

RESPONSABILIDADE PENAL DAS PESSOAS JURÍDICAS POR CRIMES CIBERNÉTICOS NO BRASIL À LUZ DA CONVENÇÃO DE BUDAPESTE

Deyber Silva Urbano

Resumo: A expansão das tecnologias digitais e o crescimento dos crimes cibernéticos têm imposto novos desafios ao Direito Penal, especialmente quanto à possibilidade de responsabilização das pessoas jurídicas por condutas praticadas no ambiente virtual. Nesse contexto, esta pesquisa teve como objetivo geral analisar a possibilidade de responsabilização penal das pessoas jurídicas pela prática de crimes cibernéticos no ordenamento jurídico brasileiro à luz da Convenção de Budapeste. Para tanto, foi realizada uma pesquisa bibliográfica, de abordagem qualitativa e caráter descritivo, fundamentada em produções científicas publicadas entre 2021 e 2026, localizadas nas bases SciELO e Google Acadêmico. Foram selecionados quinze trabalhos acadêmicos e oito documentos oficiais, totalizando vinte e três materiais analisados. Os resultados demonstraram que a legislação brasileira apresenta avanços no tratamento dos crimes cibernéticos, porém ainda existem limitações quanto à responsabilização penal direta das pessoas jurídicas nesse campo. Verificou-se que a Convenção de Budapeste contempla a responsabilidade dos entes coletivos, mas admite sua configuração nas esferas criminal, civil ou administrativa, conforme os princípios jurídicos de cada Estado. Concluiu-se, portanto, que a incorporação da Convenção ao ordenamento brasileiro não estabelece automaticamente um regime geral de responsabilidade penal das pessoas jurídicas por crimes cibernéticos. Nesse sentido, eventuais aperfeiçoamentos legislativos devem estabelecer critérios claros de imputação e conciliar a efetividade do combate à criminalidade digital com os princípios e garantias fundamentais do Direito Penal.

Palavras-chave: crimes cibernéticos. responsabilidade penal. pessoa jurídica. Convenção de Budapeste. direito penal.

Abstract: The expansion of digital technologies and the growth of cybercrime have created new challenges for Criminal Law, particularly regarding the possibility of holding legal entities criminally liable for conduct carried out in digital environments. In this context, the general objective of this research was to analyze the possibility of criminal liability of legal

entities for cybercrimes under the Brazilian legal system in light of the Budapest Convention. A bibliographic research study was conducted using a qualitative and descriptive approach, based on scientific publications issued between 2021 and 2026 and retrieved from SciELO and Google Scholar. Fifteen academic studies and eight official documents were selected, totaling twenty-three materials analyzed. The results demonstrated that Brazilian legislation has advanced in addressing cybercrime, although significant limitations remain regarding the direct criminal liability of legal entities in this field. The analysis showed that the Budapest Convention provides for the liability of legal entities but allows such liability to be criminal, civil, or administrative, according to the legal principles of each State. Therefore, the incorporation of the Convention into the Brazilian legal system does not automatically establish a general framework for the criminal liability of legal entities for cybercrimes. Accordingly, possible legislative improvements should establish clear criteria for attribution of liability while reconciling effective responses to digital crime with the fundamental principles and guarantees of Criminal Law.

Keywords: cybercrime. criminal liability. legal entities. Budapest Convention. criminal law.

INTRODUÇÃO

O avanço das tecnologias digitais e a crescente integração de sistemas informatizados às atividades econômicas, sociais e institucionais modificaram significativamente as formas de interação e circulação de informações na sociedade contemporânea. Paralelamente aos benefícios proporcionados pela transformação digital, surgiram novas possibilidades para a prática de condutas ilícitas, caracterizadas pelo uso de computadores, redes, sistemas e dados como instrumentos ou alvos de atividades criminosas. Nesse sentido, Lima Filho (2021) destaca que as transformações tecnológicas associadas à Quarta Revolução Industrial produziram novos desafios para o Direito Penal, especialmente diante da expansão e diversificação das práticas criminosas desenvolvidas no ambiente digital.

Além da responsabilização das pessoas físicas diretamente envolvidas nas condutas criminosas, o desenvolvimento da criminalidade cibernética suscita discussões acerca da participação e da responsabilidade das pessoas jurídicas. Empresas e outras organizações podem dispor de estruturas tecnológicas, recursos financeiros e sistemas capazes de serem utilizados para a prática ou facilitação de ilícitos digitais, inclusive em benefício da própria organização. A possibilidade de responsabilização dos entes coletivos nesse contexto ganha especial relevância diante das novas configurações assumidas pela criminalidade tecnológica (Costa & Buzetti, 2025).

No cenário internacional, a Convenção de Budapeste sobre o Crime Cibernético constitui importante instrumento de harmonização legislativa e cooperação entre os Estados, contemplando também disposições relacionadas à responsabilidade das pessoas jurídicas. Araujo (2022) destaca a importância desse instrumento internacional para a construção de respostas jurídicas aos crimes cibernéticos, enquanto sua incorporação ao ordenamento brasileiro foi formalizada por meio do Decreto nº 11.491/2023 (Brasil, 2023).

