Revista Ibero-Americana de Humanidades, Ciências e Educação — REASE

doi.org/10.51891/rease.v12i11.31537

OS DESAFIOS DA INVESTIGAÇÃO CRIMINAL DO RANSOMWARE NO ORDENAMENTO JURÍDICO BRASILEIRO

THE CHALLENGES OF CRIMINAL INVESTIGATION OF RANSOMWARE UNDER THE BRAZILIAN LEGAL SYSTEM

Gabriel Martins de Sousa[1]
Justino Soares dos Santos Filho[2]

RESUMO: A crescente digitalização das relações sociais, empresariais e estatais ampliou a exposição de sistemas informáticos a práticas ilícitas de elevada complexidade. Nesse contexto, o ransomware destaca-se por associar a invasão de dispositivos, a criptografia ou o bloqueio de dados e a exigência de pagamento de resgate, frequentemente efetuado por meio de criptoativos de difícil rastreamento. Nesse contexto, examina-se os obstáculos enfrentados pela persecução penal brasileira diante dessa modalidade delitiva, com o objetivo de verificar se o conjunto normativo e operacional vigente, Lei nº 12.737/2012, Lei nº 14.155/2021, Marco Civil da Internet, Lei Geral de Proteção de Dados Pessoais e as normas de cadeia de custódia da prova digital, revela-se suficiente para assegurar a identificação de autoria, a preservação de evidências e a efetiva responsabilização dos autores. Adota-se o método dedutivo, com abordagem qualitativa, mediante pesquisa bibliográfica e documental, fundamentada em doutrina especializada, legislação pertinente e jurisprudência dos tribunais superiores. Os resultados indicam que não obstante os avanços legislativos, o ransomware permanece sem tipificação penal autônoma no Brasil, sendo enquadrado por construção doutrinária e jurisprudencial no crime de invasão de dispositivo informático e, em concurso aparente, no de extorsão. Conclui-se que a eficácia da resposta estatal reclama, além da eventual aprovação de tipos penais específicos, objeto de projetos de lei em tramitação no Congresso Nacional, o aprimoramento da perícia digital, o fortalecimento da cooperação internacional e a modernização dos instrumentos de rastreamento de criptoativos.

Palavras-chave: Ransomware. Investigação criminal. Crimes cibernéticos. Legislação Brasileira. Prova digital.

ABSTRACT: The increasing digitalization of social, business, and state interactions has heightened the exposure of computer systems to highly complex illicit activities. In this context, ransomware stands out by combining device intrusion, data encryption or blocking, and ransom demands often settled via hard-to-trace crypto-assets. This study examines the obstacles facing Brazilian criminal prosecution regarding this type of crime, aiming to determine whether the current legal and operational framework comprising Law No. 12.737/2012, Law No. 14.155/2021, the Internet Civil Rights Framework (Marco Civil da Internet), the General Personal Data Protection Law, and regulations on the chain of custody for digital evidence is sufficient to ensure the identification of perpetrators, the preservation of evidence, and the effective holding of offenders accountable. A deductive method with a qualitative approach is employed, based on bibliographic and documentary research involving specialized legal doctrine, relevant legislation, and superior court jurisprudence. The results indicate that, despite legislative advances, ransomware remains without a distinct statutory definition in Brazil; instead, it is classified through doctrinal and judicial interpretation under the crime of unauthorized intrusion into a computing device and, in a case of apparent conflict of norms, as extortion. The study concludes that effective state response requires not only the potential enactment of specific criminal offenses currently

[1] Acadêmico do curso de Direito. Universidade de Gurupi (UNIRG).
[2] Orientador. Professor do curso de Direito. Universidade de Gurupi (UNIRG).

the subject of bills pending in the National Congress but also the enhancement of digital forensics, the strengthening of international cooperation, and the modernization of tools for tracking crypto-assets.

Keywords: Ransomware. Criminal investigation. Cybercrimes. Brazilian legislation. Digital evidence.

1 INTRODUÇÃO

A evolução do Direito Penal e Processual Penal no ordenamento jurídico brasileiro, especialmente a partir da popularização da internet e da transformação digital, promoveu significativa ampliação das formas de criminalidade, deslocando o enfoque tradicional de ilícitos materiais para uma perspectiva centrada na proteção de sistemas informáticos, na preservação de dados e na responsabilização de condutas praticadas no ambiente virtual. Nesse contexto, o *ransomware* passou a ser concebido não apenas como mera invasão de dispositivo, mas como um complexo de ações que reúnem a invasão de sistemas, o bloqueio ou a criptografia de dados e a exigência de pagamento de resgate, ordinariamente mediante criptoativos de difícil rastreamento (GOMES; NUNES; WILMERS, 2020).

A partir dessa nova configuração, emergiu no cenário jurídico a discussão acerca dos desafios da investigação criminal do *ransomware* e da suficiência dos instrumentos normativos e operacionais disponíveis para garantir a identificação de autoria, a preservação da prova digital e a responsabilização penal dos infratores. Trata-se de tema que suscita intensos debates doutrinários e jurisprudenciais, marcados por relevantes divergências quanto aos limites da tipificação penal vigente e à própria extensão da persecução penal nesse contexto (SANTOS FILHO; FURLAN, 2021).

