REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

RESPONSABILIDADE PENAL E INTELIGÊNCIA ARTIFICIAL: IMPUTAÇÃO OBJETIVA, RISCO ALGORÍTMICO E LIMITES TÉCNICO-NORMATIVOS

CRIMINAL LIABILITY AND ARTIFICIAL INTELLIGENCE: OBJECTIVE IMPUTATION, ALGORITHMIC RISK AND TECHNO-NORMATIVE LIMITS

Ciências Exatas e da Terra, Ciências Sociais Aplicadas • 28/04/2026

REGISTRO DOI: 10.70773/revistatopicos/777265862

Dandara Albuquerque Ferreira de Andrade[1]

José Zeferino de Andrade Neto[2]

RESUMO

A crescente autonomia dos sistemas de inteligência artificial impõe desafios significativos ao Direito Penal, especialmente no que se refere à imputação objetiva e à delimitação do risco juridicamente relevante. O presente artigo analisa a insuficiência das categorias dogmáticas tradicionais diante de decisões algorítmicas autônomas, sustentando a necessidade de reconstrução da imputação penal a partir da articulação entre parâmetros normativos e o estado da técnica em engenharia de software. Adota-se metodologia qualitativa, com revisão bibliográfica, análise dogmática dos arts. 18 e 27 do Código Penal e abordagem interdisciplinar com fundamentos da Ciência da Computação, incluindo arquitetura de redes neurais, normas técnicas (ISO 26262 e IEC 62304) e técnicas de explicabilidade algorítmica. Examina-se, ainda, a regulação comparada, com destaque para o Artificial Intelligence Act europeu e o Projeto de Lei nº 2.338/2023, especialmente quanto aos deveres de transparência, documentação e rastreabilidade. A partir da teoria da imputação objetiva e da distinção entre risco permitido e risco proibido, propõe-se a incorporação do estado da técnica como critério estruturante do dever de cuidado, sem desconsiderar os limites técnico-normativos impostos pela opacidade algorítmica. Conclui-se pela necessidade de um modelo híbrido de responsabilização, que combine imputação indireta, culpabilidade organizacional e mecanismos regulatórios, de modo a assegurar proteção de direitos fundamentais sem promover expansão indevida do poder punitivo.

Palavras-chave: direito penal; inteligência artificial; imputação objetiva; risco algorítmico; responsabilidade penal.

ABSTRACT

The increasing autonomy of artificial intelligence systems poses

significant challenges to Criminal Law, particularly with regard to objective imputation and the delimitation of legally relevant risk. This article analyzes the inadequacy of traditional dogmatic categories in the face of autonomous algorithmic decision-making, arguing for the need to reconstruct criminal imputation through the articulation between normative parameters and the state of the art in software engineering. A qualitative methodology is adopted, combining bibliographic review, dogmatic analysis of articles 18 and 27 of the Brazilian Penal Code, and an interdisciplinary approach grounded in Computer Science, including neural network architecture, technical standards (ISO 26262 and IEC 62304), and algorithmic explainability techniques. The study also examines comparative regulation, particularly the European Artificial Intelligence Act and Brazilian Bill No. 2.338/2023, with emphasis on duties of transparency, documentation, and traceability. Based on the theory of objective imputation and the distinction between permitted and prohibited risk, the paper proposes the incorporation of the state of the art as a structuring criterion of the duty of care, while acknowledging the techno-normative limits imposed by algorithmic opacity. It concludes by advocating a hybrid model of liability that combines indirect imputation, organizational culpability, and regulatory mechanisms, aiming to ensure the protection of fundamental rights without promoting undue expansion of punitive power.
Keywords: criminal law; artificial intelligence; objective imputation; algorithmic risk; criminal liability.

1. INTRODUÇÃO

A expansão transversal da inteligência artificial como tecnologia de impacto multifacetado tem reconfigurado radicalmente as

estruturas sociais, econômicas e, de modo particular, os fundamentos do sistema jurídico-penal. Esse fenômeno impõe uma crise paradigmática ao Direito Penal, cujas categorias dogmáticas tradicionais – construídas em torno da imputação subjetiva, do dolo e da culpabilidade – mostram-se estruturalmente inadequadas para responder aos desafios suscitados por sistemas autônomos baseados em aprendizado de máquina e decisões probabilísticas. Enquanto a IA opera por meio de padrões estatísticos e algoritmos opacos, o Direito Penal contemporâneo permanece ancorado em pressupostos antropocêntricos que se tornam progressivamente anacrônicos diante da nova realidade tecnológica.