Conforme Hammerschmidt e David (2023), a responsabilização penal da pessoa coletiva envolve questões relevantes relacionadas ao princípio da culpabilidade, enquanto Murata e Torres (2023) evidenciam que a promulgação da Convenção de Budapeste no Brasil trouxe novos aspectos a serem considerados quanto aos seus efeitos e à adequação do ordenamento jurídico nacional. Assim, estabelece-se como problema de pesquisa: em que medida o ordenamento jurídico brasileiro permite a responsabilização penal das pessoas jurídicas por crimes cibernéticos diante das disposições da Convenção de Budapeste?

Pressupõe-se que a incorporação da Convenção ao sistema brasileiro fortalece o debate sobre a responsabilidade corporativa no ambiente digital, mas não produz, isoladamente, uma ampliação automática da responsabilidade penal das pessoas jurídicas, podendo evidenciar a necessidade de aperfeiçoamentos legislativos e de maior adequação normativa.

O objetivo geral desta pesquisa consiste em analisar a possibilidade de responsabilização penal das pessoas jurídicas pela prática de crimes cibernéticos no ordenamento jurídico brasileiro à luz da Convenção de Budapeste. Especificamente, busca-se compreender os crimes cibernéticos e sua regulamentação no Brasil; examinar os fundamentos, limites e possibilidades da responsabilidade penal das pessoas jurídicas no sistema jurídico nacional; analisar as disposições da Convenção de Budapeste relacionadas à responsabilidade das pessoas jurídicas; e discutir a compatibilidade entre os compromissos internacionais assumidos pelo Brasil e a legislação interna, identificando possíveis lacunas e perspectivas de aperfeiçoamento jurídico.

A relevância desta pesquisa decorre da crescente presença das pessoas jurídicas no ambiente digital e da necessidade de respostas jurídicas adequadas diante da utilização de estruturas empresariais e organizacionais para a prática ou facilitação de ilícitos cibernéticos. No campo científico, o estudo contribui para o debate acerca dos limites da responsabilidade penal dos entes coletivos e da incorporação de normas internacionais ao Direito brasileiro, aproximando as discussões do Direito Penal, do Direito Digital e do Direito Internacional.

METODOLOGIA

A presente pesquisa caracteriza-se como uma pesquisa bibliográfica, de abordagem qualitativa e caráter descritivo, desenvolvida com a finalidade de analisar a responsabilidade penal das pessoas jurídicas pela prática de crimes cibernéticos no ordenamento jurídico brasileiro, especialmente diante das disposições da Convenção de Budapeste.

De acordo com Gil (2019), a pesquisa bibliográfica é elaborada com base em materiais já publicados, especialmente livros e artigos científicos, permitindo ao pesquisador conhecer e analisar diferentes contribuições teóricas relacionadas ao problema investigado. De maneira complementar, Marconi e Lakatos (2021) destacam que a pesquisa bibliográfica possibilita estabelecer contato com conhecimentos anteriormente produzidos acerca do objeto de estudo, favorecendo sua análise e interpretação.

Para a construção da revisão bibliográfica, foram consideradas produções publicadas nos últimos cinco anos, compreendendo o período de 2021 a 2026, buscando privilegiar perspectivas recentes sobre as transformações da criminalidade digital e os efeitos da adesão brasileira à Convenção de Budapeste. As buscas foram realizadas nas bases SciELO e Google Acadêmico, utilizando as palavras-chave “responsabilidade penal da pessoa jurídica”, “crimes cibernéticos” e “Convenção de Budapeste”, de maneira isolada e combinada, a fim de localizar produções relacionadas diretamente aos eixos centrais da investigação.

Como critérios de inclusão, foram selecionados artigos e trabalhos acadêmicos publicados entre 2021 e 2026, disponíveis em língua portuguesa e relacionados diretamente à questão de pesquisa, especialmente aqueles que abordassem responsabilidade penal das

peessoas jurídicas, crimes cibernéticos, legislação penal brasileira, Convenção de Budapeste, cooperação internacional, provas digitais e desafios jurídicos decorrentes da criminalidade informática.

Foram excluídos estudos publicados fora do período delimitado, trabalhos duplicados, produções que não apresentassem relação direta com o objeto investigado e materiais que, após a leitura do título, resumo ou conteúdo, não contribuíssem para responder ao problema de pesquisa.

Após a aplicação dos critérios estabelecidos, foram selecionados 15 trabalhos acadêmicos, publicados entre 2021 e 2026, que constituíram a base da revisão bibliográfica. Além das produções acadêmicas, realizou-se pesquisa documental complementar, necessária em razão da natureza jurídica do objeto investigado. Foram selecionados oito documentos oficiais, compreendendo a Constituição da República Federativa do Brasil de 1988, o Código Penal, a Lei nº 9.605/1998, a Lei nº 12.735/2012, a Lei nº 12.737/2012, a Lei nº 12.965/2014, o Decreto Legislativo nº 37/2021 e o Decreto nº 11.491/2023.

Esses documentos foram utilizados independentemente do recorte temporal estabelecido para os artigos científicos, considerando que permanecem relevantes para a compreensão do regime jurídico vigente e dos fundamentos normativos relacionados ao problema estudado.

Entre os documentos analisados, recebeu especial atenção o Decreto nº 11.491/2023, responsável pela promulgação da Convenção sobre o Crime Cibernético no ordenamento brasileiro, particularmente seu art. 12, relacionado à responsabilidade da pessoa jurídica. Também foram examinadas as normas brasileiras referentes aos crimes informáticos e, para fins comparativos, a Lei nº 9.605/1998, considerando sua importância

para a compreensão da responsabilidade penal das pessoas jurídicas no sistema jurídico nacional. Ao todo, o corpus da pesquisa foi constituído por 23 materiais, sendo 15 produções acadêmicas e oito documentos oficiais.

