AFYA CENTRO UNIVERSITÁRIO

BACHARELADO EM DIREITO

DIÊGO RICARDO BATISTA

EXTORSÃO DIGITAL POR MEIO DE RANSOMWARE: UMA ANÁLISE JURÍDICA DA RESPONSABILIZAÇÃO PENAL FRENTE AOS DESAFIOS À INVESTIGAÇÃO CIBERNÉTICA

BARREIRAS-BA

2026

DIÊGO RICARDO BATISTA

EXTORSÃO DIGITAL POR MEIO DE RANSOMWARE: UMA ANÁLISE JURÍDICA DA RESPONSABILIZAÇÃO PENAL FRENTE AOS DESAFIOS À INVESTIGAÇÃO CIBERNÉTICA

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da AFYA Centro Universitário, como requisito parcial para obtenção do título de Bacharel em Direito.

Orientador Prof. Me. Fábio Pereira de Souza.

BARREIRAS-BA

2026

AGRADECIMENTOS

A realização deste trabalho foi possível graças ao apoio e à contribuição de diversas pessoas e instituições, às quais registro meus sinceros agradecimentos.

Primeiramente, a Deus, pela saúde, discernimento e força necessários para a condução desta pesquisa.

À minha família, em especial aos meus pais e irmãos e a minha filha, pelo amor incondicional, pelo incentivo constante e pelo sacrifício dedicado à minha formação acadêmica. A eles devo a base que me sustenta em todos os projetos de vida.

Ao professor orientador, pela paciência, pela disponibilidade e pelas valiosas orientações que foram essenciais para o amadurecimento deste estudo e para o meu desenvolvimento intelectual.

À AFYA Centro Universitário, pelo ambiente propício ao aprendizado e pela oportunidade de aprofundamento acadêmico proporcionada ao longo do curso.

Aos colegas de turma e amigos, pelas trocas de ideias, pelo companheirismo e pelos momentos de descontração que aliviaram as etapas mais intensas desta jornada.

Por fim, a todos os autores e pesquisadores cujas obras fundamentaram este trabalho, contribuindo para a qualidade e a robustez das análises aqui apresentadas.

A todos, o meu eterno reconhecimento.

“A segurança não é um produto, mas um processo — e, no mundo digital, a lei deve correr tão rápido quanto a tecnologia que regula.”
(**BRUCE SCHNEIER**)

DIÊGO RICARDO BATISTA

EXTORSÃO DIGITAL POR MEIO DE RANSOMWARE: UMA ANÁLISE JURÍDICA DA RESPONSABILIZAÇÃO PENAL FRENTE AOS DESAFIOS À INVESTIGAÇÃO CIBERNÉTICA

Trabalho para conclusão do curso de Bacharelado em Direito da AFYA Centro Universitário – Barreiras-BA, como requisito para conclusão de graduação.

Barreiras-BA, 16 de Junho de 2026

BANCA EXAMINADORA

gov.br Documento assinado digitalmente
FABIO PEREIRA DE SOUZA
Data: 27/06/2026 15:59:21 -0300
Verifique em https://validar.iti.gov.br

Professor Orientador
Prof. Me. Fábio Pereira de Souza.

gov.br Documento assinado digitalmente
SUZANA WONG DOS SANTOS
Data: 27/06/2026 15:21:05 -0300
Verifique em https://validar.iti.gov.br

Membro da Banca 1
Prof. Me Suzana Wong dos Santos

gov.br Documento assinado digitalmente
MATEUS DE CAMPOS BALDIN
Data: 27/06/2026 11:22:31 -0300
Verifique em https://validar.iti.gov.br

Membro da Banca 2
Prof. Me Mateus de Campos Baldin

B333e Batista, Diêgo Ricardo

Extorsão digital por meio de Ransomware: uma análise jurídica da responsabilização penal frente aos desafios à investigação cibernética. / Diêgo Ricardo Batista -- Barreiras, 2026.
24 p.

Trabalho de Conclusão de Curso (Graduação – Curso de Direito) AFYA Centro Universitário – Barreiras/BA.
Orientador (a): Prof. Me. Fábio Pereira de Souza.

1. Direito penal. 2. Ransomware. 3. Extorsão digital. I. Souza, Fábio Pereira de II. Título.

CDU 343
CDD 345

Ficha catalográfica elaborada pelo Bibliotecário
Ednilson M. Brito Filho – CRB 5/1743

EXTORSÃO DIGITAL POR MEIO DE RANSOMWARE: UMA ANÁLISE JURÍDICA DA RESPONSABILIZAÇÃO PENAL FRENTE AOS DESAFIOS À INVESTIGAÇÃO CIBERNÉTICA

Diêgo Ricardo Batista[1]
Fábio Pereira de Souza[2]

RESUMO

Diante da complexidade técnica e da natureza transnacional dos ataques de ransomware, a aplicação do Direito Penal tradicional e a efetividade da persecução criminal no Brasil são postas à prova. A dificuldade em rastrear os agentes criminosos, a volatilidade das provas digitais e a necessidade de cooperação internacional impõem barreiras significativas. O presente trabalho busca responder à questão norteadora: qual a eficácia da legislação penal brasileira na responsabilização dos agentes de extorsão digital por ransomware e quais os principais desafios jurídicos e operacionais enfrentados pela investigação cibernética para a concretização dessa responsabilização? O objetivo geral consiste em analisar o regime jurídico da responsabilização penal nesses casos, com foco nos desafios impostos à investigação cibernética. Os objetivos específicos incluem conceituar o fenômeno do ransomware e mapear sua subsunção aos artigos 158 (extorsão) e 154-A (invasão de dispositivo informático) do Código Penal; identificar e discutir os principais obstáculos técnicos, jurídicos e de jurisdição que dificultam a investigação e a coleta de provas; e avaliar a adequação e a suficiência da legislação brasileira, incluindo o Marco Civil da Internet e a Lei Carolina Dieckmann, para o combate eficaz a essa modalidade criminosa. A metodologia adotada é qualitativa, mediante pesquisa bibliográfica e documental, com abordagem dedutiva. Como principais conclusões, identificam-se lacunas legislativas e operacionais, propondo-se caminhos para aprimorar a responsabilização penal e a investigação cibernética no contexto do ransomware.