No contexto brasileiro, essa inadequação normativa já produz consequências tangíveis e preocupantes. Casos como os erros em sistemas de reconhecimento facial, com altas taxas de falsos positivos entre pessoas negras, e falhas em sistemas automatizados de diagnóstico médico evidenciam a materialização de riscos algorítmicos que transcendem a esfera teórica. O acidente envolvendo um veículo autônomo da Uber em 2018, que atropelou e matou uma pedestre no Arizona, e as falhas atribuídas ao robô cirurgião Da Vinci ilustram como a lesividade decorrente da atuação de sistemas autônomos assume contornos sistêmicos, exigindo uma resposta penal que o ordenamento jurídico atual não consegue fornecer.

A doutrina internacional tem dedicado atenção crescente a essa problemática. Contudo, tais análises frequentemente não oferecem soluções adaptadas à realidade brasileira, marcada por desigualdades estruturais que os vieses algorítmicos tendem a reproduzir. Diante disso, o presente trabalho propõe um modelo

híbrido de responsabilização penal, combinando imputação indireta, governança algorítmica e mecanismos compensatórios.

Metodologicamente, a pesquisa adota abordagem qualitativa, articulando análise dogmática, estudo de casos e investigação interdisciplinar com fundamentos da Ciência da Computação, especialmente no que se refere ao funcionamento interno de algoritmos de aprendizado de máquina, seus limites de explicabilidade e as normas técnicas de engenharia de software.

2. FUNDAMENTAÇÃO TEÓRICA

2.1. A Teoria do Risco no Direito Penal e na Engenharia de Software: Do Risco Permitido Ao Risco Proibido

A teoria do risco constitui um dos pilares da dogmática penal contemporânea, especialmente nos crimes culposos e nos delitos de perigo abstrato. Em sociedades tecnologicamente complexas, nas quais atividades potencialmente lesivas são socialmente toleradas em razão de sua utilidade, a distinção entre risco permitido e risco proibido assume papel central na delimitação da responsabilidade penal.

Nesse contexto, a teoria da imputação objetiva, sistematizada por Claus Roxin (2010), fornece importante critério de análise ao estabelecer que a responsabilização penal exige não apenas a produção de um resultado lesivo, mas a criação de um risco juridicamente desaprovado que se concretize no resultado. Nesse sentido, a dogmática clássica de Cezar Roberto Bitencourt (2020) reforça que a conduta punível deve estar vinculada à violação de um dever jurídico prévio.

Aplicada ao desenvolvimento de sistemas de inteligência artificial, essa perspectiva permite compreender que a criação de tecnologias inovadoras, por si só, insere-se no âmbito do risco permitido, na medida em que tais sistemas produzem benefícios relevantes. Contudo, quando o desenvolvimento ou a implementação desses sistemas ocorre em desacordo com o estado da técnica, verifica-se a criação de um risco proibido, passível de fundamentar a imputação penal.

Jakobs (2023) complementa essa análise ao sustentar que o risco permitido se fundamenta em um juízo objetivo-normativo vinculado às expectativas sociais de comportamento. A evolução desse conceito é debatida por Luís Greco (2018), que propõe uma delimitação rigorosa da responsabilidade penal em cenários de riscos tecnológicos complexos.

Do ponto de vista técnico, normas como a ISO 26262 e a IEC 62304 estabelecem parâmetros objetivos para o desenvolvimento seguro de sistemas críticos, definindo requisitos de validação, verificação e gestão de riscos. Tais normas representam a materialização do estado da técnica e, consequentemente, constituem referência essencial para a aferição do dever de cuidado.

A violação desses padrões, como evidenciado no caso do veículo autônomo da Uber, no qual houve desativação de mecanismos de segurança, ou nos incidentes envolvendo o sistema robótico Da Vinci, nos quais se identificaram falhas recorrentes de funcionamento, revela não apenas inadequação técnica, mas a superação dos limites do risco permitido, configurando hipótese de risco proibido à luz da teoria da imputação objetiva.