Nesse sentido, coloca-se como problema central da presente pesquisa a seguinte indagação: os instrumentos normativos e operacionais atualmente disponíveis a Lei nº 12.737/2012 (BRASIL, 2012), a Lei nº 14.155/2021 (BRASIL, 2021), o Marco Civil da Internet (BRASIL, 2014), a Lei Geral de Proteção de Dados (BRASIL, 2018) e as regras processuais de cadeia de custódia introduzidas pelo Pacote Anticrime (BRASIL, 2019) são suficientes para garantir a identificação de autoria, a preservação da prova digital e a responsabilização penal dos infratores, ou, ao contrário, subsistem lacunas que comprometem a efetividade da resposta estatal?

A relevância do tema justifica-se não apenas pela sua atualidade, mas também pela necessidade de se estabelecer critérios jurídicos seguros para a investigação e a persecução penal de ataques de *ransomware*, evitando tanto a impunidade de condutas que violam a integridade de sistemas informáticos e a confidencialidade de dados, quanto a ineficácia da resposta estatal

diante da sofisticação técnica e da transnacionalidade desse fenômeno. Levantamentos recentes situam o Brasil entre os países mais atingidos por ataques dessa natureza (WAKKA, 2019).

O objetivo geral do presente trabalho consiste em analisar os principais obstáculos enfrentados pela persecução penal brasileira em face de ataques de *ransomware*, à luz da legislação vigente, da doutrina contemporânea e da jurisprudência dos tribunais superiores. Como objetivos específicos, busca-se: (i) examinar o conceito, o *modus operandi* e a distinção do *ransomware* em relação a outros cibercrimes; (ii) analisar a legislação brasileira aplicável, da Lei Carolina Dieckmann aos projetos de lei em tramitação; (iii) identificar os desafios investigativos relacionados à prova digital, ao rastreamento de criptoativos e à cooperação internacional; (iv) delimitar os limites impostos pelo princípio da legalidade estrita; e (v) examinar a jurisprudência do Superior Tribunal de Justiça e casos concretos de persecução penal.

Para tanto, adotou-se o método dedutivo, com abordagem qualitativa, mediante pesquisa bibliográfica e documental, baseada na análise de doutrina especializada, legislação pertinente e julgados relevantes dos tribunais superiores.

Por fim, o trabalho encontra-se estruturado em sete seções: na primeira, são apresentados os fundamentos introdutórios do tema; na segunda, o conceito, o *modus operandi* e a distinção do *ransomware* de outras modalidades de cibercrime, incluindo panorama do fenômeno no Brasil; na terceira, a legislação brasileira aplicável, da Lei Carolina Dieckmann aos projetos de lei em tramitação; na quarta, os desafios investigativos, prova digital e cadeia de custódia, rastreamento de criptoativos, cooperação internacional e os limites do princípio da legalidade estrita; na quinta, a análise jurisprudencial, com precedentes do Superior Tribunal de Justiça; na sexta, as considerações finais; e, na sétima, as referências.

2 O RANSOMWARE: CONCEITO, MODUS OPERANDI E DISTINÇÃO DE OUTROS CIBERCRIMES

2.1 Conceito e natureza técnica

O *ransomware* pode ser definido como *software* malicioso (*malware*) desenvolvido para restringir o acesso da vítima a um sistema, dispositivo ou conjunto de dados, condicionando sua liberação ao pagamento de um resgate. O *malware* é implantado por criminosos que exploram vulnerabilidades em dispositivos, servidores ou redes para infectar alvos específicos, com o

objetivo de inutilizar total ou parcialmente o sistema e, com frequência, extrair dados confidenciais (GOMES; NUNES; WILMERS, 2020).

Do ponto de vista técnico, a doutrina especializada distingue duas modalidades principais. O *ransomware* pode comprometer as funções básicas do computador, o chamado *ransomware* de bloqueio, ou *locker*, ou atingir apenas parte dos arquivos por meio de criptografia, hipótese conhecida como *crypto ransomware*. Essa distinção é relevante porque impacta diretamente a perícia forense: no primeiro caso, o sistema fica inoperante como um todo; no segundo, os dados permanecem fisicamente no dispositivo, porém inacessíveis sem a chave de descriptografia, o que exige técnicas periciais distintas para a reconstrução da prova.

2.2 Modus operandi

O ataque de *ransomware* não se limita a um único ato de invasão; trata-se, em regra, de uma cadeia de condutas encadeadas, que pode ser dividida, para fins didáticos, em quatro fases. O comprometimento inicial costuma ocorrer por meio de *phishing*, exploração de vulnerabilidades do sistema operacional, roubo de credenciais ou uso de outro *malware* como vetor de entrada. Uma vez dentro do ambiente, o *ransomware* busca compreender a estrutura do sistema local para localizar informações e dados de valor a serem sequestrados. Segue-se uma etapa de reconhecimento e localização do ponto inicial da infecção, o chamado "paciente zero", informação relevante tanto para a resposta ao incidente quanto, posteriormente, para a investigação criminal. Relatório recente da Europol indica que o acesso inicial a sistemas, obtido inclusive pela exploração de vulnerabilidades em infraestruturas expostas à internet, circula em um mercado criminal organizado, e que credenciais e acessos assim obtidos são aproveitados por grupos de *ransomware* (EUROPOL, 2025).

