www.revistaft.com.br

Revista FT | ISSN 1678-0817 | v. 30, n. 159, 2026 | DOI: 10.69849/wh5nw251

A extradição de criminosos digitais: desafios jurídicos e efetividade no Brasil (2012–2025).

The extradition of digital criminals: legal challenges and effectiveness in Brazil (2012–2025).

Luiz Alberto dos Santos Silva[1]
Orientadora: Profa. Rosana Reis de Melo Silva[2]

RESUMO

O avanço das tecnologias digitais e da conectividade global ampliou a ocorrência de crimes cibernéticos com repercussões transnacionais, impondo novos desafios aos mecanismos de persecução penal e à cooperação jurídica internacional. Nesse contexto, este estudo analisa os desafios jurídicos relacionados à extradição de criminosos digitais no Brasil, no período de 2012 a 2025, com enfoque nos conflitos de jurisdição, no princípio da dupla incriminação e na proteção dos direitos fundamentais do extraditando. O objetivo da pesquisa consiste em compreender os fatores que influenciam a efetividade dos pedidos extradicionais diante da crescente complexidade dos delitos praticados em ambiente virtual. A fundamentação teórica baseia-se na doutrina do Direito Digital, do Direito Penal e do Direito Internacional, bem como na legislação brasileira e em instrumentos internacionais voltados ao enfrentamento do cibercrime. A metodologia possui abordagem qualitativa, fundamentada em pesquisa bibliográfica e documental, com análise normativa de legislações nacionais e internacionais. Os resultados indicam que a ausência de harmonização legislativa, a diversidade de tipificações penais e os desafios probatórios reduzem a eficiência dos mecanismos tradicionais de extradição. Conclui-se que o fortalecimento da cooperação internacional e o aperfeiçoamento normativo são medidas essenciais para ampliar a efetividade da responsabilização penal no contexto da criminalidade digital transnacional.

[1] Graduando(a) do curso de Bacharelado em Direito,no Centro Universitário FAMETRO. Manaus, Amazonas, Brasil E-mail: luizkorn@hotmail.com. ORCID iD: 0009-0003-1510-6801. Disponível em: https://orcid.org/0009-0003-1510-6801

[2] Prof.ª Orientadora e Coordenadora do TCC II, no Centro Universitário FAMETRO: Prof.ª Esp. Rosana Reis de Melo Silva. Manaus, Amazonas, Brasil. E-mail: rosanareismello@gmail.com

Palavras-chave: Extradição. Crimes digitais. Cooperação internacional. Dupla incriminação. Direitos fundamentais.

ABSTRACT

The advancement of digital technologies and global connectivity has increased the occurrence of cybercrimes with transnational repercussions, creating new challenges for criminal prosecution and international legal cooperation. In this context, this study analyzes the legal challenges related to the extradition of digital criminals in Brazil between 2012 and 2025, focusing on jurisdictional conflicts, the principle of double criminality, and the protection of the extradited person's fundamental rights. The objective of this research is to understand the factors influencing the effectiveness of extradition requests in light of the growing complexity of crimes committed in digital environments. The theoretical framework is based on Digital Law, Criminal Law, and International Law doctrines, as well as Brazilian legislation and international legal instruments related to cybercrime. The methodology adopts a qualitative approach based on bibliographic and documentary research, including normative analysis of national and international legal frameworks. The findings indicate that the lack of legislative harmonization, divergences in criminal classification, and evidentiary challenges reduce the effectiveness of traditional extradition mechanisms. It is concluded that strengthening international cooperation and improving legal frameworks are essential measures to enhance accountability in transnational cybercrime.

Keywords: Extradition. Cybercrime. International cooperation. Double criminality. Fundamental rights.

1 INTRODUÇÃO

A expansão das tecnologias digitais e da conectividade global transformou significativamente as relações sociais, econômicas e institucionais, permitindo novas formas de comunicação, circulação de informações e interação entre indivíduos. Paralelamente a esses avanços, verificou-se o crescimento de práticas ilícitas realizadas no ambiente virtual, especialmente crimes cibernéticos caracterizados pela rapidez de execução, dificuldade de identificação dos agentes e alcance transnacional.

