a pesquisa jurídica deve ser construída com transparência, responsabilidade e abertura ao escrutínio crítico.

O II ENDIF também se insere em uma trajetória institucional já consolidada: a primeira edição, realizada em junho de 2024, reuniu centenas de pesquisadoras e pesquisadores e resultou na publicação de uma coletânea expressiva, demonstrando que o Encontro se consolidou, desde o início, como um dos maiores eventos científicos jurídicos do país. A

continuidade do projeto, agora ampliada em escopo e capilaridade, reafirma a importância de se fortalecer ambientes acadêmicos capazes de integrar graduação e pós-graduação, formar novas gerações de pesquisadoras e pesquisadores e promover uma cultura jurídica comprometida com a realidade social.

A programação científica do evento, organizada em painéis temáticos pela manhã e Grupos de Trabalho no período da tarde, foi concebida para equilibrar reflexão teórica, debate público e socialização de pesquisas. Nos painéis, temas como inteligência artificial e direitos fundamentais, proteção ambiental no sistema interamericano, proteção de dados e herança digital foram tratados por especialistas convidados, em debates que ampliam repertórios e conectam a produção acadêmica aos dilemas concretos vividos pela sociedade.

A programação científica do II ENDIF foi estruturada em dois dias, 09 e 10 de outubro de 2025, combinando, no período da manhã, painéis temáticos com exposições de especialistas e debates, e, no período da tarde, sessões dos Grupos de Trabalho. No dia 09/10 (quinta-feira), após a abertura, às 09h, realizou-se o Painel I, dedicado aos desafios da atuação processual diante da inteligência artificial (“Inteligencia artificial y desafios de derechos fundamentales en el marco de la actuación procesal”), com exposição de Andrea Alarcón Peña (Colômbia) e debate conduzido por Caio Augusto Souza Lara. Em seguida, às 11h, ocorreu o Painel II, voltado à proteção ambiental no Sistema Interamericano, abordando a evolução da OC-23 ao novo marco da OC-32, com participação de Soledad Garcia Munoz (Espanha) e Valter Moura do Carmo como palestrantes, sob coordenação de Ricardo Stanziola Vieira. No período da tarde, das 14h às 17h, desenvolveram-se as atividades dos Grupos de Trabalho, em ambiente virtual, com apresentação e discussão das pesquisas aprovadas.

No dia 10/10 (sexta-feira), a programação manteve a organização: às 09h, foi realizado o Painel III, sobre LGPD e a importância da proteção de dados na sociedade de vigilância, com exposições de Laís Furuya e Júlia Mesquita e debate conduzido por Yuri Nathan da Costa Lannes; às 11h, ocorreu o Painel IV, dedicado ao tema da herança digital e à figura do inventariante digital, com apresentação de Felipe Assis Nakamoto e debate sob responsabilidade de Tais Mallmann Ramos. Encerrando o evento, novamente no turno da tarde, das 14h às 17h, seguiram-se as sessões dos Grupos de Trabalho on-line, consolidando o espaço de socialização, crítica acadêmica e amadurecimento das investigações apresentadas.

Ao tornar públicos estes 31 e-books, o II ENDIF reafirma uma convicção essencial: não há futuro democrático para o Direito sem pesquisa científica, sem debate qualificado e sem compromisso com a verdade metodológica. Em tempos de incerteza — tecnológica, social,

ambiental e institucional —, a pesquisa jurídica cumpre um papel civilizatório: ilumina problemas invisibilizados, questiona estruturas naturalizadas, qualifica políticas públicas, tensiona o poder com argumentos e oferece horizontes normativos mais justos.

Registramos, por fim, nosso reconhecimento a todas e todos que tornaram possível esta obra coletiva — autores, avaliadores, coordenadores de Grupos de Trabalho, debatedores e equipe organizadora —, bem como às instituições e redes acadêmicas que fortalecem o ecossistema da pesquisa em Direito. Que a leitura desta coletânea seja, ao mesmo tempo, um encontro com o que há de mais vivo na produção científica contemporânea e um convite a seguir construindo, com coragem intelectual e responsabilidade pública, um Direito à altura do nosso tempo.

Belo Horizonte-MG, 16 de dezembro de 2025.