Os materiais selecionados foram submetidos à leitura, organização e análise qualitativa, sendo agrupados conforme os principais eixos temáticos da pesquisa. A interpretação ocorreu mediante o confronto entre a literatura científica recente e o conteúdo dos documentos oficiais, buscando compreender os limites e as possibilidades da responsabilidade penal das pessoas jurídicas por crimes cibernéticos no Brasil.

DESENVOLVIMENTO

3.1 Crimes cibernéticos e sua regulamentação no ordenamento jurídico brasileiro

O desenvolvimento das tecnologias digitais alterou significativamente as relações sociais, econômicas e institucionais, ampliando a circulação de informações e a dependência de sistemas conectados. Essa transformação também proporcionou novas oportunidades para a prática de condutas criminosas, fazendo com que o ambiente virtual se tornasse espaço relevante para diferentes modalidades delitivas. Lima Filho (2021) relaciona esse cenário às transformações decorrentes da Quarta Revolução Industrial e aos novos desafios impostos ao Direito Penal.

A criminalidade cibernética apresenta características que dificultam sua compreensão a partir das categorias tradicionais do Direito Penal. As condutas podem ocorrer de maneira instantânea, alcançar vítimas localizadas em diferentes territórios e envolver agentes cuja identificação nem sempre é simples. Para Coltro e Waldman (2021), a criminalidade digital evidencia problemas relacionados à aplicação das normas existentes,

especialmente diante da dimensão transnacional adquirida por determinadas práticas realizadas por intermédio das tecnologias da informação.

Nesse contexto, os crimes cibernéticos podem ser compreendidos como condutas ilícitas relacionadas ao uso de computadores, redes, dispositivos e sistemas digitais, seja porque esses recursos constituem o próprio alvo da ação criminosa, seja porque funcionam como instrumentos para sua realização. Nóbrega (2022) demonstra que a diversidade dessas práticas exige atenção quanto ao enquadramento penal, pois o desenvolvimento tecnológico ocorre em ritmo distinto daquele observado na produção e atualização das normas jurídicas.

Uma distinção relevante para a compreensão do fenômeno ocorre entre crimes cibernéticos próprios e impróprios. Nos primeiros, sistemas, dispositivos ou dados informáticos constituem elementos diretamente atingidos pela conduta, enquanto, nos segundos, a tecnologia funciona principalmente como meio para a realização de crimes já conhecidos pelo Direito Penal. Essa diversidade contribui para dificuldades de tipificação e aplicação normativa, conforme destacam Silva e Fayão (2025), sobretudo diante do surgimento contínuo de novas práticas digitais.

No ordenamento brasileiro, o Código Penal permanece como uma das principais referências para a repressão de condutas criminosas realizadas por meios tecnológicos, embora sua elaboração seja muito anterior à expansão da internet (Brasil, 1940). Diversos delitos tradicionais passaram a ser praticados também no ambiente virtual, exigindo interpretações e posteriores alterações legislativas. Essa realidade demonstra que o enfrentamento da criminalidade digital ocorreu, em

grande medida, mediante adaptações de estruturas jurídicas anteriormente existentes.

A necessidade de respostas mais específicas levou à edição da Lei nº 12.735/2012, que promoveu alterações relacionadas às condutas realizadas mediante sistemas eletrônicos, digitais ou semelhantes e estabeleceu medidas direcionadas ao enfrentamento dessas práticas (Brasil, 2012a). Entretanto, a produção de novas normas não eliminou as dificuldades existentes. Simões (2023) identifica deficiências legislativas no tratamento dos crimes cibernéticos, principalmente em razão da velocidade das mudanças tecnológicas e da constante criação de novas formas de atuação criminosa.

Também em 2012 foi promulgada a Lei nº 12.737, conhecida pela associação ao caso Carolina Dieckmann, responsável por introduzir no Código Penal a tipificação da invasão de dispositivo informático. A legislação representou avanço na proteção penal de dispositivos e informações digitais ao estabelecer resposta específica para determinadas formas de acesso indevido (Brasil, 2012b). Ainda assim, Nóbrega (2022) observa que a complexidade dos crimes cibernéticos exige constante avaliação da capacidade normativa brasileira de acompanhar novas práticas.

As fraudes eletrônicas constituem outro aspecto relevante da criminalidade digital contemporânea, especialmente porque técnicas de engenharia social podem ser utilizadas para induzir vítimas a fornecer informações ou realizar operações financeiras. Entre essas práticas encontra-se o phishing, caracterizado pelo emprego de mecanismos fraudulentos destinados à obtenção de dados e vantagens indevidas. Oliveira e Silva (2026) ressaltam os desafios investigativos e jurídicos

associados ao phishing e ao estelionato eletrônico após as alterações legislativas promovidas no Brasil.

O ambiente virtual também possibilitou a ampliação do alcance de crimes contra a honra, uma vez que conteúdos ofensivos podem ser rapidamente publicados, compartilhados e armazenados em diferentes plataformas. Cruz (2024) analisa essas práticas destacando particularmente seus efeitos no campo da responsabilidade civil, demonstrando que o ambiente digital pode produzir consequências jurídicas em diferentes esferas. Essa perspectiva permite distinguir a reparação do dano da responsabilização penal decorrente de uma conduta tipificada como crime.