No contexto da criminalidade digital, a extradição assume papel relevante como instrumento de cooperação jurídica internacional, sobretudo em situações nas quais o autor do delito se encontra em país distinto daquele em que os efeitos da infração ocorreram. Entretanto, a efetividade dos pedidos extradicionais enfrenta obstáculos relacionados à diversidade legislativa entre os Estados, à complexidade

probatória e às dificuldades de definição da jurisdição competente.

Os crimes digitais desafiam institutos clássicos do Direito Penal e do Direito Internacional, especialmente em razão da multiplicidade de territórios envolvidos na prática criminosa, da volatilidade das provas eletrônicas e da ausência de harmonização legislativa entre países. Segundo Teixeira (2022), a criminalidade digital impõe ao Direito necessidade contínua de adaptação normativa e fortalecimento dos mecanismos de cooperação internacional, uma vez que o ambiente virtual relativiza limites territoriais tradicionalmente adotados pelos sistemas jurídicos.

Nesse cenário, o presente estudo tem como problema de pesquisa compreender de que forma os conflitos de jurisdição, o princípio da dupla incriminação e a proteção dos direitos fundamentais influenciam a efetividade da extradição de criminosos digitais no Brasil entre os anos de 2012 e 2025.

Parte-se da hipótese de que a ausência de harmonização legislativa internacional, associada às divergências na tipificação penal e às limitações dos mecanismos tradicionais de cooperação jurídica, compromete a efetividade dos pedidos extradicionais relacionados à criminalidade digital.

O objetivo geral consiste em analisar os principais desafios jurídicos relacionados à extradição de criminosos digitais no Brasil, considerando os impactos dos conflitos jurisdicionais, da dupla incriminação e dos direitos fundamentais na efetividade dos pedidos extradicionais. Como objetivos específicos, busca-se compreender os conflitos de jurisdição no ciberespaço, examinar os desafios da dupla incriminação nos crimes digitais, discutir os limites constitucionais da extradição e analisar os reflexos das novas tecnologias sobre a responsabilização penal internacional.

A relevância da pesquisa decorre do crescimento da criminalidade digital e dos impactos sociais, econômicos e jurídicos produzidos por fraudes eletrônicas, invasões de sistemas, crimes patrimoniais digitais e ataques cibernéticos. Dessa forma, o fortalecimento da cooperação internacional apresenta-se como medida necessária para ampliar a capacidade de responsabilização penal sem afastar a proteção das garantias fundamentais asseguradas pelo Estado Democrático de Direito.

2 CRIMES DIGITAIS E EXTRADIÇÃO INTERNACIONAL

A expansão das tecnologias digitais ampliou significativamente a ocorrência de

práticas criminosas realizadas em ambiente virtual, impondo desafios relevantes à persecução penal e aos mecanismos tradicionais de cooperação jurídica internacional. Os crimes digitais, também denominados crimes cibernéticos ou informáticos, correspondem às condutas ilícitas praticadas por intermédio de sistemas computacionais, redes digitais ou dispositivos eletrônicos, podendo ter a tecnologia como instrumento ou como objeto diretamente atingido pela infração.

A criminalidade digital apresenta características próprias, como rapidez de execução, dificuldade de rastreamento dos responsáveis, volatilidade das provas e alcance transnacional. Diferentemente dos delitos convencionais, os crimes praticados em ambiente virtual frequentemente envolvem múltiplos territórios, dificultando a definição da competência jurisdicional e a responsabilização penal dos envolvidos.

Segundo Teixeira (2022), o desenvolvimento tecnológico desafia institutos clássicos do Direito Penal, especialmente aqueles relacionados à territorialidade, à individualização da conduta e à produção de provas. Nesse contexto, a extradição assume papel relevante como instrumento de cooperação internacional voltado à responsabilização de indivíduos que praticam delitos em determinado país e se encontram fisicamente em outro território.

2.1 Tipicidade penal dos crimes digitais

No ordenamento jurídico brasileiro, a tipificação penal dos crimes digitais ocorreu de maneira gradual. Durante muitos anos, condutas praticadas no ambiente virtual eram enquadradas em tipos penais tradicionais, sobretudo crimes patrimoniais, estelionato, falsidade documental e delitos contra a honra.