Palavras-chave: Ransomware. Extorsão digital. Direito penal. Investigação cibernética. Criptomoedas.

ABSTRACT

Given the technical complexity and transnational nature of ransomware attacks, the application of traditional Criminal Law and the effectiveness of criminal prosecution in Brazil are put to the test. The difficulty in tracking criminal agents, the volatility of digital evidence, and the need for international cooperation impose significant barriers. This course completion paper seeks to answer the guiding question: what is the effectiveness of Brazilian criminal legislation in holding agents of digital extortion by ransomware accountable, and what are the main legal and operational challenges faced by cyber investigations in achieving this accountability? The general objective is to analyze the legal framework for criminal accountability in cases of digital

---

[1] Discente do curso de Direito da AFYA Centro Universitário – Barreiras-BA.
[2] Mestre em Propriedade Intelectual e Transferência de Tecnologia para Inovação, graduação em Direito, graduação em Matemática. Pós-graduado em Finanças Corporativa, Gestão de Pessoas, Ciências Criminais e Direito. Atualmente é professor da AFYA e Universidade Maurício de Nassau (UNINASSAU), Barreiras-BA, Advogado.

extortion by ransomware in Brazil, focusing on the challenges imposed on cyber investigations. Specific objectives include mapping the ransomware phenomenon and its subsumption under Articles 158 (extortion) and 154-A (invasion of computer device) of the Criminal Code; identifying and discussing the main technical, legal, and jurisdictional obstacles that hinder the investigation and collection of evidence in ransomware crimes; and evaluating the adequacy and sufficiency of Brazilian criminal and criminal procedural legislation, including the Internet Civil Framework and the Carolina Dieckmann Law, for the effective combat against this criminal modality. The adopted methodology is qualitative, through bibliographic and documentary research, with a deductive approach. The main conclusions are expected to identify legislative and operational gaps, proposing ways to improve criminal accountability and cyber investigations in the context of ransomware.

Keywords: Ransomware. Digital extortion. Criminal law. Cyber investigation. Cryptocurrencies.

SUMÁRIO

1 INTRODUÇÃO

A sociedade contemporânea testemunha uma acelerada transformação digital, na qual a dependência de sistemas e redes de computadores tornou-se onipresente, permeando desde as relações pessoais até as infraestruturas críticas estatais e corporativas. Paralelamente a essa evolução tecnológica, observa-se o surgimento e a sofisticação de novas modalidades criminosas que exploram as vulnerabilidades desse ambiente digital. Dentre elas, a extorsão digital por meio de *ransomware* emerge como um dos fenômenos mais disruptivos da cibercriminalidade global.

No contexto brasileiro, a prática se enquadra majoritariamente no tipo penal de extorsão (Art. 158 do Código Penal (CP)), podendo também configurar o crime de invasão de dispositivo informático (Art. 154-A do CP), a depender da dinâmica do ataque. A extorsão digital por meio de *ransomware* representa uma das ameaças cibernéticas mais complexas e atuais na era da informação. Diante do crescimento exponencial desses ataques, surge a necessidade de analisar, do ponto de vista jurídico, os mecanismos de responsabilização penal aplicáveis aos autores desse delito.

O avanço tecnológico tem proporcionado inúmeros benefícios à sociedade, mas também tem sido explorado para práticas ilícitas, como o uso de *ransomware* para fins de extorsão digital. Os ataques comprometem a integridade de dados e sistemas, afetando tanto pessoas físicas quanto jurídicas, inclusive órgãos públicos, colocando em risco informações sensíveis e a segurança digital. No contexto jurídico, verifica-se um descompasso entre a evolução tecnológica e o ordenamento jurídico penal brasileiro, que ainda não dispõe de legislação suficientemente específica para tratar de crimes cibernéticos complexos. Ademais, a atuação investigativa enfrenta limitações técnicas, legais e estruturais, especialmente quando os autores dos ataques operam fora do território nacional.

A relevância deste estudo se manifesta em três esferas. Do ponto de vista social, a análise contribui para a conscientização sobre os riscos inerentes à sociedade da informação e a necessidade de um arcabouço legal robusto. Na esfera jurídica, o tema é de vanguarda, exigindo uma interpretação evolutiva dos tipos penais existentes e o debate sobre a necessidade de novas tipificações específicas para o sequestro digital. Sob a ótica acadêmica, a pesquisa preenche uma lacuna ao

sistematizar a discussão sobre a aplicação da teoria do crime aos ataques de *ransomware* e ao mapear as dificuldades práticas da investigação, oferecendo subsídios para futuros estudos e para a atuação de profissionais do Direito.

Diante da complexidade técnica dos ataques de ransomware e da natureza transnacional de muitos desses crimes, a aplicação do Direito Penal tradicional e a efetividade da persecução criminal são postas à prova. A dificuldade em rastrear os agentes criminosos, a volatilidade das provas digitais e a necessidade de cooperação internacional impõem barreiras significativas.

Nesse cenário, o presente trabalho busca responder à seguinte questão norteadora: qual a eficácia da legislação penal brasileira na responsabilização dos agentes de extorsão digital por *ransomware* e quais os principais desafios jurídicos e operacionais enfrentados pela investigação cibernética para a concretização dessa responsabilização?

O objetivo geral consiste em analisar o regime jurídico da responsabilização penal nos casos de extorsão digital por *ransomware* no Brasil, com foco nos desafios impostos à investigação cibernética. Os objetivos específicos compreendem conceituar o fenômeno do *ransomware* e mapear sua subsunção aos tipos penais de extorsão (Art. 158, CP) e invasão de dispositivo informático (Art. 154-A, CP); identificar e discutir os principais obstáculos técnicos, jurídicos e de jurisdição que dificultam a investigação e a coleta de provas; e avaliar a adequação e a suficiência da legislação penal e processual penal brasileira, incluindo o Marco Civil da Internet e a Lei Carolina Dieckmann, para o combate eficaz a essa modalidade criminosa.