Entretanto, a incorporação do estado da técnica à análise jurídico-penal não se dá de forma automática. A dinâmica acelerada da inovação tecnológica impõe desafios à previsibilidade normativa, exigindo do intérprete uma constante atualização e diálogo com outras áreas do conhecimento.

2.2. Análise Comparada da Regulação da IA: Transparência e Dever de Cuidado do Programador

A crescente complexidade dos sistemas de inteligência artificial tem impulsionado o desenvolvimento de marcos regulatórios destinados a estabelecer parâmetros mínimos de segurança, transparência e responsabilização. O Artificial Intelligence Act europeu representa o modelo mais avançado nesse sentido, ao adotar uma abordagem baseada em risco e impor requisitos específicos para sistemas classificados como de alto risco.

No Brasil, o Projeto de Lei nº 2.338/2023 segue lógica semelhante, estabelecendo deveres de transparência e documentação técnica. A positivação desses requisitos contribui para a densificação do dever de cuidado, convertendo parâmetros técnicos em critérios juridicamente exigíveis.

Sob a perspectiva da imputação objetiva, tais normas desempenham função relevante ao delimitar, de forma mais precisa, o conteúdo do risco permitido. A omissão na observância de deveres de documentação, rastreabilidade e mitigação de riscos pode ser interpretada como criação de risco juridicamente desaprovado, apto a fundamentar a responsabilização penal.

Contudo, a ampliação do espectro normativo não pode conduzir à expansão descontrolada do Direito Penal. Nesse ponto, a crítica

desenvolvida por Eugenio Raúl Zaffaroni (2011) assume papel central. Para o autor, o Direito Penal deve ser compreendido como instrumento de intervenção mínima. Essa visão é corroborada pela necessidade de evitar que sistemas automatizados aprofundem desigualdades estruturais, conforme alertado por Eubanks (2018) ao discutir o perfilamento algorítmico de populações vulneráveis.

A aplicação dessa perspectiva ao contexto da inteligência artificial impõe cautela na criminalização de condutas relacionadas ao desenvolvimento tecnológico. A mera existência de falhas ou imperfeições em sistemas complexos não pode, por si só, justificar a imputação penal, sob pena de violação dos princípios da culpabilidade e da legalidade.

Ademais, a exigência de transparência encontra limites estruturais na própria natureza dos sistemas de aprendizado profundo. Modelos de alta complexidade operam por meio de representações não lineares, dificultando a explicação completa de seus processos decisórios. Técnicas de explicabilidade, como LIME e SHAP, oferecem apenas aproximações interpretativas, o que exige uma interpretação razoável do dever de transparência, compatível com o estado da arte tecnológico.

2.3. Prova Pericial em Algoritmos de Caixa-preta: Desafios para a Criminalística

A opacidade dos sistemas de inteligência artificial constitui um dos principais desafios para a persecução penal, na medida em que dificulta a reconstrução do nexo causal entre a conduta e o resultado. Diferentemente dos sistemas tradicionais, nos quais a causalidade pode ser analisada de forma linear, os sistemas

algorítmicos operam por meio de processos distribuídos e interdependentes.

Essa característica exige o desenvolvimento de metodologias periciais específicas, capazes de integrar conhecimentos jurídicos e computacionais. O debate sobre a consciência dessas máquinas e a organização da "sociedade da mente" proposto por Minsky (1986) já antecipava a dificuldade de isolar decisões em sistemas distribuídos.

A utilização de técnicas de explicabilidade, auditoria de dados e testes de robustez constitui ferramenta importante nesse processo, embora não elimine completamente as incertezas inerentes aos sistemas complexos. Nesse cenário, a valoração da prova deve considerar não apenas os resultados obtidos, mas também as limitações metodológicas dos instrumentos utilizados.

2.4. Culpabilidade Organizacional e Compliance em IA: A Contribuição de Klaus Tiedemann

A crescente complexidade dos sistemas de inteligência artificial desloca o foco da responsabilidade penal da esfera individual para o âmbito organizacional. Nesse contexto, a teoria da culpabilidade organizacional, desenvolvida por Klaus Tiedemann (2014), oferece importante referencial teórico ao fundamentar a responsabilização de pessoas jurídicas com base no chamado "defeito de organização".