Entretanto, o aumento de ataques cibernéticos e invasões de dispositivos informáticos evidenciou a necessidade de regulamentação específica. Nesse cenário, a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, introduziu no Código Penal o artigo 154-A, criminalizando a invasão de dispositivo informático mediante violação indevida de mecanismo de segurança para obtenção, adulteração ou destruição de dados sem autorização do titular.

Posteriormente, a Lei nº 14.155/2021 fortaleceu o enfrentamento aos delitos eletrônicos ao ampliar penas relacionadas à fraude eletrônica e disciplinar condutas praticadas por meios digitais, especialmente fraudes patrimoniais executadas com utilização de redes sociais, engenharia social e invasão de dispositivos.

A tipicidade penal assume relevância central no procedimento extradicional, pois a responsabilização do agente depende da existência de correspondência mínima entre os sistemas jurídicos envolvidos. Assim, diferenças legislativas podem dificultar o reconhecimento da conduta criminosa, comprometendo a efetividade da cooperação internacional.

2.2 Transnacionalidade e conflitos de jurisdição

Uma das principais características dos crimes digitais consiste em sua dimensão transnacional. Em muitos casos, o agente encontra-se localizado em determinado país, utiliza servidores hospedados em outro território e produz danos em localidades distintas, tornando complexa a definição da competência jurisdicional.

No Brasil, a definição do local do crime encontra fundamento na teoria da ubiquidade, prevista no artigo 6º do Código Penal, segundo a qual o delito considera-se praticado tanto no local da ação ou omissão quanto no local do resultado.

Essa teoria possui especial relevância nos crimes digitais, pois permite ampliar possibilidades de responsabilização penal diante da multiplicidade de conexões territoriais existentes no ambiente virtual. Entretanto, a simples incidência da teoria da ubiquidade não elimina conflitos positivos de jurisdição, situações nas quais diferentes Estados se reconhecem simultaneamente competentes para processar e julgar determinado fato criminoso.

Além da teoria da ubiquidade, a definição da jurisdição competente em crimes digitais envolve discussão sobre os limites da soberania estatal diante da circulação global de dados e informações. Em diversos casos, a prática criminosa ocorre de forma fragmentada, envolvendo países distintos em uma mesma dinâmica delitiva. O agente pode executar comandos em determinado território, utilizar servidores instalados em outro país e produzir efeitos econômicos ou patrimoniais em diferentes localidades, tornando complexa a delimitação da competência jurisdicional.

> Segundo Rezek (2018), o fortalecimento da cooperação internacional tornou-se indispensável diante da crescente interdependência entre os Estados, especialmente em situações nas quais a atividade ilícita transcende fronteiras territoriais tradicionais. No ambiente digital, essa realidade assume dimensão ainda mais significativa, pois os fluxos informacionais

frequentemente não respeitam limitações geográficas estatais.

Outro fator relevante refere-se à disputa entre jurisdições potencialmente competentes para processar e julgar determinado fato criminoso. Em crimes cibernéticos de elevada repercussão econômica ou institucional, diferentes países podem reivindicar competência com fundamento na nacionalidade da vítima, na localização dos prejuízos financeiros, na proteção de interesses estratégicos nacionais ou no local em que a ação foi iniciada. Nessas hipóteses, a cooperação internacional e a definição de critérios coordenados tornam-se indispensáveis para evitar impunidade e conflitos diplomáticos.

Nessas hipóteses, podem coexistir múltiplos fundamentos de competência, incluindo o local da ação, o local do resultado, a nacionalidade do agente, a nacionalidade da vítima ou a proteção de interesses estratégicos do Estado. Tal cenário exige intensificação da cooperação internacional para evitar impunidade e insegurança jurídica.

2.3 Produção probatória e identificação dos agentes

Outro desafio relevante refere-se à volatilidade das provas digitais e à identificação dos responsáveis pelas infrações. Diferentemente das provas tradicionais, os registros eletrônicos podem ser rapidamente alterados, excluídos ou transferidos, dificultando a reconstrução dos fatos e a individualização da autoria.