A identificação do autor representa uma das dificuldades encontradas na investigação de crimes cibernéticos. Recursos tecnológicos podem dificultar a localização do responsável pela conduta, enquanto determinadas práticas envolvem diferentes indivíduos e estruturas digitais. Sobrinho e Grott (2022) discutem os sujeitos ativos no cibercrime e a responsabilidade penal do ofensor, evidenciando a importância da correta individualização da autoria. O problema torna-se ainda mais complexo quando as ações ultrapassam fronteiras territoriais e envolvem diferentes jurisdições.

Além da identificação da autoria, a investigação depende frequentemente da obtenção, preservação e análise de provas digitais. Fonseca e Gennarini (2022) destacam que a adesão brasileira à Convenção de Budapeste possui repercussões importantes para a produção dessas provas. Dados armazenados em dispositivos, registros de conexão e outras informações eletrônicas podem ser determinantes para a investigação, mas sua natureza exige procedimentos adequados para garantir integridade, autenticidade e utilização válida no processo penal.

A produção da prova digital ganha complexidade adicional quando os elementos necessários à investigação se encontram armazenados fora do território nacional. Conforme Dias (2025), a cooperação jurídica internacional assume papel relevante na obtenção de evidências relacionadas aos crimes cibernéticos. A estrutura descentralizada da internet dificulta respostas exclusivamente nacionais, pois provedores, servidores, autores e vítimas podem estar situados em diferentes países, tornando necessária a criação de instrumentos capazes de facilitar a colaboração entre autoridades.

No campo da regulamentação da internet, a Lei nº 12.965/2014, conhecida como Marco Civil da Internet, estabeleceu princípios, garantias, direitos e deveres relacionados ao uso da rede no Brasil (Brasil, 2014). Embora não constitua legislação destinada especificamente à tipificação de crimes cibernéticos, o diploma integra o marco jurídico necessário à compreensão das relações digitais. Corrêa e Neto (2023) demonstram que o enfrentamento do cibercrime demanda articulação entre instrumentos nacionais e mecanismos de cooperação internacional.

Essa dimensão internacional ganhou maior relevância com a incorporação da Convenção de Budapeste ao ordenamento brasileiro. A Convenção foi promulgada pelo Decreto nº 11.491/2023 e estabelece mecanismos relacionados à criminalidade cibernética e à cooperação entre os Estados (Brasil, 2023). Segundo Murata e Torres (2023), sua promulgação representa etapa relevante para o enfrentamento dos crimes cibernéticos no país, ao mesmo tempo que suscita discussões sobre os efeitos e adequações decorrentes dos compromissos assumidos pelo Brasil.

Araujo (2022) destaca a importância de compreender a Convenção de Budapeste dentro do campo dos tratados internacionais e das respostas

jurídicas construídas para a criminalidade cibernética. A análise conjunta da literatura e da legislação demonstra que o Brasil avançou na regulamentação das condutas digitais, mas ainda enfrenta desafios relacionados à tipificação, investigação, produção de provas e cooperação internacional. Essas limitações tornam especialmente relevante discutir quem pode responder penalmente pelos delitos, inclusive quando organizações participam ou se beneficiam dessas práticas.

3.2 Responsabilidade penal das pessoas jurídicas e sua aplicação aos crimes cibernéticos

A responsabilidade penal das pessoas jurídicas constitui tema complexo no Direito Penal, especialmente porque seus fundamentos foram historicamente desenvolvidos a partir da conduta individual. A pessoa jurídica possui personalidade própria e capacidade para assumir direitos e obrigações, mas a atribuição de responsabilidade criminal encontra dificuldades relacionadas à identificação de vontade, ação e culpabilidade. Hammerschmidt e David (2023) destacam justamente os desafios de compatibilizar a responsabilidade da pessoa coletiva com o princípio da culpabilidade.

A culpabilidade representa um dos principais pontos de discussão quando se pretende atribuir responsabilidade penal diretamente a organizações. No modelo tradicional, a reprovação penal pressupõe a análise da conduta e das condições do indivíduo que praticou o fato. Segundo Costa e Buzetti (2025), a expansão dos crimes cibernéticos conduz a novos debates sobre a responsabilidade das pessoas jurídicas, especialmente quando estruturas empresariais são empregadas para possibilitar ou favorecer práticas ilícitas realizadas no ambiente digital.

Outro aspecto fundamental envolve o princípio da pessoalidade da pena, previsto constitucionalmente ao determinar que nenhuma pena poderá passar da pessoa do condenado (Brasil, 1988). A individualização da responsabilidade torna-se especialmente relevante diante de organizações compostas por administradores, empregados, representantes e outros agentes. Nesse sentido, Sobrinho e Grott (2022) ressaltam a necessidade de identificação dos sujeitos ativos do cibercrime, evitando que a responsabilização penal seja estabelecida sem a adequada demonstração da participação na conduta investigada.

Apesar dessas dificuldades dogmáticas, o ordenamento jurídico brasileiro admite a responsabilização penal da pessoa jurídica em contexto específico. A Constituição Federal estabelece, no art. 225, § 3º, que condutas e atividades consideradas lesivas ao meio ambiente sujeitam seus infratores, pessoas físicas ou jurídicas, a sanções penais e administrativas, independentemente da obrigação de reparar os danos (Brasil, 1988). Esse dispositivo constitui referência indispensável para compreender os limites atualmente existentes para a imputação penal aos entes coletivos.