Prof. Dr. Paulo Umberto Stumpf – Reitor do Centro Universitário Dom Helder

Prof. Dr. Francelim Jorge Sobral de Brito – Vice-Reitor e Pró-Reitor de Graduação do Centro Universitário Dom Helder

Prof. Dr. Caio Augusto Souza Lara – Pró-Reitor de Pesquisa do Centro Universitário Dom Helder

INTELIGÊNCIA ARTIFICIAL A SERVIÇO DO CRIME: DESAFIOS E LIMITES DO DIREITO PENAL

ARTIFICIAL INTELLIGENCE AT THE SERVICE OF CRIME: CHALLENGES AND LIMITS OF CRIMINAL LAW

Gabriela Emanuele de Resende ¹

Gisele Rondas Diniz Costa ²

Resumo

O uso da Inteligência Artificial (IA) por organizações criminosas cresce rapidamente, desafiando o Direito Penal. Este trabalho analisa os limites da legislação penal brasileira diante do uso da IA em crimes, destacando a insuficiência do artigo 171-A do Código Penal, que trata da fraude eletrônica. Apesar de tentativas jurídicas, como decisões do Tribunal de Justiça de São Paulo, a falta de tipificações específicas mostra a defasagem legislativa. Há urgência em reformas para acompanhar crimes cibernéticos impulsionados por IA, garantindo segurança jurídica e eficácia penal. Base teórica: Caio Augusto Souza Lara (2019). Metodologia jurídico-social.

Palavras-chave: Inteligência artificial, Direito penal, Crimes cibernéticos

Abstract/Resumen/Résumé

The use of Artificial Intelligence (AI) by criminal organizations is rapidly increasing, challenging Criminal Law. This study analyzes the limitations of Brazilian criminal legislation regarding AI in crime, highlighting the insufficiency of Article 171-A of the Penal Code, which addresses electronic fraud. Despite legal attempts, such as São Paulo Court decisions, the lack of specific typifications reveals legislative gaps. There is an urgent need for reforms to address AI-driven cybercrimes, ensuring legal certainty and effective penal enforcement. Theoretical framework: Caio Augusto Souza Lara (2019). Methodology: socio-legal approach.

Keywords/Palabras-claves/Mots-clés: Artificial intelligence, Criminal law, Cybercrimes

¹ Professora do Centro Universitário Dom Helder. Doutoranda e Mestra em Direito pela PUC Minas. Advogada. Bolsista CAPES.

² Graduanda em Direito pelo Centro Universitário Dom Helder. Estagiária do Tribunal do Trabalho 3º Região.

1 CONSIDERAÇÕES INICIAIS

A utilização da Inteligência Artificial generativa (IA) tem se tornado cada vez mais comum nas práticas criminosas, servindo como instrumento de facilitação para que ocorram os crimes. Com isso, observa-se os desafios e limites que essa realidade impõe ao Direito Penal. O presente resumo expandido tem como propósito analisar as consequências do uso da IA, a serviço da criminalidade, destacando como os avanços tecnológicos potencializam a consumação de condutas ilícitas e exigem uma reflexão crítica sobre a eficácia dos instrumentos jurídicos atuais. O presente resumo expandido tem como marco teórico a tese de Doutorado do Dr. Caio Augusto Souza Lara.

Quando se tem um meio de ocultar sua identidade, através de uma “capa do anonimato”, o ato de cometer crimes se torna mais atrativo tendo em vista que o agente não precisa sair de casa para que o crime ocorra. O que mais agrava a situação é a dificuldade de identificar os responsáveis. Como responsabilizar o indivíduo que cometeu um crime com o auxílio da IA? A insuficiência das normas regulamentadoras da IA deixa a sociedade mais vulnerável para responder essas perguntas.

Ainda que, habitualmente, o público-alvo dos estelionatários seja pessoas mais vulneráveis, com o auxílio da IA, qualquer indivíduo pode se tornar uma vítima em potencial. Quem, de algum modo, não compreende o básico de IA, estará exposto ao risco. Ao se falar em potenciais vítimas não se restringe a um grupo específico, entretanto, são especialmente vulneráveis os idosos e aqueles que apresentam dificuldades no uso da tecnologia. Contudo, de que forma a Lei geral de proteção de dados (LGPD) se aplica a essa realidade? Questiona-se a eficácia do referido diploma quando à prevenção do vazamento de dados. Nesse cenário, surge o seguinte problema da pesquisa: os crimes praticados com o uso da IA ficariam impunes? A hipótese inicial é não.