Consumado o comprometimento, os dados são criptografados ou o sistema é bloqueado, e passa a ser exigido o pagamento do resgate, tipicamente em criptoativos de difícil rastreamento. Em muitos casos contemporâneos, o grupo criminoso já copia os dados antes de criptografá-los, ameaçando divulgá-los publicamente caso o resgate não seja pago, a chamada dupla extorsão, que soma à ameaça de indisponibilidade a ameaça à confidencialidade dos dados. Por fim, na fase de monetização, o pagamento, quando realizado, não garante a devolução do acesso; há casos em que, mesmo após o pagamento, os criminosos não cumprem o acordado, ampliando o prejuízo da vítima (GOMES; NUNES; WILMERS, 2020).

2.3 Distinção de outros cibercrimes

É importante diferenciar o *ransomware* de outras modalidades de criminalidade cibernética mais estudadas pela doutrina nacional, como o *phishing* e o estelionato eletrônico. Nestes últimos, o núcleo da conduta está na fraude: induz-se a vítima a erro para que ela mesma forneça dados, senhas ou realize a transferência de valores. No *ransomware*, por outro lado, a conduta central é técnica, a invasão e o comprometimento do sistema, e o consentimento da vítima é irrelevante para a consumação do delito.

Sob a ótica penal brasileira, essa natureza híbrida gera um problema de tipificação: o ataque de *ransomware* reúne, na mesma conduta, elementos de dois tipos penais distintos. O Código Penal tipifica no art. 154-A a invasão de dispositivo informático mediante violação indevida de mecanismo de segurança, com o fim de obter, adulterar ou destruir dados sem autorização do titular (BRASIL, 1940). Quando o dispositivo é invadido para viabilizar a exigência de vantagem indevida mediante grave ameaça, a exigência do resgate, configura-se também o crime de extorsão (art. 158 do Código Penal). A doutrina penal brasileira resolve esse concurso aparente pela regra da consunção, segundo a qual o crime que serve de meio necessário para a execução de outro é absorvido pelo delito mais grave, evitando a dupla incriminação pela mesma conduta. Essa solução, no entanto, é criticada por parte da doutrina especializada, que sustenta ser insuficiente para capturar a gravidade e a especificidade econômica do sequestro de dados (GOMES; NUNES; WILMERS, 2020).

2.4 Panorama do fenômeno no Brasil

Os dados disponíveis indicam a centralidade do Brasil nesse cenário. O país ocupa a segunda posição mundial em número de ataques de *ransomware*, respondendo por 10,75% dessa modalidade de ameaça em todo o mundo (WAKKA, 2019). Levantamentos setoriais apontam ainda um crescimento de 92% nesse tipo de ataque no Brasil, percentual superior à média global. Esse crescimento não se limita ao setor privado: instituições públicas brasileiras de relevo já foram alvo de ataques de *ransomware*, a exemplo do Superior Tribunal de Justiça em novembro de 2020 e, em 2021, do Tribunal Regional Federal da 3ª Região, do Tribunal de Justiça do Rio Grande do Sul e do Ministério da Saúde, com impacto direto em sistemas críticos como o processo eletrônico e o ConecteSUS. Esses episódios ilustram a gravidade prática do problema jurídico examinado nas seções seguintes: a insuficiência da resposta normativa brasileira diante de um fenômeno técnica e economicamente sofisticado. No plano internacional, a avaliação

anual da Europol sobre a criminalidade organizada na internet aponta o *ransomware* como a ameaça cibernética de maior potencial disruptivo, em um cenário de crescente convergência entre o crime organizado tradicional e o cibercrime (EUROPOL, 2025).

3 LEGISLAÇÃO BRASILEIRA FRENTE AO RANSOMWARE

3.1 Lei nº 12.737/2012 (Lei Carolina Dieckmann)

O primeiro marco normativo brasileiro a tratar da invasão de dispositivos informáticos foi a Lei nº 12.737/2012, que incluiu o art. 154-A no Código Penal (BRASIL, 2012). A lei surgiu em resposta a um caso concreto amplamente divulgado a invasão do computador da atriz Carolina Dieckmann, cujas imagens íntimas foram obtidas por *hackers* e usadas como instrumento de extorsão, evidenciando que, até aquele momento, o ordenamento brasileiro não dispunha de tipo penal específico para condutas dessa natureza. Na redação original, o art. 154-A exigia que a invasão ocorresse "mediante violação indevida de mecanismo de segurança" e cominava pena de detenção de três meses a um ano, além de multa, sanção branda diante da gravidade e da extensão dos danos que um ataque cibernético pode causar.