No plano infraconstitucional, a Lei nº 9.605/1998 desenvolveu esse modelo ao estabelecer a possibilidade de responsabilização administrativa, civil e penal das pessoas jurídicas em situações relacionadas aos danos ambientais (Brasil, 1998). A existência dessa previsão demonstra que a responsabilidade criminal do ente coletivo não é inteiramente desconhecida pelo sistema brasileiro. Entretanto, sua previsão setorial provoca questionamentos sobre a possibilidade de transportar semelhante lógica para outras modalidades delitivas, entre elas os crimes praticados em ambientes digitais.

A comparação com o regime ambiental evidencia uma questão importante: o reconhecimento da responsabilidade penal das pessoas jurídicas depende de fundamento normativo compatível com os princípios constitucionais e penais. Hammerschmidt e David (2023) observam que a responsabilização da pessoa coletiva exige enfrentar diretamente o princípio da culpabilidade. Nos crimes cibernéticos, entretanto, não existe atualmente uma disciplina geral equivalente àquela estabelecida pela legislação ambiental, circunstância que limita tentativas de ampliar a imputação penal apenas por interpretação.

Essa limitação deve ser compreendida também à luz do princípio da legalidade, elemento estruturante do Direito Penal brasileiro. O Código Penal determina que não há crime sem lei anterior que o defina nem pena sem prévia cominação legal (Brasil, 1940). Assim, a crescente utilização de empresas e organizações no ambiente tecnológico não autoriza automaticamente a criação interpretativa de novas hipóteses de responsabilidade criminal. Silva e Fayão (2025) apontam justamente dificuldades existentes entre novas condutas cibernéticas e sua adequada tipificação penal.

As estruturas empresariais também podem ser utilizadas como instrumentos para obtenção de vantagens decorrentes de práticas digitais ilícitas. Fraudes eletrônicas, apropriação de dados e outras condutas podem envolver diversos agentes e recursos organizacionais. Oliveira e Silva (2026), ao examinarem o phishing e o estelionato eletrônico, demonstram que essas práticas apresentam desafios relevantes para investigação e responsabilização penal. Ainda assim, eventual benefício econômico recebido por uma organização não significa, isoladamente, que esteja configurada sua responsabilidade criminal.

A distinção entre responsabilidade penal e responsabilidade civil é particularmente necessária nesse debate. Uma pessoa jurídica pode estar sujeita a deveres de reparação ou outras consequências jurídicas sem que isso represente automaticamente reconhecimento de responsabilidade criminal. Cruz (2024), ao analisar crimes contra a honra praticados no ambiente virtual, evidencia a importância da esfera civil na reparação dos danos decorrentes das condutas digitais. A responsabilização penal, por sua vez, depende de pressupostos próprios e de previsão normativa específica.

A ausência de regulamentação abrangente produz dificuldades adicionais diante da constante evolução das tecnologias. Simões (2023) identifica deficiências legislativas relacionadas aos crimes cibernéticos, indicando que a velocidade das transformações digitais desafia a capacidade de atualização das normas. Nesse cenário, a responsabilização das pessoas jurídicas revela uma lacuna particularmente sensível, pois a participação de estruturas organizacionais em condutas digitais pode assumir diferentes formas sem que exista, necessariamente, um regime penal específico destinado aos entes coletivos.

Ao mesmo tempo, qualquer tentativa de solucionar essas lacunas mediante expansão indiscriminada do Direito Penal deve ser examinada com cautela. Lima Filho (2021) discute a necessidade de uma expansão razoável da intervenção penal diante dos crimes associados às transformações tecnológicas. Isso significa que a busca por respostas mais efetivas à criminalidade cibernética precisa permanecer compatível com legalidade, culpabilidade e individualização da pena, impedindo que mudanças tecnológicas sejam utilizadas como justificativa suficiente para ampliar automaticamente a punição criminal.

A adesão brasileira à Convenção de Budapeste ampliou especialmente o debate sobre a responsabilização dos entes coletivos. Conforme Murata e Torres (2023), a promulgação da Convenção trouxe novas questões sobre seus efeitos no ordenamento nacional. O Decreto nº 11.491/2023 incorporou o instrumento ao sistema brasileiro e seu art. 12 aborda expressamente a responsabilidade das pessoas jurídicas, admitindo, conforme os princípios jurídicos de cada Parte, que essa responsabilidade possua natureza criminal, civil ou administrativa (Brasil, 2023).

Nesse sentido, a Convenção não deve ser interpretada como criação automática de responsabilidade penal das pessoas jurídicas por todos os crimes cibernéticos praticados no Brasil. Araujo (2022), ao examinar os tratados internacionais e a Convenção de Budapeste, evidencia a necessidade de considerar a relação entre os compromissos internacionais e o ordenamento interno. Corrêa e Neto (2023) igualmente chamam atenção para a tensão existente entre fortalecimento do combate ao cibercrime e possível expansão da intervenção penal.