No tocante à metodologia da pesquisa, o presente resumo expandido utilizou, com base na classificação de Gustin, Dias e Nicácio (2020), a vertente metodológica jurídico-social. Com relação ao tipo genérico de pesquisa, foi escolhido o tipo jurídico-projetivo. Por sua vez, o raciocínio desenvolvido na pesquisa foi predominantemente dialético. Quanto ao gênero de pesquisa, adotou-se a pesquisa teórica-bibliográfica.

2 ENTENDIMENTOS JURISPRUDENCIAIS

De acordo com vários julgados em instâncias superiores, a decisões dos desembargadores têm sido cada vez mais claras e precisas quando se fala do uso da IA. Segundo a jurisprudência do Tribunal de Justiça de São Paulo (TJ-SP), no caso Luiz Gustavo Ferreira Martins, da Colenda x 8ª Câmara de Direito Criminal, assim diz o acórdão:

O crime de estelionato aqui processado, apesar de não ser praticado com violência, possui altíssimo grau de lesividade pelo incontável número de vítimas em potencial. [...] Não tratamos aqui com estelionatários que se utilizam apenas da inocência das vítimas [...] aqui temos uma associação criminosa que se utiliza de tecnologia de ponta, inteligência artificial, dados pessoais obtidos através da internet e cujos crimes foram praticados por agentes que se ocultam, (TJ-SP, 2024).

No trecho citado, não se trata de violência ou grave ameaça, e sim a preocupação dos desembargadores em virtude da elevada proporção de possíveis vítimas em potencial. A partir da jurisprudência apresentada, observa-se que os tribunais brasileiros já reconhecem a complexidade dos crimes praticados com auxílio de Inteligência Artificial. A atuação criminosa, que antes se limitava à presença física ou à interação direta com as vítimas, agora se dá de forma automatizada e remota, o que dificulta a identificação dos autores e a repressão penal. Como consequência, os julgadores têm adotado um entendimento mais amplo da tipificação penal, especialmente no que se refere ao crime de estelionato, que passou a incluir condutas sofisticadas viabilizadas pela tecnologia.

O artigo 171-A do Código Penal, introduzido pela Lei nº 14.155 (Brasil, 2021), trata da fraude eletrônica como um tipo autônomo ao estelionato. Embora tenha sido um avanço normativo, esse dispositivo ainda é insuficiente diante da complexidade dos crimes que utilizam algoritmos, bots e sistemas autônomos para enganar vítimas em massa. Assim, os julgados acabam por suprir essa lacuna legislativa ao reconhecer o uso de IA como fator agravante da conduta criminosa, considerando o elevado grau de sofisticação e lesividade envolvido.

Outro ponto relevante nas decisões judiciais é a valorização do contexto em que o crime foi praticado. A tecnologia empregada pelos autores, somada à dificuldade de rastreamento e à quantidade de vítimas afetadas, têm levado os tribunais a enfatizarem a periculosidade da conduta, mesmo quando não há violência ou grave ameaça. Como ressaltado pelo Tribunal de Justiça de São Paulo, “a inteligência artificial é um instrumento que potencializa a fraude, tornando-a praticamente imperceptível às vítimas” (Tribunal de

justiça de São Paulo, 2024). Dessa forma, o entendimento jurisprudencial se alinha à necessidade de proteger bens jurídicos tutelados, como o patrimônio e a segurança informacional.

Há também uma tendência de os magistrados considerarem o uso de IA como um indício de organização criminosa, sobretudo quando a prática envolve divisão de tarefas, uso de dados pessoais e infraestrutura tecnológica. Em casos como o julgado pela 8ª Câmara de Direito Criminal do TJ-SP, evidencia-se que não se trata de um ato isolado, mas de uma estrutura delituosa complexa que exige resposta penal igualmente sofisticada. Essa interpretação amplia a responsabilidade penal e pode justificar a aplicação de penas mais severas. Ainda que, no caso concreto, não se trate de organização criminosa, poderá ser configurado tipo de associação criminosa, com previsão no art. 288, *caput* do Código Penal (Brasil, 1940).