No que se refere à configuração metodológica, a presente investigação assume, de maneira preponderante, um caráter qualitativo. Tal escolha paradigmática afasta-se deliberadamente da pretensão de quantificar dados estatísticos ou de estabelecer correlações numéricas, direcionando-se, em contrapartida, para a hermenêutica jurídica e para o exame analítico e interpretativo de construções conceituais, preceitos normativos, entendimentos doutrinários consolidados e orientações jurisprudenciais firmadas. O intento central reside em captar a multidimensionalidade e a complexidade intrínseca ao fenômeno do ransomware, observando-o sob a perspectiva crítica do Direito Penal e do Direito Processual Penal, com o fito de aferir a adequação teleológica e a eficácia normativa do ordenamento jurídico pátrio diante de tal desafio contemporâneo (Gil, 2022).

Nesse viés interpretativo, o esforço investigativo concentra-se na desconstrução e na recomposição dos fundamentos que estruturam a resposta estatal aos crimes cibernéticos, priorizando a análise qualitativa em detrimento de mensurações puramente aritméticas. Busca-se, portanto, penetrar nas camadas de significado que permeiam a aplicação da lei penal aos delitos de extorsão digital, examinando como os conceitos dogmáticos se articulam com as normas vigentes e como a jurisprudência tem moldado a concretização da justiça em cenários de alta volatilidade tecnológica. Dessa forma, a pesquisa visa não apenas descrever o quadro normativo, mas compreender como o sistema jurídico brasileiro internaliza, adapta e responde às nuances processuais e materiais impostas pela criminalidade virtual, avaliando criticamente se o arcabouço legal atual se mostra suficientemente robusto e operacional para garantir a tutela dos bens jurídicos penalmente relevantes.

A opção por uma abordagem qualitativa encontra sua fundamentação teórica na imperiosa necessidade de examinar a essência jurídica e as ramificações dogmáticas do fenômeno em estudo, privilegiando a apreensão dos significados, das relações de causa e efeito normativas e das consequências institucionais decorrentes da responsabilização penal por condutas de extorsão no ambiente digital. Conforme magistralmente pontuado por Severino (2007), a investigação de natureza qualitativa opera por meio de um processo contínuo de compreensão, interpretação e tratamento de informações que visam revelar a natureza profunda do objeto analisado, constituindo-se, desse modo, em instrumento metodológico particularmente propício ao universo das Ciências Jurídicas. Isso se deve ao fato de que os fenômenos sociais e legais, especialmente aqueles vinculados à inovação tecnológica e à dinâmica penal, não se submetem adequadamente a mensurações quantitativas diretas, exigindo, antes, um olhar sensível às nuances contextuais e às construções hermenêuticas que dão sentido à norma.

No plano procedimental, o desenvolvimento do estudo pautou-se na conjugação de técnicas de pesquisa bibliográfica e documental, sendo a primeira erigida como o alicerce estrutural de toda a investigação. A pesquisa bibliográfica materializou-se por meio do levantamento sistemático, da triagem criteriosa e da análise reflexiva de corpus teórico já publicado e consolidado, abarcando monografias, dissertações, teses acadêmicas, artigos científicos indexados e obras doutrinárias de reconhecido prestígio. A seleção do material bibliográfico obedeceu a

critérios rigorosos de pertinência temática, atualização cronológica e autoridade intelectual, com foco especial nas subáreas do Direito Penal, do Direito Processual Penal, do Direito Digital e da disciplina dedicada ao Cibercrime, garantindo, assim, uma base teórica sólida e atualizada para o desenvolvimento dos argumentos propostos (Marconi; Lakatos, 2023).

Paralelamente, a pesquisa documental foi empregada como estratégia complementar para o acesso e a exegese de fontes primárias e secundárias de natureza normativa e institucional. Tal procedimento envolveu o exame minucioso do texto da Constituição Federal, do Código Penal, do Código de Processo Penal, bem como da legislação específica que regula o ambiente digital e a proteção de dados, notadamente a Lei nº 12.737/2012, a Lei nº 12.965/2014 e a Lei nº 13.709/2018. Somaram-se a esse acervo normativo as decisões proferidas pelos Tribunais Superiores, que orientam a aplicação concreta do direito, e os relatórios técnicos emitidos por órgãos de segurança pública nacionais e por organizações internacionais dedicadas ao combate ao crime cibernético, constituindo um panorama documental robusto e fidedigno para a análise empírica e normativa do tema (Brasil, 1940; Brasil, 2012; Brasil, 2014).

O método de abordagem empregado foi o dedutivo. Partindo de premissas gerais e universais (a teoria do crime, os princípios do Direito Penal e a legislação brasileira), o estudo se direcionou para a análise de um caso particular e específico (a extorsão digital por *ransomware*). O objetivo foi verificar se e como as normas e os conceitos jurídicos estabelecidos se aplicam de forma eficaz ao fenômeno da cibercriminalidade, permitindo a conclusão sobre a adequação do sistema penal (Demo, 2024). Conforme explica o IDP (2024), o método dedutivo percorre o caminho do geral para o particular, partindo de argumentos que se consideram verdadeiros para, utilizando essa premissa lógica, chegar a conclusões formais que se busca.

As técnicas de pesquisa utilizadas foram a análise de conteúdo e o fichamento, aplicadas para interpretar o material bibliográfico e documental, buscando identificar as categorias centrais de análise e as convergências e divergências entre os autores e as decisões judiciais (Bardin, 2016). A análise de conteúdo, conforme Bardin (2016), divide-se em abordagem quantitativa e qualitativa. Na abordagem qualitativa, focalizam-se elementos que, embora não sejam frequentes, estimulam a inferência, sendo relevante particularmente na

elaboração das deduções específicas sobre um acontecimento ou uma variável de inferência precisa.

O fichamento foi utilizado para organizar e sistematizar as informações coletadas, facilitando a citação correta das fontes e a construção lógica dos argumentos ao longo dos capítulos. A combinação desses métodos e técnicas visa garantir a profundidade, a validade e a confiabilidade das conclusões a serem apresentadas no trabalho.