Diante desse panorama, observa-se que o sistema brasileiro apresenta possibilidades e limites claros para a responsabilização penal dos entes coletivos. A experiência da Lei nº 9.605/1998 demonstra a existência de um modelo penal aplicável às pessoas jurídicas, porém restrito a contexto normativamente delimitado. Costa e Buzetti (2025) apontam novos horizontes para essa discussão nos crimes cibernéticos, tornando necessário avaliar se futuras alterações legislativas poderão preencher lacunas sem comprometer as garantias fundamentais do Direito Penal.

3.3 Convenção de Budapeste e os desafios da responsabilização das pessoas jurídicas por crimes cibernéticos no Brasil

A Convenção de Budapeste constitui um dos principais instrumentos internacionais voltados ao enfrentamento da criminalidade praticada por meio de sistemas informáticos. Sua estrutura busca aproximar legislações nacionais, estabelecer parâmetros para investigação e fortalecer a cooperação entre os Estados diante de delitos que frequentemente ultrapassam fronteiras territoriais. Araujo (2022) destaca sua relevância no contexto dos tratados internacionais, especialmente pela necessidade de respostas coordenadas aos desafios produzidos pela expansão dos crimes cibernéticos.

A importância desse instrumento decorre das próprias características da criminalidade digital, na qual autores, vítimas, servidores e dados podem estar localizados em diferentes países. Coltro e Waldman (2021) ressaltam que a aplicabilidade da Convenção representa questão relevante para o enfrentamento da criminalidade digital brasileira. Nesse sentido, sua contribuição não se restringe à definição de condutas ilícitas, alcançando mecanismos destinados à investigação, obtenção de informações e cooperação entre autoridades de diferentes jurisdições.

No Brasil, o processo de incorporação da Convenção passou inicialmente pela aprovação de seu texto pelo Congresso Nacional, formalizada pelo Decreto Legislativo nº 37/2021 (Brasil, 2021). Posteriormente, o Decreto nº 11.491/2023 promulgou a Convenção sobre o Crime Cibernético no ordenamento brasileiro (Brasil, 2023). Murata e Torres (2023) observam que essa promulgação inaugurou importantes discussões acerca dos efeitos concretos do instrumento internacional e das adaptações necessárias para sua aplicação no cenário jurídico nacional.

Entre as disposições especialmente relevantes para esta pesquisa encontra-se o art. 12 da Convenção, que disciplina a responsabilidade das pessoas jurídicas. O dispositivo estabelece parâmetros para que os Estados adotem medidas destinadas à responsabilização dos entes coletivos em determinadas circunstâncias relacionadas às infrações previstas no instrumento (Brasil, 2023). Para Costa e Buzetti (2025), essa matéria abre novos horizontes para discutir a responsabilidade penal das pessoas jurídicas diante do crescimento e da complexidade dos crimes cibernéticos.

Um aspecto decisivo é que a Convenção não determina obrigatoriamente a adoção de responsabilidade exclusivamente penal. Conforme estabelece o próprio art. 12, a responsabilidade da pessoa jurídica poderá ser criminal, civil ou administrativa, de acordo com os princípios jurídicos de cada Parte (Brasil, 2023). Essa previsão é particularmente relevante para o Brasil, pois Hammerschmidt e David (2023) demonstram que a responsabilização criminal da pessoa coletiva envolve dificuldades relacionadas à culpabilidade e aos fundamentos tradicionais da imputação penal.

A análise da compatibilidade com o sistema brasileiro exige considerar que a Constituição Federal admite expressamente sanções aplicáveis às pessoas jurídicas no campo ambiental (Brasil, 1988). Essa previsão foi desenvolvida pela Lei nº 9.605/1998, que estabelece responsabilidade administrativa, civil e penal das pessoas jurídicas em determinadas circunstâncias relacionadas às infrações ambientais (Brasil, 1998). Entretanto, não existe disciplina geral equivalente que estabeleça, de maneira expressa, responsabilidade penal dos entes coletivos especificamente pela prática de crimes cibernéticos.

Essa diferença normativa impede que o modelo existente para os crimes ambientais seja automaticamente transferido para os delitos cibernéticos. O princípio da legalidade exige previsão anterior da conduta criminosa e da respectiva sanção (Brasil, 1940), impondo limites à ampliação interpretativa da responsabilidade penal. Sobrinho e Grott (2022) reforçam a importância da correta atribuição da responsabilidade ao sujeito ativo, aspecto que assume maior complexidade quando dirigentes, funcionários e estruturas organizacionais participam de uma mesma dinâmica criminosa.

Embora as Leis nº 12.735/2012 e nº 12.737/2012 tenham representado avanços no tratamento legislativo das condutas relacionadas aos sistemas informáticos, elas não instituíram um regime abrangente de responsabilidade penal das pessoas jurídicas por crimes cibernéticos (Brasil, 2012a, 2012b). Nóbrega (2022) observa que a legislação penal brasileira precisa ser analisada diante das exigências trazidas pela criminalidade digital, enquanto Simões (2023) identifica deficiências normativas que dificultam respostas plenamente adequadas às novas modalidades de delitos tecnológicos.

O Marco Civil da Internet também integra esse cenário ao estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil (Brasil, 2014). Contudo, suas disposições não equivalem à criação de responsabilidade criminal geral das empresas por delitos praticados no ambiente virtual. Cruz (2024) contribui para compreender essa diferenciação ao abordar a responsabilidade civil decorrente de ilícitos digitais, demonstrando que consequências reparatórias e patrimoniais não podem ser confundidas com a imputação penal, submetida a requisitos próprios.