Essa formulação inicial já continha, em germe, o núcleo típico que hoje é aplicado por analogia ao *ransomware*: invadir dispositivo alheio com o fim de obter, adulterar ou destruir dados sem autorização do titular. No entanto, a lei de 2012 não previu qualquer tratamento específico para a hipótese em que a invasão é seguida de bloqueio ou criptografia dos dados com exigência de resgate, fenômeno que, à época, ainda não tinha a escala e a sofisticação que viria a adquirir a partir de 2017.

3.2 Lei nº 14.155/2021

Quase uma década depois, a Lei nº 14.155/2021 promoveu alterações relevantes no art. 154-A, tornando mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica (BRASIL, 2021). Entre as principais mudanças, a nova redação suprimiu a exigência de "violação indevida de mecanismo de segurança" como elemento do tipo ampliando, portanto, sua incidência e elevou substancialmente a pena da forma básica, que passou de detenção de três meses a um ano para reclusão de um a quatro anos, além de multa. A lei também qualificou a conduta quando da invasão resulta a obtenção de conteúdo de comunicações privadas, segredos comerciais ou industriais, informações sigilosas ou o controle

remoto não autorizado do dispositivo invadido, hipótese em que a pena sobe para reclusão de dois a cinco anos.

Apesar do avanço, a Lei nº 14.155/2021 não criou um tipo penal autônomo para o *ransomware*; ela apenas recrudesceu as penas do delito já existente de invasão de dispositivo informático. A doutrina especializada é enfática ao apontar que o Brasil segue tratando o *ransomware* por meio do enquadramento combinado dos crimes de invasão de dispositivo informático e de extorsão, absorvido este pela regra da consunção, sem que exista, na legislação penal, uma figura típica que capture a especificidade técnica do sequestro de dados e da exigência de resgate em criptoativos (GOMES; NUNES; WILMERS, 2020). No mesmo sentido, a literatura recente destaca os desafios da tipificação penal do chamado sequestro digital no Brasil (CARVALHO, 2024).

Complementarmente, como o *ransomware* combina a invasão do dispositivo com a posterior exigência de resgate, é indispensável analisar também o tipo penal de extorsão (art. 158 do Código Penal), ao qual a conduta é enquadrada por concurso aparente de normas, resolvido pela consunção. A pena cominada ao crime de extorsão sensivelmente mais grave que a prevista para a invasão de dispositivo informático mesmo após a Lei nº 14.155/2021 é o que, na prática, tem levado parte da doutrina a sustentar que a conduta de *ransomware* deveria ser processada preponderantemente sob esse tipo penal, com a invasão absorvida como crime-meio, ainda que tal solução, por depender de construção doutrinária e jurisprudencial, não ofereça o mesmo grau de segurança jurídica que uma tipificação penal específica proporcionaria.

3.3 Marco Civil da Internet e LGPD como reforço processual e preventivo

Ainda que não tipifiquem condutas penais, a Lei nº 12.965/2014 (Marco Civil da Internet) e a Lei nº 13.709/2018 (LGPD) cumprem papel relevante na investigação e na prevenção de ataques de *ransomware* (BRASIL, 2014; BRASIL, 2018). O Marco Civil disciplina a guarda de registros de conexão e de acesso a aplicações por provedores, viabilizando, mediante ordem judicial, a obtenção de *logs* que auxiliam na reconstrução da cadeia de eventos de um ataque e na identificação de pontos de comprometimento inicial. A LGPD, por sua vez, impõe às organizações vítimas de incidentes de segurança o dever de notificar a Autoridade Nacional de Proteção de Dados e os titulares afetados em caso de vazamento de dados pessoais, obrigação especialmente relevante nos ataques de dupla extorsão, em que os criminosos ameaçam divulgar publicamente informações exfiltradas antes da criptografia.

Some-se a isso o regramento da cadeia de custódia da prova digital, introduzido nos arts. 158-A a 158-F do Código de Processo Penal pela Lei nº 13.964/2019 (Pacote Anticrime), que estabelece o rito de reconhecimento, coleta, acondicionamento e preservação de vestígios eletrônicos, etapa central para que a prova obtida em um servidor comprometido ou em um dispositivo criptografado seja considerada válida em juízo (BRASIL, 2019).

3.4 Projetos de lei específicos em tramitação

A insuficiência do art. 154-A para capturar a especificidade do *ransomware* tem impulsionado, nos últimos anos, diferentes iniciativas legislativas voltadas à criação de um tipo penal autônomo. O Projeto de Lei nº 879/2022, de autoria do senador Carlos Viana, propõe a inclusão de tipo penal específico para o bloqueio de dados e o *ransomware*, cominando pena de três a seis anos de reclusão e multa para quem invade dispositivos ou redes para bloquear arquivos, pena que sobe para quatro a oito anos quando comprovada a exigência de resgate para a devolução do acesso; o projeto ainda prevê aumento de um terço a metade da pena quando o crime é praticado contra órgão público (BRASIL, 2022a).