Elementos como endereços IP, registros de conexão, dados de acesso e informações armazenadas em servidores dependem frequentemente de preservação imediata e de cooperação entre autoridades nacionais e estrangeiras. A demora na obtenção dessas informações pode comprometer investigações e inviabilizar pedidos extradicionais.

A produção probatória nos crimes digitais apresenta dificuldades específicas em razão da natureza dinâmica dos ambientes tecnológicos e da facilidade de manipulação ou eliminação de vestígios eletrônicos. Diferentemente das provas materiais convencionais, elementos digitais dependem frequentemente de preservação imediata, sob pena de comprometer a integridade das informações relevantes para a investigação criminal.

A identificação dos agentes envolvidos em delitos cibernéticos também enfrenta obstáculos decorrentes do uso de tecnologias de anonimização, redes

privadas virtuais (*virtual private networks* – VPN), perfis falsos, criptografia e mecanismos de mascaramento de endereço IP, circunstâncias que dificultam a individualização da autoria e a vinculação entre conduta e responsável.

Segundo Teixeira (2022), a persecução penal no ambiente digital exige não apenas atualização legislativa, mas também aprimoramento técnico das autoridades investigativas e fortalecimento da cooperação entre instituições nacionais e internacionais. Em muitos casos, a coleta de evidências depende da colaboração de provedores de internet, plataformas digitais e empresas responsáveis pelo armazenamento de dados em servidores estrangeiros.

Além disso, a demora na obtenção de registros eletrônicos pode comprometer significativamente a investigação, sobretudo diante da volatilidade dos dados armazenados digitalmente. Por essa razão, medidas de preservação cautelar de provas e instrumentos de assistência jurídica internacional assumem relevância estratégica para a efetividade dos pedidos extradicionais relacionados à criminalidade digital transnacional.

No procedimento de extradição, a demonstração mínima da autoria e da materialidade possui relevância essencial, pois o Estado requerente deve apresentar elementos capazes de justificar a legitimidade do pedido, preservando simultaneamente garantias processuais e direitos fundamentais do indivíduo submetido à persecução penal.

3. O PRINCÍPIO DA DUPLA INCRIMINAÇÃO E A COOPERAÇÃO INTERNACIONAL

O princípio da dupla incriminação constitui requisito tradicional da cooperação penal internacional e representa um dos principais fundamentos jurídicos dos procedimentos extradicionais. Em termos gerais, exige-se que a conduta atribuída ao indivíduo seja considerada crime tanto no Estado requerente quanto no Estado requerido, ainda que existam diferenças quanto à nomenclatura ou à estrutura legislativa adotada (MAZZUOLI, 2021).

Esse princípio atua como mecanismo de proteção da legalidade penal e da soberania estatal, impedindo que determinado país entregue um indivíduo para responder por conduta não reconhecida como criminosa em seu próprio ordenamento jurídico. Nesse sentido, a dupla incriminação relaciona-se diretamente ao princípio da

legalidade, segundo o qual não há crime nem pena sem previsão legal anterior (*nullum crimen, nulla poena sine lege*) (BRASIL, 1988).

Nos crimes digitais, entretanto, a aplicação deste requisito torna-se mais complexa em razão da velocidade das transformações tecnológicas e da ausência de uniformidade legislativa internacional. Conforme observa Teixeira (2022), a criminalidade digital impõe “desafios permanentes de atualização normativa”, sobretudo diante do surgimento contínuo de novas modalidades criminosas mediadas por tecnologia.

3.1 A dupla incriminação nos crimes digitais

A principal dificuldade relacionada à dupla incriminação nos crimes digitais decorre da fragmentação normativa existente entre os Estados. Enquanto alguns países desenvolveram legislações específicas para ataques cibernéticos, invasão de sistemas, fraudes eletrônicas e manipulação indevida de dados, outros ainda realizam enquadramento dessas condutas em tipos penais tradicionais (TEIXEIRA, 2022).

No Brasil, a Lei nº 12.737/2012 introduziu relevante proteção penal ao tipificar a invasão de dispositivo informático, enquanto a Lei nº 14.155/2021 fortaleceu o enfrentamento às fraudes eletrônicas mediante agravamento de penas e ampliação da proteção patrimonial digital (BRASIL, 2012; BRASIL, 2021).