Nesse contexto, a adesão à Convenção de Budapeste não pode ser compreendida como autorização automática para ampliar a responsabilidade penal das pessoas jurídicas no Brasil. Corrêa e Neto (2023) chamam atenção para a relação entre cooperação internacional e expansão do Direito Penal no enfrentamento ao cibercrime. Da mesma forma, Lima Filho (2021) sustenta a necessidade de avaliar cuidadosamente a expansão da intervenção penal diante das transformações tecnológicas, preservando os limites e garantias próprios desse ramo jurídico.

A principal lacuna identificada encontra-se, portanto, na inexistência de disciplina específica e suficientemente clara para a responsabilização penal direta das pessoas jurídicas por crimes cibernéticos. Silva e Fayão (2025) destacam dificuldades relacionadas à tipificação e à efetivação das medidas legais de combate, enquanto Costa e Buzetti (2025) apontam a necessidade de aprofundar o debate sobre a responsabilidade dos entes coletivos. Eventual aperfeiçoamento legislativo deverá estabelecer critérios objetivos de imputação, evitando responsabilizações automáticas decorrentes exclusivamente da atuação de seus integrantes.

O ordenamento brasileiro dispõe de instrumentos para combater diferentes modalidades de crimes cibernéticos e passou a integrar formalmente o sistema de cooperação previsto pela Convenção de Budapeste, mas isso não significa que tenha sido instituído um regime geral de responsabilidade penal das pessoas jurídicas nesse campo. A literatura analisada indica que o aperfeiçoamento normativo permanece necessário, devendo conciliar efetividade no enfrentamento ao cibercrime com legalidade, culpabilidade, individualização da responsabilidade e demais garantias fundamentais.

CONSIDERAÇÕES FINAIS

A presente pesquisa buscou responder em que medida o ordenamento jurídico brasileiro permite a responsabilização penal das pessoas jurídicas por crimes cibernéticos diante das disposições da Convenção de Budapeste. A partir da análise realizada, verificou-se que o sistema jurídico nacional ainda apresenta limitações para a imputação penal direta às pessoas jurídicas nessa modalidade de criminalidade. Embora o Brasil reconheça a responsabilidade penal dos entes coletivos em situações expressamente previstas, especialmente na esfera ambiental, não existe atualmente um regime geral e específico que permita estender automaticamente essa responsabilização aos crimes cibernéticos.

Em relação aos objetivos específicos, foi possível compreender que os crimes cibernéticos apresentam características próprias, como transnacionalidade, rapidez de execução, dificuldades de identificação dos agentes e complexidade na obtenção e preservação das provas digitais. Verificou-se ainda que a legislação brasileira avançou na tipificação e no tratamento de determinadas condutas praticadas no ambiente virtual, mas permanece diante do desafio de acompanhar a velocidade das transformações tecnológicas.

Também foi possível examinar os fundamentos e limites da responsabilidade penal das pessoas jurídicas, identificando que princípios como legalidade, culpabilidade, pessoalidade da pena e individualização da responsabilidade precisam ser observados em qualquer proposta destinada a ampliar a imputação criminal aos entes coletivos.

A análise das disposições da Convenção de Budapeste permitiu alcançar o objetivo de compreender sua relação com o ordenamento

jurídico brasileiro e identificar os principais desafios relacionados à responsabilidade das pessoas jurídicas. Constatou-se que a adesão brasileira representa importante avanço para o enfrentamento dos crimes cibernéticos, especialmente ao favorecer a harmonização normativa e a cooperação internacional.

Entretanto, a Convenção não determina necessariamente que a responsabilidade atribuída às pessoas jurídicas seja de natureza penal, admitindo respostas nas esferas criminal, civil ou administrativa. Dessa maneira, confirmou-se a hipótese de que sua incorporação não é suficiente para criar, isoladamente, novas hipóteses de responsabilidade criminal, sendo necessária previsão normativa compatível com os fundamentos constitucionais e penais brasileiros.

Diante dos resultados obtidos, considera-se que o objetivo geral da pesquisa foi alcançado, pois foi possível analisar as possibilidades e os limites da responsabilização penal das pessoas jurídicas por crimes cibernéticos no Brasil à luz da Convenção de Budapeste. Como limitação do estudo, destaca-se seu caráter exclusivamente bibliográfico e documental, baseado na produção científica recente e nos principais documentos normativos relacionados ao tema.

Além disso, trata-se de matéria ainda em desenvolvimento no cenário jurídico brasileiro, marcada por mudanças tecnológicas constantes e por debates doutrinários que permanecem abertos, o que impede a formulação de respostas definitivas sobre todas as situações em que organizações possam estar relacionadas à prática de delitos cibernéticos.

Recomenda-se que pesquisas futuras aprofundem a discussão sobre modelos de imputação aplicáveis às pessoas jurídicas no ambiente digital,

investigando critérios capazes de diferenciar a atuação individual de dirigentes e empregados daquela efetivamente vinculada à estrutura e aos interesses da organização. Também se mostra pertinente analisar experiências legislativas estrangeiras adotadas após a Convenção de Budapeste e sua possível contribuição para o sistema brasileiro.

REFERÊNCIAS

ARAUJO, Clayton Vinicius Pegoraro. Os aspectos gerais dos tratados internacionais e a Convenção de Budapeste sobre Crimes Cibernéticos. *Revista da Faculdade de Direito da Universidade Federal de Uberlândia, Uberlândia*, v. 50, n. 1, p. 145-165, 2022.