No tocante aos aspectos éticos, a pesquisa observou os princípios de confidencialidade e responsabilidade ao discutir técnicas de ataque. A Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018), embora permita o tratamento de dados para fins acadêmicos, impõe a observância de princípios como a segurança, a prevenção e a não discriminação. O pesquisador adotou medidas de anonimização dos dados sempre que possível, transformando-os de forma que não fosse possível identificar o titular, direta ou indiretamente. Ademais, ao discutir técnicas de ataque cibernético, o estudo manteve o foco na compreensão das vulnerabilidades e na proposição de medidas de defesa e prevenção, evitando a divulgação de detalhes técnicos excessivos que pudessem ser mal utilizados, em conformidade com os artigos 154-A, 286 e 287 do Código Penal.

2 FUNDAMENTAÇÃO TEÓRICA

A compreensão da extorsão digital por meio de *ransomware* exige, preliminarmente, a análise de seus contornos técnicos e de sua trajetória evolutiva no âmbito da criminalidade informática contemporânea. Etimologicamente, o termo advém da aglutinação dos vocábulos ingleses *ransom* (resgate) e software (programa), designando uma espécie de *malware* especificamente desenvolvido para restringir o acesso a sistemas ou dados críticos. Conforme lecionam Wendt e Jorge (2022), o *ransomware* opera essencialmente através da criptografia de arquivos, transformando a informação em um ativo inacessível para o proprietário legítimo. A liberação desses dados é condicionada ao pagamento de um resgate, geralmente exigido em *criptoativos*, o que dificulta o rastreamento pelas autoridades e consolida a natureza extorsiva da conduta no ambiente digital.

O fenômeno do *ransomware* não pode ser compreendido de forma isolada do contexto mais amplo da cibercriminalidade global. Nos últimos anos, observa-se uma escalada sem precedentes na frequência e na sofisticação dos ataques. Segundo dados divulgados pela ISH Tecnologia em 2026, os ataques de *ransomware* cresceram 17,8% no mundo em 2025, na comparação com o ano anterior, totalizando 7.410 empresas alvo de grupos especializados nesse tipo de ataque. O Brasil aparece como o nono país mais afetado globalmente e o primeiro na América Latina, posicionando-se como alvo prioritário dos cibercriminosos. Conforme apontado por Fabio Assolini, diretor da Equipe Global de Pesquisa e Análise da *Kaspersky* para a América Latina, os cibercriminosos tendem a priorizar ataques em países que contam com legislações que responsabilizam legalmente as empresas pela proteção de dados, tornando as companhias alvos mais atraentes, já que estão mais pressionadas a resolver rapidamente incidentes para evitar sanções (Security Leaders, 2025).

Ainda no que tange ao cenário brasileiro, a *Kaspersky* registrou um crescimento de 12% nos ataques de *ransomware* no Brasil em comparação com o ano anterior, com 549 mil tentativas bloqueadas nos últimos 12 meses, o equivalente a 1.664 por dia. Entre agosto de 2024 e junho de 2025, o Brasil liderou esse tipo de ataque na América Latina, concentrando metade dos ataques da região (Security Leaders, 2025). Esses números evidenciam a urgência de uma resposta jurídica robusta e atualizada.

2.1 O FENÔMENO DO RANSOMWARE: ASPECTOS TÉCNICOS E EVOLUÇÃO

Tecnicamente, o *ransomware* opera por meio de um mecanismo de criptografia que torna os arquivos da vítima inacessíveis sem a chave de decriptação. A criptografia pode ser assimétrica ou simétrica, ou ainda uma combinação híbrida dessas duas modalidades. Na criptografia simétrica, utiliza-se uma única chave tanto para criptografar quanto para descriptografar os dados. Essa abordagem, embora rápida, apresenta a vulnerabilidade de que a chave pode ser encontrada no sistema local por especialistas em segurança, permitindo a recuperação dos dados sem o pagamento do resgate. Para contornar essa limitação, os ataques mais recentes empregam predominantemente a criptografia assimétrica, que utiliza um par de chaves: uma pública, para criptografar, e uma

privada, para descriptografar. A chave privada é armazenada no servidor do atacante e somente liberada mediante o pagamento do resgate (Trend Micro, 2025).

A evolução técnica dos *ransomwares* modernos incorporou ainda a criptografia híbrida, que combina a velocidade da criptografia simétrica com a segurança da assimétrica. Nesse modelo, os arquivos da vítima são primeiro criptografados com uma chave simétrica gerada localmente; em seguida, essa chave simétrica é criptografada com a chave pública do atacante. Somente a chave privada correspondente, mantida sob o controle do criminoso, pode descriptografar a chave simétrica, que por sua vez permite a recuperação dos dados. Essa arquitetura torna praticamente impossível a recuperação dos arquivos sem a cooperação do atacante (Trend Micro, 2025).

O ataque geralmente se inicia com a invasão de dispositivo informático, prevista no Art. 154-A do Código Penal, por meio de *phishing*, exploração de vulnerabilidades de software ou acesso remoto não autorizado. A sofisticação atual dos ataques transcendeu a mera criptografia de dados, evoluindo para modelos de negócio criminoso altamente organizados, conforme relatado por Crespo (2021).

Duas tendências merecem destaque na evolução do cibercrime. Primeiramente, o modelo *Ransomware-as-a-Service* (RaaS), que permite que criminosos com pouca habilidade técnica lancem ataques. Desenvolvedores de *ransomware* vendem ou alugam seu *malware* e infraestrutura para afiliados, que executam os ataques e dividem o lucro com os desenvolvedores, conforme descrito por IBM (2025). Em segundo lugar, a tática de *Double Extortion* (dupla extorsão), que surgiu como resposta à crescente adoção de backups pelas vítimas. Além de criptografar os dados, os criminosos *exfiltram* informações sensíveis. A ameaça passa a ser dupla: o não pagamento resulta tanto na inacessibilidade dos dados quanto na sua publicação em sites de vazamento, expondo segredos comerciais e dados pessoais (Zscaler, 2025).