Em sentido semelhante, o Projeto de Lei nº 1.049/2022, do senador Angelo Coronel, já aprovado pela Comissão de Comunicação e Direito Digital do Senado e em tramitação com urgência na Comissão de Constituição e Justiça, propõe inserir no Código Penal o crime de extorsão digital, descrito como a invasão de computadores e celulares e o bloqueio do acesso do proprietário como meio de constrangê-lo a pagar resgate, cominando pena de dois a cinco anos de reclusão e multa (BRASIL, 2022b).

A permanência dessas propostas em tramitação, sem conversão em lei até o presente momento, reforça a tese central deste artigo: o ordenamento jurídico brasileiro ainda não dispõe de resposta penal proporcional à especificidade técnica e econômica do *ransomware*, o que produz reflexos diretos sobre os desafios enfrentados pela investigação criminal. Estudo recente sobre *ransomware* e infraestruturas críticas, construído a partir do caso Colonial Pipeline, também aponta a existência de um vazio legal penal no Brasil quanto a essa modalidade delitiva (NEPOMUCENO, 2025).

4 DESAFIOS DA INVESTIGAÇÃO CRIMINAL DO RANSOMWARE

4.1 Prova digital e cadeia de custódia

A investigação do *ransomware* enfrenta, em primeiro lugar, uma dificuldade que lhe é estrutural: a prova do crime existe apenas em meio digital, e esse meio é, por natureza, instável. Diferentemente das evidências do mundo físico, os vestígios de um ataque cibernético podem ser apagados, alterados ou sobrescritos com facilidade, seja pela própria ação do criminoso que costuma eliminar *logs* e rastros de acesso após a consumação do delito, seja pela própria vítima, que ao tentar restaurar o sistema comprometido pode inadvertidamente destruir evidências relevantes para a perícia.

Esse cenário reforça a importância central das regras de cadeia de custódia da prova digital. O reconhecimento, a coleta e o acondicionamento adequados de um servidor comprometido, de discos criptografados ou de registros de acesso são o que permite, mais adiante, que a prova obtida resista ao contraditório processual. Somese a isso um problema temporal característico do *ransomware*: como observado por Santos Filho e Furlan (2021), o dano no mundo virtual muitas vezes não é percebido de imediato pela vítima como ocorre no mundo físico, o que faz com que evidências relevantes já tenham se perdido no momento em que a investigação é iniciada. A doutrina e a jurisprudência recentes tratam a cadeia de custódia como garantia associada à confiabilidade da prova digital (MONTEIRO, 2026).

Nesse contexto, a perícia forense computacional assume papel central e distinto daquele exercido na investigação de crimes convencionais: não basta identificar o resultado do ataque (o bloqueio ou a criptografia dos dados), mas é necessário reconstruir toda a cadeia de eventos, o vetor de invasão, a movimentação dentro da rede, o momento exato da criptografia para viabilizar tanto a atribuição de autoria quanto a eventual recuperação dos dados sequestrados. A literatura técnica internacional reforça essa premissa: a revisão de fundamentos científicos conduzida pelo NIST considera as técnicas de investigação digital confiáveis quando adequadamente aplicadas, mas ressalva que nem toda evidência pode ser descoberta, que a recuperação de arquivos apagados pode trazer material estranho ao fato e que a atualização de softwares pode alterar o significado dos artefatos digitais (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2022).

4.2 Identificação de autoria e rastreamento de criptoativos

O segundo grande desafio da investigação do *ransomware* está na identificação de quem efetivamente praticou o crime, problema que se agrava significativamente pelo uso de criptoativos como meio de pagamento do resgate. O pagamento em criptomoedas não representa anonimato absoluto todas as transações ficam registradas de forma pública no *blockchain*, mas a ausência de vinculação direta entre as chaves públicas utilizadas e a identidade real de seus titulares torna a atribuição de autoria uma tarefa tecnicamente complexa, a ponto de o crime de *ransomware* ser recorrentemente descrito na literatura especializada como um "crime quase perfeito" (GOMES; NUNES; WILMERS, 2020).

Gomes, Nunes e Wilmers (2020) explicam que a identificação do criminoso permanece possível em duas hipóteses principais: quando há descuido do agente na ocultação de seu endereço IP, e no momento da conversão dos criptoativos em moeda convencional, etapa que geralmente exige a utilização de uma corretora de câmbio sujeita a regulação e, portanto, ao dever de identificação de seus usuários. Essa segunda hipótese, contudo, vem sendo sistematicamente contornada por criminosos mais sofisticados por meio de serviços de *mixing*, que consistem em misturar os criptoativos de diversos usuários entre si, embaralhando a relação entre remetente e destinatário e dificultando sem necessariamente eliminar a rastreabilidade da transação original, prática que pode caracterizar, adicionalmente, o crime de lavagem de dinheiro.

Some-se a isso a instabilidade dos próprios vetores de identificação técnica: o IP de um dispositivo, embora seja apontado como espécie de "impressão digital" capaz de indicar a origem de um acesso, pode ser mascarado por criminosos com relativa facilidade, exigindo dos investigadores brasileiros conhecimento técnico que vai muito além da formação jurídica tradicional. A literatura internacional converge quanto a essas limitações: revisão sobre o estado da arte da forense de criptomoedas indica que a área ainda se ressente de técnicas forenses mais robustas e de maior coordenação entre agências (DUDANI et al., 2023). No cenário brasileiro, revisão da literatura científica publicada entre 2019 e 2025 sobre técnicas de investigação forense de *blockchain* e criptomoedas volta-se justamente a orientar a atuação da Polícia Judiciária (QUEIROZ RODRIGUES; SANTOS, 2026).