BRASIL. Congresso Nacional. Decreto Legislativo nº 37, de 2021. Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001. Brasília, DF: Congresso Nacional, 2021. Disponível em: Decreto Legislativo nº 37/2021. Acesso em: 12 ago. 2026.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988. Disponível em: Constituição Federal de 1988. Acesso em: 12 ago. 2026.

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. Brasília, DF: Presidência da República, 2023. Disponível em: Decreto nº 11.491/2023. Acesso em: 12 ago. 2026.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Brasília, DF: Presidência da República, 1940. Disponível em: Código Penal. Acesso em: 12 ago. 2026.

BRASIL. Lei nº 12.735, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 – Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Brasília, DF: Presidência da República, 2012. Disponível em: Lei nº 12.735/2012. Acesso em: 12 ago. 2026.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Brasília, DF: Presidência da República, 2012. Disponível em: Lei nº 12.737/2012. Acesso em: 12 ago. 2026.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: Marco Civil da Internet – Lei nº 12.965/2014. Acesso em: 12 ago. 2026.

BRASIL. Lei nº 9.605, de 12 de fevereiro de 1998. Dispõe sobre as sanções penais e administrativas derivadas de condutas e atividades lesivas ao meio ambiente, e dá outras providências. Brasília, DF: Presidência da República, 1998. Disponível em: Lei nº 9.605/1998. Acesso em: 12 ago. 2026.

COLTRO, Rafael Khalil; WALDMAN, Ricardo Libel. Criminalidade digital no Brasil: a problemática e a aplicabilidade da convenção de Budapeste. *Revista Em Tempo*, v. 21, n. 1, p. 104-123, 2021.

CORRÊA, Isadora Donza; NETO, João Araújo Monteiro. A adesão do Brasil à Convenção de Budapeste e o enfrentamento do Cibercrime:: entre a

Cooperação Internacional e a expansão do Direito Penal. *Direito & TI*, v. 1, n. 16, p. 32-60, 2023.

COSTA, Rafael; BUZETTI, Bruno Starcke. Novos horizontes na responsabilidade penal das pessoas jurídicas pela prática de crimes cibernéticos. *Revista Jurídica da Escola Superior do Ministério Público de São Paulo*, v. 26, p. 125-154, 2025.

CRUZ, Nicole Nathane Feitosa. A responsabilidade civil nos crimes contra a honra praticados no ambiente virtual. *Repositório Institucional do Unifip*, v. 9, n. 1, 2024.

DIAS, Bruna Mariana Coutinho. A cooperação jurídica internacional e a produção da prova digital: uma análise das ferramentas previstas na Convenção de Budapeste. *Portal de Trabalhos Acadêmicos*, v. 18, n. 1, 2025.

FONSECA, Marcos De Lucca; GENNARINI, Juliana Caramigo. A Adesão do Brasil à Convenção de Budapeste e os Impactos para a Produção de Provas Digitais. *Direito Penal e Processo Penal*, v. 4, n. 1, p. 55-70, 2022.

GIL, Antonio Carlos. Métodos e técnicas de pesquisa social. 7. ed. São Paulo: Atlas, 2019.

HAMMERSCHMIDT, Karina Silveira; DAVID, Décio Franco. Responsabilidade Penal da Pessoa Coletiva e o Princípio da Culpabilidade nos Crimes Informáticos em Redes Sociais. *Caderno Paic*, 2023.

LIMA FILHO, Paulo Roberto Aguiar. O direito penal na quarta revolução industrial: a expansão razoável frente aos crimes cibernéticos. *Delictae Revista de Estudos Interdisciplinares sobre o Delito*, v. 6, n. 10, 2021.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. Fundamentos de metodologia científica. 9. ed. São Paulo: Atlas, 2021.

MURATA, Ana Maria Lumi Kamimura; TORRES, Me Paula Ritzmann. A convenção de Budapeste sobre os crimes cibernéticos foi promulgada, e agora?. Boletim IBCCRIM, v. 31, n. 368, p. 13-16, 2023.

NÓBREGA, Juliana Medeiros. Os crimes cibernéticos e a legislação penal brasileira: um estudo a partir da convenção de Budapeste. Repositório Institucional do Unifip, v. 7, n. 1, 2022.

OLIVEIRA, Rafaela Louise de Souza Silva; SILVA, Rosana Reis. Phishing e estelionato eletrônico: desafios da investigação e da responsabilidade penal após a lei 14.155/2021. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 12, n. 6, p. 1-21, 2026.

SILVA, Alcides Belfort; FAYÃO, Vincenzo de Campos Agonilha. Crimes cibernéticos: a tipificação penal e os desafios na efetivação das medidas legais de combate. Transições, v. 6, n. 2, p. 145-175, 2025.

SIMÕES, Caroline Amorim. As deficiências legislativas quanto aos crimes cibernéticos. Repositório Institucional do Unifip, v. 8, n. 1, 2023.

SOBRINHO, Jéssica Rafaela; GROTT, Sergio. Os sujeitos ativos no cibercrime e a responsabilidade penal do ofensor. Revista Científica Multidisciplinar do CEAP, v. 4, n. 2, 2022.

Recebido em: 19 de agosto de 2026.

Aprovado em: 3 de setembro de 2026.