A transnacionalidade desses crimes e o uso de *criptoativos* como meio de pagamento impõem desafios inéditos à persecução penal. A cadeia de custódia digital, conforme introduzido pelo Pacote Anticrime (Lei nº 13.964/2019) nos artigos 158-A a 158-F do Código de Processo Penal, exige rigor extremo na preservação da prova digital. Qualquer falha no isolamento ou no registro do acesso ao dado pode gerar a nulidade da prova, sob a alegação de que o vestígio foi adulterado (Nucci, 2023).

2.2 ANÁLISE DOGMÁTICA DA TIPIFICAÇÃO PENAL NO BRASIL

No ordenamento jurídico brasileiro, a conduta de extorsão digital por *ransomware* não possui um tipo penal específico, sendo enquadrada por meio da interpretação e subsunção a tipos penais já existentes no Código Penal. A doutrina majoritária converge para a aplicação dos artigos 158 e 154-A do Código Penal, a depender da fase e do objetivo da conduta, conforme sustentado por Cunha (2018) e Nucci (2023).

O crime de extorsão, previsto no Art. 158 do Código Penal, é o tipo penal que melhor se adequa à finalidade última do ataque de *ransomware*: a obtenção de vantagem econômica indevida mediante coação. O bem jurídico tutelado no crime de extorsão é complexo, abrangendo tanto o patrimônio quanto a liberdade individual. No contexto do *ransomware*, a grave ameaça se materializa na privação do acesso aos dados (criptografia) ou na ameaça de divulgação (dupla extorsão), o que constrange a vítima a pagar o resgate para reaver seu patrimônio e sua liberdade de dispor dos próprios dados. A doutrina penal moderna reconhece que a ameaça de dano virtual, como a perda ou exposição de dados, é plenamente capaz de configurar a grave ameaça exigida pelo tipo (Bitencourt, 2025).

A adequação típica é considerada satisfatória pela maioria dos penalistas, que veem na extorsão digital uma modalidade de extorsão comum, onde o meio de execução, com o emprego da tecnologia, não altera a essência do crime.

Entretanto, o crime de invasão de dispositivo informático, introduzido pela Lei nº 12.737/2012 (Lei Carolina Dieckmann), é frequentemente o crime-meio para a execução da extorsão por *ransomware*. O Art. 154-A está inserido no Título I do Código Penal, que trata dos Crimes Contra a Pessoa, especificamente no Capítulo VI, que versa sobre os Crimes Contra a Liberdade Individual. O bem jurídico tutelado é, portanto, a inviolabilidade dos dados e da comunicação e, mediatamente, a liberdade individual e a privacidade do usuário (Cunha, 2018).

Na prática do *ransomware*, o agente, para extorquir a vítima, primeiro invade o dispositivo informático. A doutrina e a jurisprudência tendem a aplicar o princípio da consunção ou o concurso formal de crimes. Se a invasão (Art. 154-A) é um meio necessário e único para a prática da extorsão (Art. 158), o crime mais grave (extorsão) absorve o menos grave (invasão), aplicando-se a pena apenas do Art.

158. Alternativamente, se a invasão e a extorsão são vistas como condutas autônomas, mas praticadas no mesmo contexto fático, pode-se aplicar o concurso formal (Art. 70 do Código Penal), com aumento da pena do crime mais grave. O concurso formal, conforme disciplinado no art. 70 do Código Penal, ocorre quando o agente, mediante uma só ação ou omissão, pratica dois ou mais crimes, idênticos ou não, aplicando-se a mais grave das penas cabíveis, aumentada de um sexto até metade (Greco, 2017; Schmitt, 2019).

A jurisprudência tem demonstrado uma tendência a considerar o *ransomware* como extorsão qualificada pelo emprego de meio fraudulento (Art. 158, § 3º, c/c Art. 154-A), ou simplesmente extorsão, absorvendo a invasão, dada a finalidade precípua de obtenção de vantagem econômica (Nucci, 2023).

2.3 DESAFIOS E LIMITAÇÕES NO CONTEXTO JURÍDICO BRASILEIRO

A extorsão digital por meio de *ransomware* representa uma das ameaças cibernéticas mais proeminentes da atualidade. No Brasil, a resposta jurídica a esse fenômeno complexo é multifacetada, envolvendo a aplicação de leis como a Lei nº 14.155/2021, que alterou o Código Penal para agravar crimes de invasão de dispositivo informático, e o Art. 158 do Código Penal. Além disso, a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018), impõe a obrigação de notificar a Autoridade Nacional de Proteção de Dados (ANPD) em casos de incidentes que possam gerar risco ou dano relevante aos titulares dos dados. Contudo, a efetividade da persecução penal e a compreensão do cenário completo são dificultadas por diversas limitações (Peck, 2021; ANPD, 2023).

Um dos maiores obstáculos para o estudo acadêmico e para a prática jurídica relacionados aos ataques de ransomware consiste na escassez de acórdãos, sentenças e demais decisões judiciais suficientemente detalhadas sobre o tema. Tal limitação decorre, em grande medida, da própria natureza dos incidentes analisados, que frequentemente envolvem o comprometimento de dados pessoais, informações empresariais estratégicas e sistemas críticos. Em razão da sensibilidade desses elementos, muitos processos são submetidos ao regime de segredo de justiça, com o objetivo de resguardar a intimidade das vítimas, proteger informações confidenciais e evitar a exposição de vulnerabilidades que possam comprometer ainda mais a segurança dos sistemas afetados.

Além disso, a reduzida quantidade de casos disponíveis para consulta pública não se explica apenas pela restrição de acesso aos autos judiciais. Em diversos episódios de ransomware, as organizações atingidas optam por solucionar o incidente fora da esfera judicial, recorrendo à contratação de consultorias especializadas em resposta a incidentes cibernéticos para conduzir as medidas de contenção, investigação e recuperação dos sistemas comprometidos. Em situações consideradas críticas, algumas empresas chegam inclusive a realizar o pagamento do resgate exigido pelos agentes maliciosos, sem comunicar formalmente o ocorrido às autoridades competentes. Como consequência, esses eventos deixam de ser submetidos à apreciação do Poder Judiciário, reduzindo significativamente a produção de precedentes e dificultando a formação de uma jurisprudência pública consolidada sobre a matéria (Barreto; Jorge, 2021).