Todavia, a existência de diferentes modelos de criminalização pode comprometer pedidos de extradição, especialmente quando o Estado requerido entende inexistir correspondência penal suficiente para justificar a entrega do extraditando. Em tais hipóteses, a cooperação internacional tende a enfrentar entraves jurídicos relacionados à equivalência material da conduta.

> Por essa razão, parte da doutrina sustenta interpretação menos formalista da dupla incriminação, admitindo análise material do comportamento investigado em vez de exigir identidade absoluta entre os tipos penais dos países envolvidos (MAZZUOLI, 2021).

3.2 Convenção de Budapeste e harmonização legislativa

A cooperação internacional constitui elemento indispensável para o enfrentamento da criminalidade digital transnacional. Em razão da ausência de

fronteiras no ambiente virtual, os Estados dependem de instrumentos multilaterais voltados à produção de provas, compartilhamento de informações e harmonização legislativa.

Nesse contexto, a Convenção sobre o Crime Cibernético, conhecida como Convenção de Budapeste, representa importante marco jurídico internacional ao estabelecer diretrizes para criminalização de condutas praticadas no ambiente digital, preservação de evidências eletrônicas e cooperação entre autoridades nacionais (CONSELHO DA EUROPA, 2001).

A Convenção de Budapeste representa importante instrumento jurídico internacional por buscar reduzir assimetrias legislativas relacionadas ao enfrentamento do cibercrime. Entre seus objetivos destacam-se a padronização mínima da criminalização de determinadas condutas, o fortalecimento da cooperação internacional e a facilitação do compartilhamento de provas eletrônicas entre Estados signatários.

A preservação de evidências digitais assume papel central nesse contexto, uma vez que registros eletrônicos podem ser rapidamente alterados, destruídos ou transferidos para jurisdições distintas. Em razão disso, a Convenção estabelece mecanismos voltados à preservação expedita de dados informáticos e ao intercâmbio de informações entre autoridades competentes, ampliando a eficiência investigativa.

> Conforme Teixeira (2022), o avanço tecnológico impõe necessidade contínua de atualização normativa, pois a velocidade das transformações digitais frequentemente supera a capacidade de resposta legislativa dos Estados. Assim, instrumentos internacionais de harmonização tornam-se relevantes para reduzir lacunas jurídicas e fortalecer mecanismos de persecução penal transnacional.

No Brasil, a promulgação da Convenção ocorreu por meio do Decreto nº 11.491/2023, fortalecendo mecanismos de assistência jurídica internacional e aproximando o país de parâmetros internacionais de enfrentamento ao cibercrime (BRASIL, 2023).

> Segundo Rezek (2018), a cooperação internacional revela-se instrumento indispensável para efetividade do Direito Internacional, especialmente quando problemas jurídicos

> ultrapassam fronteiras territoriais e exigem atuação coordenada entre Estados soberanos.

Apesar dos avanços, persistem desafios relacionados às diferenças culturais, legislativas e políticas entre países, o que demonstra que a harmonização normativa permanece em processo gradual e em constante transformação.

3.3 Limites e efetividade da extradição

A efetividade da extradição em crimes digitais depende não apenas da existência de tratados internacionais, mas também da capacidade dos Estados em produzir elementos mínimos de autoria, materialidade e conexão jurisdicional capazes de justificar o pedido extradicional.

> Nos delitos cibernéticos, dificuldades probatórias relacionadas à volatilidade dos registros digitais, anonimização de usuários e utilização de servidores internacionais frequentemente reduzem a eficiência investigativa (TEIXEIRA, 2022).

Além disso, a multiplicidade de jurisdições potencialmente competentes pode gerar disputas entre Estados e atrasar a persecução penal, comprometendo a efetividade do combate ao crime digital transnacional.

Dessa forma, verifica-se que a cooperação internacional, a atualização legislativa e a interpretação coordenada do princípio da dupla incriminação constituem fatores essenciais para ampliar a eficiência da extradição sem afastar garantias fundamentais asseguradas ao extraditando.