4.3 Transnacionalidade e cooperação internacional

O terceiro eixo de desafios decorre da natureza intrinsecamente transnacional do *ransomware*. Diferentemente de crimes tradicionais, em que o princípio da territorialidade oferece um critério relativamente estável para a definição de jurisdição e competência, o ataque de *ransomware* pode ser planejado em um país, executado por meio de servidores localizados em um segundo país, contra uma vítima situada em um terceiro, com o resgate sendo convertido em uma corretora de criptoativos sediada em um quarto cenário que, segundo Gomes, Nunes e Wilmers (2020), instaura não apenas um conflito de jurisdição, mas também de aplicação da lei penal no espaço.

Essa característica torna a cooperação internacional elemento indispensável e, ao mesmo tempo, um dos pontos mais frágeis da persecução penal do *ransomware* brasileiro. Instrumentos como a Convenção de Budapeste sobre Crimes Cibernéticos, da qual o Brasil é signatário, buscam justamente facilitar esse tipo de cooperação entre autoridades de diferentes países, mas sua efetividade prática depende da adesão e da celeridade de Estados que, muitas vezes, servem de base operacional para os próprios grupos criminosos. As avaliações da Europol sobre a criminalidade organizada na internet igualmente destacam a importância da cooperação entre autoridades e com o setor privado para o enfrentamento de ameaças como o *ransomware* (EUROPOL, 2025).

A esse quadro se somam problemas de ordem interna. Santos Filho e Furlan (2021) apontam que a morosidade na expedição e no cumprimento de mandados, a falta de celeridade pericial e a insuficiente integração entre as forças de segurança pública comprometem a efetividade da investigação mesmo quando não há obstáculo transnacional algum.

4.4 O desafio da tipificação e o princípio da legalidade estrita

Para além dos obstáculos propriamente técnicos analisados nas subseções anteriores, a investigação e a persecução penal do *ransomware* enfrentam um desafio de natureza dogmática: a ausência de tipificação penal autônoma impõe ao aplicador do Direito a tarefa de enquadrar uma conduta tecnicamente sofisticada que combina invasão, criptografia e extorsão dentro de tipos penais pensados para realidades distintas, o que tensiona o princípio da legalidade estrita (art. 5º, XXXIX, da Constituição Federal, e art. 1º do Código Penal), segundo o qual não há crime sem lei anterior que o defina (BRASIL, 1988; BRASIL, 1940).

Essa tensão se manifesta de forma concreta na própria controvérsia doutrinária: se o *ransomware* é resolvido pela absorção do crime de invasão de dispositivo informático pelo crime de extorsão, ou se, ao contrário, subsiste concurso material de crimes, a resposta não é unânime na doutrina penal brasileira, o que gera insegurança jurídica tanto para a acusação quanto para a defesa e, em última análise, para a própria vítima.

A ausência de tipo penal específico também repercute na fase investigativa propriamente dita, na medida em que a qualificação jurídica provisória dada ao fato no boletim de ocorrência ou no inquérito policial determina, na prática, quais medidas cautelares poderão ser requeridas, qual autoridade policial será competente e qual será o prazo prescricional aplicável, com impacto direto sobre a celeridade e a efetividade da resposta estatal ao ataque.

5 A JURISPRUDÊNCIA DO STJ SOBRE PROVA DIGITAL E CADEIA DE CUSTÓDIA

Embora os tribunais superiores brasileiros ainda não tenham firmado precedente específico sobre a tipificação penal do *ransomware*, o Superior Tribunal de Justiça já consolidou entendimento relevante sobre a validade da prova digital em geral entendimento diretamente aplicável à investigação do *ransomware*, na medida em que praticamente toda a prova de autoria e materialidade desse crime é, por definição, digital.

Um primeiro grupo de precedentes trata do critério para reconhecimento da nulidade da prova digital por quebra da cadeia de custódia, a Sexta Turma do STJ, no julgamento do AgRg no RHC 147.885/SP, firmou-se o reconhecimento da nulidade da prova digital por quebra da cadeia de custódia, nos seguintes termos:

> "A quebra da cadeia de custódia não gera nulidade automática da prova, mas apenas a torna potencialmente imprestável, exigindo-se a demonstração de efetivo prejuízo ou de concreto risco de adulteração para que a prova seja excluída dos autos" (STJ, AgRg no RHC 147.885/SP).

Esse entendimento foi reafirmado em outros julgados mais recentes, como o AgRg no HC 958.288/SP e o HC 978.953/PE, ambos da Sexta Turma, vejamos:

> "Demonstração concreta de adulteração ou comprometimento do iter probatório, não bastando ilações genéricas ou parecer técnico unilateral" (AgRg no HC 958.288/SP; HC 978.953/PE).