A obtenção de estatísticas oficiais confiáveis no Brasil é dificultada pela fragmentação dos registros. Embora a LGPD obrigue a comunicação de incidentes de segurança à ANPD quando houver risco aos titulares, essa notificação tem caráter administrativo. Não há, ainda, uma integração sistêmica que converta todas essas notificações em dados estatísticos criminais unificados para fins de segurança pública. Registros de ocorrência podem ser feitos como estelionato, extorsão ou danos, dependendo da interpretação do agente no momento da lavratura, o que gera ruído nos dados estatísticos de incidência real desse crime específico (Rezende, 2022).

De acordo com dados divulgados pela ANPD em 2025, até o mês de abril foram registrados 77 casos de incidentes de segurança, dos quais 23 estavam relacionados a *ransomware*, sendo 14 sem transferência de dados e 9 com *exfiltração* e vazamento de informações. O estado de São Paulo concentrou o maior número de comunicações (26 casos), seguido pelo Distrito Federal (16 casos). Nota-se que diversos estados das regiões Norte e Nordeste não registraram nenhum caso, o que pode indicar não a ausência de incidentes, mas uma possível *subnotificação* por parte das organizações (Convergência Digital, 2025; Tera Tecnologia, 2025).

> A subnotificação é uma questão esperada neste contexto, devido à falta de maturidade das empresas em lidar com incidentes de segurança da informação. Isso evidencia a necessidade de uma gestão eficaz de incidentes nas organizações brasileiras. É preciso investir e disseminar o conhecimento sobre o tema, especialmente porque nem todas as empresas

> enfrentavam exigências regulatórias e punitivas que as obrigam a comunicação de incidentes antes da LGPD, como é o caso das instituições bancárias. (Tera Tecnologia, 2025)

O maior desafio da investigação de *ransomware* no Brasil é a atribuição. No Direito Penal, a responsabilidade é subjetiva; é preciso provar quem agiu. No entanto, o atacante utiliza camadas de ocultação que desafiam a capacidade de resposta do Estado. O resgate é exigido em *criptomoedas* (como Bitcoin ou Monero). Embora o *blockchain* seja público, os criminosos utilizam serviços de mixagem para lavar os ativos, quebrando o nexo de causalidade entre o pagamento e a identidade do receptor. A investigação depende, então, de ordens judiciais para corretoras (*exchanges*), que muitas vezes estão fora da jurisdição nacional (Aras, 2020). Os ataques são orquestrados via servidores espalhados por múltiplos países. Identificar o terminal de origem exige que a polícia brasileira solicite dados de provedores estrangeiros que, em muitos casos, não mantêm *logs* de acesso por tempo suficiente, ferindo o princípio da preservação da prova.

De acordo com o Art. 158-A do Código de Processo Penal, a cadeia de custódia é o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio. No *ransomware*, o vestígio é imaterial e volátil. Muitas vezes, os artefatos do vírus e as chaves de criptografia residem apenas na memória volátil (RAM) do servidor atacado. Se o administrador do sistema reiniciar a máquina por pânico, a prova digital é destruída. A investigação forense, portanto, exige uma intervenção imediata que as polícias judiciárias, por limitações operacionais, nem sempre conseguem oferecer (Nucci, 2023).

A transnacionalidade é o obstáculo jurídico mais severo. O Art. 7º do Código Penal trata da extraterritorialidade, mas a aplicação prática é complexa. O Brasil ratificou sua adesão à Convenção de Budapeste sobre o Crime Cibernético (Decreto nº 11.491/2023), que permite a preservação rápida de dados informáticos e a cooperação mútua. O desafio investigativo aqui é a padronização: os investigadores brasileiros precisam redigir pedidos de cooperação que atendam aos requisitos de leis estrangeiras (como o GDPR europeu ou o Cloud Act americano), sob pena de a prova ser considerada ilícita no Brasil por vício de origem. Países que não são signatários da convenção podem se recusar a fornecer dados de tráfego de internet, tornando o criminoso invisível assim que o pacote de dados cruza essa fronteira digital (Rezende, 2022; Souza, 2021).

A eficácia da investigação criminal é diretamente proporcional à capacidade operacional do Estado. No Brasil, observa-se um descompasso entre a modernização do crime e a estrutura das polícias judiciárias. Há uma carência de peritos especializados em crimes de alta tecnologia e analistas de inteligência cibernética nas delegacias de polícia civil e federal. A formação contínua desses profissionais é cara e exige constante atualização diante de novas linguagens de programação e métodos de invasão. Ferramentas de extração de dados possuem alto custo de licenciamento, muitas vezes em moeda estrangeira, o que impede que pequenas delegacias realizem perícias básicas, sobrecarregando os Institutos de Criminalística centrais (Wendt, 2022). Ademais, a falta de integração entre os sistemas das polícias estaduais e federais dificulta o cruzamento de dados de inteligência, mantendo a investigação focada em casos isolados em vez de desarticular organizações criminosas.

3 RESULTADOS E DISCUSSÕES

Os resultados da pesquisa evidenciam que o ordenamento jurídico brasileiro possui dispositivos aplicáveis à extorsão digital por *ransomware*, mas esses dispositivos funcionam como uma colcha de retalhos. Atualmente, o *ransomware* é enquadrado pela combinação dos artigos 154-A (Invasão) e 158 (Extorsão) do CP. Embora esses artigos permitam a punição, eles carecem de especificidade para as nuances do crime digital moderno, como a extorsão dupla (criptografia de dados mais ameaça de vazamento). A legislação ainda é limitada na abrangência de medidas assecuratórias modernas e na definição de crimes de auxílio ou hospedagem de serviços criminosos (Peck, 2021; Cunha, 2018).