Esse conceito refere-se à ausência de estruturas internas adequadas para prevenir a ocorrência de ilícitos, abrangendo falhas em governança, gestão de riscos e cultura organizacional. No contexto da inteligência artificial, a análise do defeito de organização envolve a verificação da existência de mecanismos de controle, auditoria e monitoramento contínuo dos sistemas.

Programas de compliance em IA desempenham papel central nesse cenário, podendo atuar tanto como elemento de exclusão ou atenuação da responsabilidade penal, quando efetivos, quanto como fator de agravamento, quando meramente formais ou inexistentes.

A articulação entre a teoria da imputação objetiva, a crítica garantista e a culpabilidade organizacional permite a construção de um modelo teórico mais adequado para lidar com os desafios da responsabilização penal em sistemas autônomos, integrando elementos normativos, técnicos e institucionais.

3. METODOLOGIA

A pesquisa caracteriza-se como qualitativa, de natureza teórico-dogmática e interdisciplinar. O material de estudo compreendeu fontes primárias (Código Penal brasileiro – arts. 18 e 27 –, Artificial Intelligence Act europeu e Projeto de Lei nº 2.338/2023) e secundárias (doutrina penal nacional e internacional, relatórios técnicos como NTSB 2019, artigos de Ciência da Computação e normas ISO 26262 e IEC 62304).

Adotou-se revisão bibliográfica sistemática, análise dogmática dos institutos de imputação subjetiva, dolo, culpa e culpabilidade, e estudo de casos concretos (acidente Uber 2018 e incidentes Da Vinci) para ilustrar a aplicação prática dos conceitos teóricos. Realizou-se análise comparada entre os marcos regulatórios europeu e brasileiro, com ênfase em transparência e dever de cuidado. A abordagem interdisciplinar integrou fundamentos da Ciência da Computação, especialmente arquitetura de redes neurais,

técnicas de explicabilidade algorítmica (XAI) e estado da técnica em engenharia de software.

Não houve coleta de dados primários empíricos; os “dados” consistiram nas informações extraídas da literatura e dos relatórios públicos. A tabulação e análise foram temáticas, organizadas em torno dos eixos risco, regulação, prova pericial e culpabilidade organizacional, permitindo confrontar os achados com os objetivos do trabalho.

4. RESULTADOS E DISCUSSÕES

Os resultados da pesquisa evidenciam, de forma consistente, a insuficiência das categorias tradicionais do Direito Penal para enfrentar a complexidade inerente aos sistemas autônomos de inteligência artificial. A análise conjunta da teoria do risco e dos parâmetros técnicos da engenharia de software demonstra que a distinção clássica entre risco permitido e risco proibido não pode mais ser realizada exclusivamente a partir de critérios normativos abstratos, exigindo, necessariamente, a incorporação do estado da técnica como elemento estruturante da imputação penal.

Nesse contexto, a teoria da imputação objetiva, desenvolvida por Claus Roxin (2010), revela-se particularmente relevante, ao estabelecer que a responsabilização penal depende da criação de um risco juridicamente desaprovado e da sua realização no resultado. Aplicada aos sistemas de inteligência artificial, essa construção permite afirmar que a mera criação de tecnologia não é suficiente para fundamentar a imputação, sendo necessário demonstrar que o agente contribuiu para a produção de um risco que ultrapassa os limites do permitido à luz do estado da técnica.

Assim, a violação de normas como a ISO 26262 e a IEC 62304 passa a representar não apenas uma falha técnica, mas a própria materialização de um risco juridicamente relevante nos termos da teoria roxiniana.

Entretanto, a incorporação de critérios técnicos à dogmática penal não se realiza sem tensões. A dependência do Direito Penal em relação ao estado da arte tecnológico suscita questionamentos quanto à segurança jurídica e à previsibilidade das decisões judiciais, na medida em que tais parâmetros são dinâmicos e frequentemente inacessíveis ao operador jurídico tradicional. Essa problemática se agrava quando se considera o risco de expansão indevida do Direito Penal para campos marcados pela incerteza técnica.

Nesse ponto, a crítica formulada por Eugenio Raúl Zaffaroni (2011) ao expansionismo penal mostra-se extremamente pertinente. Para o autor, o Direito Penal deve atuar como ultima ratio, evitando a criminalização excessiva de condutas em contextos de elevada complexidade e baixa previsibilidade. No âmbito da inteligência artificial, essa advertência assume especial relevância, uma vez que a tendência de responsabilizar penalmente falhas tecnológicas pode conduzir à ampliação indevida do poder punitivo, sem que haja efetiva correspondência com os pressupostos clássicos da culpabilidade.