Esse critério, contudo, não afasta a possibilidade de nulidade quando a falha na preservação da prova é de tal magnitude que impossibilita qualquer verificação de sua integridade. Em julgamento amplamente noticiado, a Sexta Turma do STJ concedeu *habeas*

corpus para determinar a exclusão de conversas de aplicativo de mensagens utilizadas para fundamentar a condenação de um policial civil por corrupção passiva, sob o fundamento de que a ausência de apreensão e perícia do dispositivo de origem tornava a prova impossível de ser auditada, repetida ou reproduzida. Em sentido semelhante, a mesma Sexta Turma, ao apreciar caso de organização criminosa e homicídio, determinou a realização de perícia oficial em celulares apreendidos diante de dúvida razoável sobre a integridade do material.

Esses precedentes, tomados em conjunto, permitem extrair um critério aplicável diretamente à investigação do *ransomware*: a mera inobservância formal de uma das etapas da cadeia de custódia previstas no art. 158-B do Código de Processo Penal não conduz automaticamente à nulidade da prova, mas a ausência de qualquer possibilidade de verificação técnica da integridade do vestígio digital compromete de forma definitiva a validade da prova (BRASIL, 1941).

6 CONSIDERAÇÕES FINAIS

O presente artigo teve como objetivo analisar os desafios enfrentados pela investigação criminal do *ransomware* no ordenamento jurídico brasileiro, partindo da hipótese de que os instrumentos normativos e operacionais atualmente disponíveis são insuficientes para garantir, de forma plena, a identificação de autoria, a preservação da prova e a responsabilização penal dos infratores. Os resultados da pesquisa confirmam essa hipótese, ainda que de forma qualificada.

Do ponto de vista dogmático, ficou demonstrado que o Brasil ainda não dispõe de tipo penal específico para o *ransomware*, sendo a conduta enquadrada, por construção doutrinária e jurisprudencial ainda não pacificada, no crime de extorsão (art. 158 do Código Penal) em concurso aparente com a invasão de dispositivo informático (art. 154-A), absorvida pela regra da consunção. Essa lacuna normativa gera insegurança jurídica que se propaga por toda a cadeia da persecução penal.

Do ponto de vista processual, a pesquisa evidenciou que as regras de cadeia de custódia da prova digital, introduzidas pelo Pacote Anticrime, representam avanço normativo relevante, mas cuja efetividade depende de uma cultura investigativa e pericial ainda em consolidação no Brasil. A análise da jurisprudência do STJ revelou que os tribunais superiores adotam critério equilibrado a nulidade da prova não decorre de toda e qualquer falha formal, mas apenas

daquelas que comprometem, de modo irremediável, a possibilidade de verificação técnica da integridade do vestígio.

Do ponto de vista investigativo propriamente dito, o estudo confirmou que o uso de criptoativos como meio de pagamento do resgate constitui o principal obstáculo à identificação de autoria, não por conferir anonimato absoluto, mas por dificultar, por meio de técnicas como o *mixing*, a vinculação entre as chaves públicas utilizadas na transação e a identidade real de seus titulares. Os casos analisados, contudo, demonstram que essa dificuldade não é intransponível quando há cooperação institucional qualificada.

Por fim, a pesquisa confirmou que a transnacionalidade é talvez o traço mais estrutural do *ransomware* contemporâneo, exigindo respostas que extrapolam a capacidade de qualquer sistema de justiça criminal isolado. Nesse sentido, a aprovação de um tipo penal específico para o *ransomware* seja pela via do PL nº 879/2022, seja pela via do PL nº 1.049/2022 representaria avanço normativo relevante, mas insuficiente se não acompanhado do fortalecimento da perícia digital, da modernização dos instrumentos de rastreamento de criptoativos e do aprofundamento de mecanismos de cooperação internacional, a exemplo da Convenção de Budapeste. Fica como sugestão para pesquisas futuras o acompanhamento da tramitação legislativa desses projetos de lei e a análise empírica, à medida que se consolidar, da jurisprudência brasileira que venha a tratar especificamente da tipificação penal do *ransomware*.

REFERÊNCIAS

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

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Rio de Janeiro, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decretolei/del2848compilado.htm. Acesso em: 14 set. 2026.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Rio de Janeiro, 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 14 set. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 set. 2026.

BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019**. Pacote Anticrime. Brasília, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato20192022/2019/lei/l13964.htm. Acesso em: 14 set. 2026.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021.** Brasília, 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 14 set. 2026.

CANALTECH. **Bloqueio de dados e ransomware podem ser incluídos no Código Penal**. 2022. Disponível em: https://canaltech.com.br/seguranca/bloqueio-de-dadose-ransomware-podem-ser-incluidos-no-codigo-penal-240248/. Acesso em: 14 set. 2026.

CANALTECH. Projeto de lei busca criminalizar o golpe com ransomware no **Brasil.** 2022. Disponível em: https://canaltech.com.br/seguranca/ransonwareprojeto-de-lei-busca-criminizalizar-o-golpe-virtual-no-brasil-215481/. Acesso em: 14 set. 2026.