A investigação criminal brasileira esbarra em um teto tecnológico. A transnacionalidade permite que o autor do crime utilize infraestruturas de países com legislação precária (os chamados safe *havens*), o que, somado ao uso de ferramentas de *anonimização* (VPNs e rede Tor) e pagamentos via *criptoativos*, torna a rastreabilidade um desafio hercúleo. A atuação das autoridades é dificultada não por falta de vontade política, mas pela volatilidade da evidência digital. Quando a prova atravessa fronteiras em milissegundos, os mecanismos tradicionais de carta

rogatória tornam-se obsoletos, resultando em uma lacuna entre a ocorrência do crime e a capacidade de resposta do Estado (Barreto; Jorge, 2021; Aras, 2020).

Dada a natureza desterritorializada do crime de extorsão digital, o isolamento jurídico do Estado é o maior aliado do criminoso. O recente passo dado pelo Brasil com a ratificação da Convenção de Budapeste (Decreto nº 11.491/2023) comprova que o caminho viável é a padronização de procedimentos de assistência mútua. O aprimoramento legislativo, exemplificado pela Lei nº 14.155/2021, que agravou penas para invasão de dispositivos e furtos qualificados por meio eletrônico, mostra que a atualização das normas aumenta o poder de dissuasão e oferece melhores ferramentas para o Ministério Público e a Magistratura. No entanto, a viabilidade depende de que a lei não seja apenas formal, mas acompanhada de tratados que permitam o acesso célere a dados em servidores estrangeiros (Rezende, 2022; Souza, 2021).

A responsabilidade penal no ambiente digital brasileiro hoje é um campo em construção. O sucesso do enfrentamento ao crime cibernético não virá apenas da criação de novas leis, mas da integração entre o rigor processual (cadeia de custódia), a agilidade diplomática (cooperação) e o investimento em perícia técnica. O equilíbrio entre o poder de punir do Estado e as garantias individuais de privacidade (LGPD) é o norte ético que deve guiar as próximas reformas legislativas. A pesquisa demonstra que, embora o Direito Penal não seja omisso, ele ainda corre atrás da evolução técnica das modalidades de extorsão digital, necessitando de tipos penais que compreendam o fenômeno em sua totalidade técnica (Wendt, 2022; Nucci, 2023).

4 CONSIDERAÇÕES FINAIS

A presente pesquisa permitiu analisar o regime jurídico da responsabilização penal nos casos de extorsão digital por *ransomware* no Brasil, com ênfase nos desafios impostos à investigação cibernética. Verificou-se que, embora o ordenamento jurídico disponha de dispositivos aplicáveis, especialmente os artigos 158 e 154-A do Código Penal, a especificidade do fenômeno do *ransomware* exige uma interpretação evolutiva e integrada das normas existentes, bem como a atualização legislativa para acompanhar a sofisticação técnica dos criminosos.

A investigação criminal brasileira enfrenta obstáculos de ordem técnica, jurídica e operacional. A volatilidade da prova digital, o uso de *criptoativos* e ferramentas de *anonimização*, aliados à transnacionalidade dos ataques, tornam a atribuição de autoria e a coleta de evidências atividades extremamente complexas. A ratificação da Convenção de Budapeste representa um avanço importante, mas sua efetividade depende da capacidade operacional das polícias judiciárias e da integração entre os sistemas de inteligência nacional e internacional.

A Lei Geral de Proteção de Dados Pessoais (LGPD) e o Marco Civil da Internet estabelecem bases importantes para a segurança da informação e a cooperação entre entes públicos e privados, mas ainda há lacunas na conversão de notificações administrativas em dados estatísticos criminais unificados. A fragmentação dos registros de ocorrência e a *subnotificação* por parte das vítimas corporativas impedem a formação de uma base de dados robusta para orientar políticas públicas de segurança cibernética.

Como encaminhamento para o enfrentamento mais eficaz da extorsão digital por ransomware, sugere-se o aperfeiçoamento da legislação penal brasileira, de modo a contemplar de forma mais específica as particularidades desse fenômeno criminoso. Embora o ordenamento jurídico atualmente disponha de tipos penais capazes de alcançar determinadas condutas relacionadas aos ataques cibernéticos, a crescente sofisticação das práticas empregadas pelos agentes criminosos evidencia a necessidade de maior precisão normativa. Nesse contexto, a tipificação específica das modalidades contemporâneas de extorsão digital pode contribuir para reduzir ambiguidades interpretativas e proporcionar maior segurança jurídica na persecução penal.

Especial atenção deve ser conferida às modalidades de dupla extorsão e ao modelo conhecido como Ransomware-as-a-Service (RaaS). A primeira caracteriza-se não apenas pela criptografia dos dados da vítima, mas também pela ameaça de divulgação pública das informações obtidas durante a invasão, ampliando significativamente o potencial coercitivo da conduta. Já o modelo RaaS permite que desenvolvedores de ferramentas maliciosas disponibilizem sua infraestrutura para terceiros mediante participação nos lucros obtidos com os ataques, promovendo a profissionalização e a expansão desse mercado ilícito. Diante dessas transformações, torna-se relevante que a legislação acompanhe a evolução tecnológica e criminal observada nos últimos anos.

Além das medidas de natureza legislativa, mostra-se necessária a adoção de mecanismos institucionais voltados à produção e à integração de informações sobre incidentes cibernéticos. Nesse sentido, a criação de um cadastro nacional de incidentes de segurança cibernética, articulado com os órgãos de persecução penal e demais entidades competentes, poderia contribuir para superar a atual fragmentação dos dados disponíveis. Paralelamente, o fortalecimento dos laboratórios de perícia forense digital e a capacitação contínua de policiais, peritos, membros do Ministério Público e magistrados constituem medidas essenciais para reduzir o descompasso existente entre a rápida evolução das técnicas empregadas pelos criminosos e a capacidade de resposta do Estado.