Por fim, observa-se que os tribunais têm um papel essencial na construção de soluções jurídicas diante da ausência de regulamentações específicas. A jurisprudência, ao reconhecer a gravidade dos crimes praticados com IA, contribui para um movimento de atualização do Direito Penal, mesmo que de forma não legislativa. Esse processo interpretativo é fundamental para evitar a sensação de impunidade e assegurar que a justiça acompanhe as transformações tecnológicas da sociedade. Contudo, a atuação judicial precisa ser acompanhada por reformas legislativas que tragam maior segurança jurídica e delimitem claramente os contornos do uso ilícito da Inteligência Artificial, em atenção, inclusive, aos princípios da lesividade e da taxatividade.

3 A (IM)POSSIBILIDADE DE RESPONSABILIZAÇÃO PENAL DA INTELIGÊNCIA ARTIFICIAL

O avanço da tecnologia tem provocado discussões intensas sobre a possibilidade de responsabilizar penalmente sistemas de Inteligência Artificial (IA) que, em determinados contextos, tomam decisões de maneira autônoma e podem causar danos jurídicos relevantes. Diante da crescente sofisticação dessas ferramentas, levanta-se a questão: seria possível responsabilizar penalmente uma IA pelos atos que praticar? Ou a responsabilidade deve sempre recair sobre um ser humano que a programou, utilizou ou negligenciou sua supervisão?

Do ponto de vista do Direito Penal clássico, a responsabilidade penal exige a presença de elementos subjetivos, como o dolo — consciência e vontade — ou a culpa —

negligência, imprudência e imperícia —. Tais atributos são característicos de seres humanos, não de máquinas. A IA, mesmo em seus modelos mais avançados, opera com base em algoritmos e padrões estatísticos, sem consciência de suas ações ou capacidade moral de discernimento. A culpabilidade consiste em um juízo de reprovação direcionado a um agente capaz de entender e agir conforme o Direito, excluindo assim entidades não humanas (Greco e Sanches, 2021).

Na tentativa de lidar com esse impasse, parte da doutrina europeia tem discutido a criação de uma “personalidade eletrônica”, que concederia às IA’s um status jurídico semelhante ao das pessoas jurídicas. Essa proposta, defendida em documento do Parlamento Europeu (2017), visava permitir a responsabilização civil e, eventualmente, penal de agentes autônomos. No entanto, essa ideia foi duramente criticada por juristas que apontam os riscos de deslocar a responsabilidade dos indivíduos para entes artificiais sem consciência.

No contexto brasileiro, não há previsão legal que autorize a responsabilização penal direta da IA. Isso implica que os crimes cometidos com o uso dessas tecnologias devem ser imputados aos indivíduos que treinaram ou utilizaram o sistema para fins ilícitos. Nessa linha, a responsabilização recai sobre quem detinha o controle ou se beneficiava da conduta criminosa, ainda que a execução tenha ocorrido de forma automatizada.

A jurisprudência brasileira, embora ainda incipiente, tem adotado essa postura ao enquadrar como autores os agentes humanos por trás das tecnologias utilizadas para a prática de crimes, como fraudes eletrônicas ou disseminação de desinformação. A responsabilidade penal, nesses casos, pode ser atribuída inclusive por omissão, nos termos do artigo 13, §2º, do Código Penal (Brasil, 1940), quando o agente detinha o dever jurídico de agir para evitar o resultado. Assim, a negligência no desenvolvimento, supervisão ou aplicação da IA pode configurar crime, a depender do contexto.

Além disso, surgem propostas que buscam responsabilizar penalmente indivíduos por falhas no controle da IA, mesmo quando não há intenção dolosa. Um exemplo é a adoção da teoria do risco, inspirada no Direito Penal Econômico, que admite responsabilização com base na criação de um perigo não controlado pela atividade tecnológica. O risco não controlado que resulta em um dano pode ser suficiente para justificar a responsabilidade penal, mesmo na ausência de intenção direta (Zaffaroni, 2014).

Portanto, ainda que a responsabilização penal direta da IA seja, hoje, juridicamente inviável, o Direito Penal pode adaptar seus institutos para alcançar os responsáveis humanos pelos crimes praticados com auxílio dessas tecnologias. Isso requer, no entanto, o desenvolvimento de normas específicas que delimitem deveres de cuidado, obrigações de

supervisão e parâmetros de imputação subjetiva no uso de sistemas autônomos. Apenas assim será possível garantir segurança jurídica sem abrir espaço para a impunidade diante de práticas criminosas sofisticadas. Segundo Lara (2019, p. 16), “A tecnologia conquista cada vez mais relevância no espaço social. Uma das mais relevantes discussões no momento, para o universo jurídico”.