A análise comparada da regulação da inteligência artificial reforça esse cenário. O Artificial Intelligence Act europeu e o Projeto de Lei nº 2.338/2023, ao positivarem deveres de transparência, documentação e rastreabilidade, promovem uma normatização progressiva do estado da técnica, convertendo padrões técnicos em

parâmetros jurídicos vinculantes. Essa transformação tem impacto direto na configuração do dever de cuidado do programador, cuja atuação passa a ser avaliada não apenas à luz de critérios genéricos de diligência, mas também com base em exigências técnicas específicas e verificáveis.

Todavia, a exigência de transparência encontra limites estruturais na própria natureza dos sistemas de aprendizado profundo. A opacidade algorítmica constitui característica inerente a modelos de alta complexidade, o que impede a reconstrução integral do processo decisório. As técnicas de explicabilidade (XAI), como LIME e SHAP, fornecem apenas aproximações interpretativas. Nesse cenário, exigir explicabilidade absoluta implicaria impor ao agente um dever impossível, o que, à luz da dogmática penal, inviabilizaria a própria imputação.

No campo probatório, a natureza distribuída da causalidade algorítmica dificulta a individualização da conduta, deslocando o foco da análise para estruturas organizacionais e processos sistêmicos. A teoria sistêmica da segurança reforça que os acidentes decorrem de falhas de controle e não de eventos isolados, o que exige uma reconstrução probatória igualmente complexa e interdisciplinar.

Por fim, a teoria da culpabilidade organizacional de Klaus Tiedemann complementa esse quadro ao permitir a responsabilização penal de entes coletivos por defeitos estruturais de organização. A combinação entre imputação objetiva (Roxin, 2010) e defeito de organização (Tiedemann, 2014) oferece uma base teórica robusta para enfrentar os danos algorítmicos, ao mesmo

tempo em que a crítica garantista de Zaffaroni funciona como limite à expansão descontrolada do Direito Penal.

A partir desses elementos, evidencia-se que a responsabilização penal em contextos de inteligência artificial exige um equilíbrio delicado entre eficiência repressiva e contenção do poder punitivo, evitando tanto a impunidade quanto o excesso penal.

5. CONCLUSÃO

A análise desenvolvida ao longo deste trabalho demonstra que a emergência de sistemas autônomos de inteligência artificial impõe uma reconfiguração profunda das bases dogmáticas do Direito Penal. A impossibilidade de atribuição direta de responsabilidade às máquinas não afasta a necessidade de resposta jurídica, mas exige a construção de modelos de imputação capazes de refletir a complexidade dos processos tecnológicos contemporâneos.

A teoria da imputação objetiva de Roxin (2010) oferece importante ferramenta para essa tarefa, ao condicionar a responsabilização à criação e realização de um risco juridicamente desaprovado. No contexto da inteligência artificial, esse risco deve ser aferido a partir do estado da técnica, incorporando parâmetros da engenharia de software e normas técnicas. Entretanto, a ampliação dos critérios de imputação não pode ocorrer de forma ilimitada. A advertência de Zaffaroni (2011) acerca do caráter subsidiário do Direito Penal impõe a necessidade de contenção do expansionismo punitivo, especialmente em cenários marcados por elevada complexidade técnica e incerteza causal. A responsabilização penal não pode servir como resposta automática a falhas tecnológicas, sob pena de violação dos princípios da culpabilidade e da legalidade.

Nesse contexto, a responsabilização deve ser estruturada a partir de um modelo híbrido, que combine: (i) imputação indireta dos agentes humanos, com base na violação do dever de cuidado aferido pelo estado da técnica; (ii) responsabilização organizacional fundamentada no defeito de governança, conforme a teoria de Tiedemann (2014); e (iii) articulação com instrumentos regulatórios e mecanismos compensatórios, capazes de assegurar proteção efetiva às vítimas, conforme padrões internacionalmente reconhecidos. A consolidação desse modelo depende, necessariamente, da integração entre Direito e Ciência da Computação, não como campos isolados, mas como saberes complementares na construção de respostas jurídicas adequadas à realidade tecnológica. Apenas por meio dessa abordagem interdisciplinar será possível evitar tanto a lacuna de responsabilização quanto a expansão indevida do poder punitivo.