Por fim, a efetiva responsabilização penal dos autores de crimes praticados no ambiente digital depende de uma abordagem sistêmica e multidisciplinar, capaz de integrar o rigor processual, a cooperação internacional célere e o investimento permanente em recursos técnicos e humanos. Nesse cenário, o equilíbrio entre o exercício do poder punitivo estatal e a preservação das garantias fundamentais de privacidade e proteção de dados deve orientar tanto as reformas legislativas quanto as práticas investigativas adotadas pelos órgãos competentes. A presente pesquisa busca contribuir para o aprofundamento do debate acadêmico acerca do tema, oferecendo subsídios para a atuação de profissionais do Direito e para a formulação de políticas públicas mais eficazes no enfrentamento da extorsão digital por meio de ransomware.

REFERÊNCIAS

ARAS, Vladimir. **Cooperação Jurídica Internacional em Matéria Penal**. São Paulo: Atlas, 2020.

BARDIN, Laurence. **Análise de Conteúdo**. São Paulo: Edições 70, 2016.

BARRETO, Valdir; JORGE, Higor. **Crimes Cibernéticos e Investigação Digital**. São Paulo: Atlas, 2021.

BITENCOURT, Cezar. **Tratado de Direito Penal: parte especial**. 25. ed., v. 2. São Paulo: Saraiva Jur, 2025.

BRASIL. ANPD (Autoridade Nacional de Proteção de Dados). **Guia Orientativo: Segurança de Dados e Incidentes.** Brasília, 2023. Disponível em: https://www.gov.br/anpd/pt-br. Acesso em: 5 maio 2026.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília, 1988.

_____. **Decreto nº 11.491**, de 12 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético, firmada em Budapeste, em 23 de novembro de 2001. Diário Oficial da União, Brasília, 13 abr. 2023. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2023/decreto/d11491.htm. Acesso em: 5 maio 2026.

_____. **Decreto-Lei nº 2.848**, de 7 de dezembro de 1940. Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 3 out. 2025.

_____. **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. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 3 out. 2025.

_____. **Lei nº 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 3 out. 2025.

_____. **Lei nº 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 5 maio 2026.

_____. **Lei nº 13.964**, de 24 de dezembro de 2019. Institui o Pacote Anticrime. Diário Oficial da União, Brasília, 26 dez. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 5 maio 2026.

_____. **Lei nº 14.155**, de 26 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para agravar as penas dos crimes de furto qualificado e de invasão de dispositivo informático. Diário Oficial da União, Brasília, 27 maio 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 5 maio 2026.

CONVERGÊNCIA DIGITAL. **ANPD divulga mapa de incidentes de segurança, São Paulo e Distrito Federal lideram**. 1 abr. 2025. Disponível em: https://convergenciadigital.com.br/governo/anpd-divulga-mapa-de-incidentes-de-seguranca-sao-paulo-e-distrito-federal-lideram/. Acesso em: 5 maio 2026.

CRESPO, Marcelo. **Crimes Digitais**. 3. ed. São Paulo: Saraiva, 2021.

CUNHA, Rogério Sanches. **Crimes Contra a Pessoa**. 18. ed. Rio de Janeiro: Forense, 2018.

DEMO, Pedro. **Introdução à Metodologia Científica**. São Paulo: Atlas, 2024.

GIL, Antonio Carlos. **Como Elaborar Projetos de Pesquisa**. 6. ed. São Paulo: Atlas, 2022.

GRECO, Rogério. **Curso de Direito Penal: parte geral**. 20. ed. Niterói: Impetus, 2017.

IBM. **What Is Ransomware-as-a-Service (RaaS)?** Disponível em: https://www.ibm.com/think/topics/ransomware-as-a-service. Acesso em: 3 out. 2025.

IDP. **Método Dedutivo: definição, características e exemplos**. Disponível em: https://www.idp.edu.br/blog/metodo-dedutivo/. Acesso em: 5 maio 2026.

KASPERSKY. **Kaspersky State of Ransomware Report 2025**. 7 maio 2025. Disponível em: https://www.kaspersky.com/about/press-releases/kaspersky-state-of-ransomware-report-2025-global-and-regional-insights-for-international-anti-ransomware-day. Acesso em: 5 maio 2026.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de Metodologia Científica**. 8. ed. São Paulo: Atlas, 2023.

NUCCI, Guilherme de Souza. **Curso de Direito Penal: parte especial**. 23. ed. Rio de Janeiro: Forense, 2023.

PECK, Patricia. **Direito Digital**. 7. ed. São Paulo: Saraiva, 2021.

REZENDE, Bruno. **Convenção de Budapeste: Reflexos na Legislação Processual Penal Brasileira**. Belo Horizonte: Editora D'Plácido, 2022.

SCHMITT, Gustavo. **Concurso de Crimes e Continuidade Delitiva**. 2. ed. São Paulo: Revista dos Tribunais, 2019.

SECURITY LEADERS. **Brasil é o nono país mais atingido por ransomware no mundo**. 23 jan. 2025. Disponível em: https://www.securityleaders.com.br/brasil-e-o-nono-pais-mais-atingido-por-ransomware-no-mundo/. Acesso em: 5 maio 2026.

SEVERINO, Antônio Joaquim. **Metodologia do Trabalho Científico**. 23. ed. rev. São Paulo: Editora Bookman, 2007.

SOUZA, Artur. **Cibercrimes e a Convenção de Budapeste**. Rio de Janeiro: Lumen Juris, 2021.

TERA TECNOLOGIA. **ANPD aponta dezenas de incidentes de segurança em 2025**. 4 abr. 2025. Disponível em: https://tera-tecnologia.com/anpd-aponta-dezenas-de-incidentes-de-seguranca-em-2025/. Acesso em: 5 maio 2026.

TREND MICRO. **Ransomware: como funciona a criptografia usada pelos cibercriminosos**. Disponível em: https://www.trendmicro.com/pt_br/research.html. Acesso em: 5 maio 2026.

WENDT, Emerson; JORGE, Higor. **Crimes Cibernéticos: Ameaças e Procedimentos de Investigação**. 4. ed. Rio de Janeiro: Juspodivm, 2022.

ZSCALER. **What Is Double Extortion Ransomware?** Disponível em: https://www.zscaler.com/resources/security-terms-glossary/what-is-double-extortion-ransomware. Acesso em: 3 out. 2025.