4 DIREITOS FUNDAMENTAIS E LIMITES À EXTRADIÇÃO

A extradição constitui instrumento relevante de cooperação jurídica internacional destinado à responsabilização de indivíduos acusados da prática de delitos transnacionais. Entretanto, sua aplicação encontra limites relacionados à proteção dos direitos fundamentais, à soberania estatal e às garantias constitucionais asseguradas ao extraditando.

No Estado Democrático de Direito, a persecução penal não pode ocorrer dissociada do respeito ao devido processo legal, ao contraditório, à ampla defesa e à

dignidade da pessoa humana, fundamentos indispensáveis para legitimidade do exercício do poder punitivo (BRASIL, 1988). Assim, o Estado requerido deve verificar não apenas requisitos formais do pedido extradicional, mas também a compatibilidade do procedimento penal estrangeiro com parâmetros mínimos de proteção dos direitos humanos.

> Segundo Mazzuoli (2021), a cooperação penal internacional deve ocorrer em conformidade com os limites impostos pelos direitos fundamentais, evitando que mecanismos de repressão criminal resultem em arbitrariedades ou violações à integridade física, moral e processual do indivíduo.

4.1 Garantias fundamentais do extraditando

A Constituição Federal estabelece limites relevantes ao procedimento extradicional, especialmente ao vedar a extradição de brasileiro nato e impedir entrega por crime político ou de opinião (BRASIL, 1988). Essas restrições refletem a preocupação constitucional com a proteção da cidadania, da liberdade política e da dignidade humana.

A proteção dos direitos fundamentais no âmbito extradicional relaciona-se diretamente ao compromisso assumido pelos Estados democráticos com os direitos humanos e com a limitação do poder punitivo. O procedimento de extradição, embora possua natureza cooperativa, não pode resultar em mitigação de garantias jurídicas mínimas asseguradas ao indivíduo submetido ao pedido.

Nesse contexto, o Estado requerido deve avaliar não apenas a legalidade formal da solicitação, mas também a compatibilidade material do sistema jurídico do Estado requerente com princípios fundamentais do devido processo legal, da ampla defesa e da dignidade da pessoa humana. A preocupação torna-se ainda mais relevante quando houver risco de penas desproporcionais, ausência de garantias processuais ou condições degradantes de custódia.

> Segundo Mazzuoli (2021), a proteção dos direitos humanos constitui limite material da cooperação penal internacional, impondo aos Estados o dever de impedir que instrumentos de repressão criminal sejam utilizados em afronta a garantias fundamentais universalmente reconhecidas.

Além disso, o Estado brasileiro deve avaliar se o extraditando estará sujeito a práticas incompatíveis com direitos fundamentais, incluindo tratamento degradante, ausência de garantias processuais mínimas ou imposição de penas vedadas pela ordem constitucional brasileira.

> Conforme observa Rezek (2018), a cooperação internacional não afasta o dever dos Estados de preservar direitos fundamentais, exigindo equilíbrio entre repressão penal e proteção jurídica do indivíduo submetido ao procedimento.

Em razão disso, pedidos de extradição relacionados à criminalidade digital também devem observar o controle de proporcionalidade, legalidade e respeito às garantias processuais do investigado, ainda que haja interesse internacional no combate ao cibercrime.

4.2 Limites constitucionais da extradição no Brasil

No Brasil, os limites constitucionais da extradição encontram fundamento especialmente no artigo 5º da Constituição Federal, que estabelece parâmetros destinados à proteção do indivíduo diante do exercício do poder estatal (BRASIL, 1988).

A vedação da extradição de brasileiro nato constitui garantia absoluta, enquanto a extradição de naturalizado apresenta restrições específicas previstas constitucionalmente. Além disso, a impossibilidade de extradição por crime político ou de opinião representa importante mecanismo de proteção contra perseguições indevidas.

No contexto dos crimes digitais, tais limitações assumem relevância crescente diante de situações envolvendo vazamento de dados, espionagem cibernética, ataques informáticos e divulgação de informações sensíveis, circunstâncias que podem gerar debates sobre liberdade de expressão, interesse público e criminalização de condutas praticadas no ambiente virtual.

Desse modo, o procedimento extradicional exige análise cuidadosa da compatibilidade entre interesses repressivos internacionais e direitos fundamentais garantidos pela Constituição brasileira.