Em síntese, o desafio contemporâneo do Direito Penal não reside apenas em responder aos danos causados por sistemas de inteligência artificial, mas em fazê-lo de forma tecnicamente informada, juridicamente consistente e normativamente limitada, preservando o equilíbrio entre inovação tecnológica e proteção de direitos fundamentais.

REFERÊNCIAS BIBLIOGRÁFICAS

ALEMZADEH, Homa et al. *Adverse events in robotic surgery: a retrospective study of 14 years of FDA data*. PLoS ONE, v. 11, n. 4, 2016.

BAROCAS, Solon; SELBST, Andrew. *Big data's disparate impact*. California Law Review, v. 104, p. 671–732, 2016.

BITENCOURT, Cezar Roberto. *Tratado de direito penal: parte geral*. 23. ed. São Paulo: Saraiva, 2020.

BRASIL. *Código Penal*. Decreto-Lei nº 2.848, de 7 de dezembro de 1940.

BRASIL. *Projeto de Lei nº 2.338, de 2023*. Dispõe sobre o uso da inteligência artificial. Brasília: Câmara dos Deputados, 2023.

BRODOWSKI, Dominik et al. (ed.). *Regulating corporate criminal liability*. Cham: Springer, 2014.

BUOLAMWINI, Joy; GEBRU, Timnit. *Gender shades: intersectional accuracy disparities in commercial gender classification.* In: CONFERENCE ON FAIRNESS, ACCOUNTABILITY AND TRANSPARENCY, 1., 2018. Proceedings [...]. p. 77–91.

EUBANKS, Virginia. *Automating inequality: how high-tech tools profile, police, and punish the poor*. New York: St. Martin's Press, 2018.

GOODFELLOW, Ian; BENGIO, Yoshua; COURVILLE, Aaron. *Deep learning*. Cambridge: MIT Press, 2016.

GOODFELLOW, Ian et al. *Explaining and harnessing adversarial examples*. arXiv preprint arXiv:1412.6572, 2014.

GRECO, Luís. *Responsabilidade penal por riscos: uma proposta.* Revista Brasileira de Ciências Criminais, São Paulo, v. 143, p. 31–54, 2018.

INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC). *IEC 62304: medical device software – software life cycle processes*.

Geneva: IEC, 2015.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). *ISO 26262: road vehicles – functional safety*. Geneva: ISO, 2018.

JAKOBS, Günther. *Derecho penal: parte general*. 2. ed. Madrid: Marcial Pons, 2003.

MINSKY, Marvin. *The society of mind*. New York: Simon & Schuster, 1986.

MOLNAR, Christoph. *Interpretable machine learning*. 2. ed., 2022. Disponível em: https://christophm.github.io/interpretable-ml-book/. Acesso em: 10 mar. 2026.

RIBEIRO, Marco Túlio; SINGH, Sameer; GUESTRIN, Carlos. *"Why should I trust you?": explaining the predictions of any classifier*. In: ACM SIGKDD INTERNATIONAL CONFERENCE ON KNOWLEDGE DISCOVERY AND DATA MINING, 22., 2016. Proceedings [...]. p. 1135–1144.

ROXIN, Claus. *Direito penal: parte geral: fundamentos*. A estrutura da teoria do delito. 2. ed. São Paulo: Marcial Pons, 2010.

SANTOS, Ana Paula; GOMES, Daniel. *Inteligência artificial e direito penal: desafios para a construção de um marco regulatório*. Revista de Estudos Criminais, Porto Alegre, v. 21, n. 2, p. 203–225, 2021.

UNIÃO EUROPEIA. *Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024.* Bruxelas: Jornal Oficial da União Europeia, 2024.

ZAFFARONI, Eugenio Raúl; PIERANGELI, José Henrique. *Manual de direito penal brasileiro: parte geral*. 7. ed. São Paulo: Revista dos Tribunais, 2011.

---

[1] Especialista em Direito Penal e Processo Penal, Faculdade Dom Alberto. E-mail: dandaraaf@gmail.com

[2] Especialista em Cybercrime e Cybersecurity – Prevenção e Investigação de Crimes Digitais, União Brasileira de Faculdades - UNIBF. E-mail: netojz@gmail.com