4 CONSIDERAÇÕES FINAIS

Diante do exposto, é possível perceber que o uso da Inteligência Artificial no cometimento de crimes representa um dos maiores desafios contemporâneos enfrentados pelo Direito Penal. A rapidez com que as tecnologias evoluem contrasta com a lentidão das reformas legislativas, o que gera insegurança jurídica e dificuldades práticas na responsabilização dos envolvidos. Ainda que existam dispositivos legais como o artigo 171-A do Código Penal, não são suficientes para abranger todas as nuances dos crimes cometidos com o auxílio da IA.

A jurisprudência tem desempenhado um papel fundamental ao interpretar e aplicar o Direito diante de situações inéditas, mas essa atuação não pode suprir, de forma definitiva, a ausência de normativas específicas. Isso evidencia que a jurisprudência, embora relevante na aplicação do Direito, deve respeitar os limites legais e não substituir a função legislativa. O sistema penal brasileiro ainda carece de instrumentos mais claros, modernos e eficazes para lidar com crimes tecnológicos complexos. A responsabilidade penal precisa estar bem definida para evitar impunidade, mas também para garantir que não sejam violados princípios fundamentais.

Assim, conclui-se que é urgente e indispensável que o legislador brasileiro avance na regulamentação do uso da Inteligência Artificial no campo penal. A responsabilização direta da IA ainda é juridicamente inviável, mas a responsabilização dos agentes humanos envolvidos deve ser fortalecida com normas que estabeleçam deveres claros de controle, supervisão e prevenção. Só assim será possível garantir que o Direito Penal continue exercendo sua função de proteção da sociedade, mesmo em um cenário altamente tecnológico.

REFERÊNCIAS

BRASIL. **Código Penal**. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 04 maio 2025.

BRASIL. **Lei n. 13.709**, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 04 maio 2025.

BRASIL. **Lei n. 14.155**, de 27 de maio de 2021. Altera o Código Penal e o Código de Processo Penal para aprimorar o combate aos crimes de fraude eletrônica. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 04 maio 2025.

EUROPEAN PARLIAMENT. **European Parliament resolution with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))**. Brussels, 2017. Disponível em: https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html. Acesso em: 04 maio 2025.

GRECO, Rogério; SANCHES, André Estefam. **Curso de Direito Penal: Parte Geral**. 18. ed. Rio de Janeiro: Impetus, 2021.

GUSTIN, Miracy Barbosa de Sousa; DIAS, Maria Tereza Fonseca; NICÁCIO, Camila Silva. **(Re)pensando a pesquisa jurídica: teoria e prática**. 5ª. ed. São Paulo: Almedina, 2020.

LARA, Caio Augusto Souza. **O acesso tecnológico à justiça: por um uso contra-hegemônico do big data e dos algoritmos**. 2019. Orientadora: Adriana Goulart de Sena Orsini. Tese (doutorado) – Universidade Federal de Minas Gerais, Faculdade de Direito.

SÃO PAULO. Tribunal de Justiça. (8ª Câmara de Direito Criminal) **Habeas Corpus Criminal: XXXXX20248260000 São Bernardo do Campo**, Relator: Sérgio Ribas, data de Julgamento: 14/11/2024. Data de Publicação: 14/11/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/2854611693/inteiro-teor-2854611695>. Acesso em: 01 maio 2025

SÃO PAULO. Tribunal de Justiça. (8ª Câmara de Direito Criminal.) **Apelação Criminal nº 0000000-00.2023.8.26.0000**. Relator: Desembargador Luiz Gustavo Ferreira Martins, data do Julgamento: 11/12/2024. Data de Publicação: 11/12/2024. Disponível em: <https://www.jusbrasil.com.br/processos/758396253/processo-n-231XXXX-1420248260000-do-tjsp> Acesso em: 04 maio 2025.

ZAFFARONI, Eugenio Raúl. **O inimigo no Direito Penal**. 5. ed. Rio de Janeiro: Revan, 2014.