4.3 Inteligência artificial e novos desafios à responsabilização penal

O avanço da inteligência artificial ampliou desafios relacionados à responsabilização penal em crimes digitais, sobretudo diante da crescente automação de sistemas e da complexidade na identificação da autoria.

> Sistemas baseados em algoritmos podem executar operações automatizadas, processar grande volume de dados e produzir decisões sem supervisão humana contínua, dificultando a individualização da conduta criminosa e a demonstração dos requisitos necessários à persecução penal (TEIXEIRA, 2022).

Nos pedidos de extradição, a dificuldade de demonstrar autoria, materialidade e vínculo subjetivo do agente pode comprometer a efetividade da responsabilização penal, especialmente quando a prática criminosa envolve múltiplos territórios, servidores internacionais e tecnologias de anonimização.

Nesse sentido, a evolução tecnológica reforça a necessidade de atualização normativa e fortalecimento dos mecanismos de cooperação internacional, permitindo respostas jurídicas mais eficazes diante da criminalidade digital contemporânea.

5 CONSIDERAÇÕES FINAIS

O presente estudo analisou os desafios jurídicos relacionados à extradição de criminosos digitais no Brasil entre os anos de 2012 e 2025, com enfoque nos conflitos de jurisdição, no princípio da dupla incriminação e na proteção dos direitos fundamentais no contexto da cooperação penal internacional.

Verificou-se que a criminalidade digital impõe dificuldades relevantes aos modelos tradicionais de persecução penal, especialmente em razão da transnacionalidade das condutas, da volatilidade das provas eletrônicas e da diversidade legislativa existente entre os Estados. A multiplicidade de territórios envolvidos na prática dos delitos amplia conflitos de jurisdição e exige mecanismos mais eficientes de articulação entre autoridades nacionais e internacionais.

Observou-se, ainda, que a dupla incriminação permanece requisito essencial da extradição, funcionando como garantia da legalidade penal e da soberania estatal. Entretanto, sua aplicação nos crimes digitais encontra obstáculos decorrentes da ausência de harmonização normativa, o que pode comprometer a efetividade dos

pedidos extradicionais.

Também se concluiu que a proteção dos direitos fundamentais constitui limite indispensável ao exercício da cooperação penal internacional, impondo ao Estado dever de compatibilizar repressão criminal e respeito às garantias constitucionais do extraditando.

Por fim, conclui-se que a efetividade da extradição de criminosos digitais depende do fortalecimento da cooperação internacional, da modernização legislativa e da construção de mecanismos jurídicos capazes de responder às transformações tecnológicas sem afastar os princípios fundamentais do Estado Democrático de Direito.

6 REFERÊNCIAS

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 3 jun. 2026.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Brasília, DF: Presidência da República, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 3 jun. 2026.

BRASIL. Decreto nº 11.491, de 5 de julho de 2023. Promulga a Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001. Diário Oficial da União, Brasília, DF, 6 jul. 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm. Acesso em: 3 jun. 2026.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Diário Oficial da União, Brasília, DF, 3 dez. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 3 jun. 2026.

BRASIL. Lei nº 13.445, de 24 de maio de 2017. Institui a Lei de Migração. Diário Oficial da União, Brasília, DF, 25 maio 2017. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13445.htm. Acesso em: 3 jun. 2026.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar fraude eletrônica e ampliar penas relacionadas a crimes cibernéticos. Diário Oficial da União, Brasília, DF, 28 maio 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 3 jun. 2026.

CONSELHO DA EUROPA. Convention on Cybercrime. Budapest, 23 Nov. 2001. Strasbourg: Council of Europe, 2001. Disponível em: https://www.coe.int/en/web/cybercrime/the-budapest-convention. Acesso em: 3 jun. 2026.

MAZZUOLI, Valerio de Oliveira. Curso de direito internacional público. 14. ed. Rio de Janeiro: Forense, 2021.

REZEK, Francisco. Direito internacional público: curso elementar. 16. ed. São Paulo: Saraiva, 2018.

TEIXEIRA, Tarcisio. Direito digital e processo eletrônico. 6. ed. São Paulo: Saraiva Educação, 2022.