CARVALHO, Claudia da Costa Bonard de. **Desafios na tipificação penal do sequestro digital (ransomware)**. Boletim IBCCRIM, v. 32, n. 383, 2024. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1221/1070. Acesso em: 27 out. 2026.

CONJUR. **Dúvida sobre custódia da prova digital deve ser resolvida por perícia, diz STJ**. 2026. Disponível em: https://www.conjur.com.br/?p=890039. Acesso em: 14 set. 2026.

CONJUR. **Prova digital é nula se não preservar formas de testar confiabilidade, diz STJ. 2025**. Disponível em: https://www.conjur.com.br/?p=840974. Acesso em: 14 set. 2026.

CONVERGÊNCIA DIGITAL. **Senado quer cinco anos de prisão para ataques de ransomware.** 2022. Disponível em: https://convergenciadigital.com.br/?p=27322. Acesso em: 14 set. 2026.

DUDANI, S. et al. **The current state of cryptocurrency forensics**. Forensic Science International: Digital Investigation, v. 46, 301576, 2023. DOI: 10.1016/j.fsidi.2023.301576. Acesso em: 29 out. 2026.

EUROPOL. **Steal, deal and repeat: how cybercriminals trade and exploit your data**: Internet Organised Crime Threat Assessment (IOCTA) 2025. Luxembourg: Publications Office of the European Union, 2025. DOI: 10.2813/4926508. Acesso em: 29 out. 2026.

EVINIS TALON. STJ define quando ocorre a quebra da cadeia de custódia. 2022. Disponível em: https://evinistalon.com/?p=22310. Acesso em: 14 set. 2026.

FELSBERG ADVOGADOS. **Nova lei criminaliza o "sequestro" de dados digitais em troca de pedido de liberação.** 2021. Disponível em: https://www.felsberg.com.br/nova-lei-criminaliza-o-sequestro-de-dados-digitais-emtroca-de-pedido-de-liberacao/. Acesso em: 14 set. 2026.

GOMES, Luiz Eduardo dos Santos Pereira; NUNES, Luana Esteche; WILMERS, Michael Felipe. **Natureza jurídica do crime de ransomware e a utilização da criptomoeda como meio de impunidade**. Revista da Escola Superior do Ministério Público do Ceará, Fortaleza, ano 12, n. 2, p. 213-234, jul./dez. 2020.

MIGALHAS. **A ameaça de ransomware e os caminhos para enfrentá-la.** 2022. Disponível em: https://www.migalhas.com.br/depeso/352666/a-ameaca-deransomware-e-os-caminhos-para-enfrenta-la. Acesso em: 14 set. 2026.

MIGALHAS. **Cadeia de custódia como garantia constitucional**. 2026. Disponível em: https://www.migalhas.com.br/depeso/450354/cadeia-de-custodia-como-garantiaconstitucional. Acesso em: 14 set. 2026.

MONTEIRO, Washington Ramos. **Cadeia de custódia e prova digital: garantismo e jurisprudência**. [S. l.], 2026. Disponível em: https://arq.migalhas.com.br/arquivos/2026/1/1a83230d05fdda_cadeiadecustodiaeprovadigital.pdf. Acesso em: 27 out. 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Digital investigation techniques: a NIST scientific foundation review**. Gaithersburg: NIST, 2022. (NIST Internal Report, 8354). DOI: 10.6028/NIST.IR.8354. Disponível em: https://doi.org/10.6028/NIST.IR.8354. Acesso em: 29 out. 2026.

NEPOMUCENO, Ana Manuela Oliveira. **Ransomware e infraestruturas críticas: análise sobre o vazio legal penal no Brasil a partir do caso Colonial Pipeline**. [S. l.], 2025. Disponível em: https://repositorio.idp.edu.br/server/api/core/bitstreams/9bd2f4d0-5a38-4b00-adb3f0c41bf7cc96/content. Acesso em: 27 out. 2026.

QUEIROZ RODRIGUES, Cleyl Anderson de; SANTOS, Sérgio Luís Oliveira dos. **Técnicas de investigação forense em blockchain e criptomoedas: revisão da literatura para aplicação em investigações criminais**. 2026. Trabalho de Conclusão de Curso (Especialização em Inteligência e Inovação no Enfrentamento ao Crime Organizado) – Universidade Federal de Santa Catarina, Florianópolis, 2026. Disponível em: https://repositorio.ufsc.br/handle/123456789/272899. Acesso em: 29 out. 2026.

SANTOS FILHO, Justino Soares dos; FURLAN, Fernando Palma Pimenta. **Crimes virtuais: uma abordagem jurídica acerca das limitações no combate aos crimes cibernéticos.** Conteúdo Jurídico, 2021. Acesso em: 14 set. 2026.

SENADO FEDERAL. **Comissão de Comunicação e Direito Digital. Parecer sobre proposta de tipificação do ransomware**. Brasília, 2022. Acesso em: 14 set. 2026.

WAKKA, Wagner. **Brasil é o 2º país com mais ameaças de ransomware no mundo, aponta estudo**. Canaltech, 2019. Disponível em: https://canaltech.com.br/seguranca/brasil-e-o-20-pais-com-mais-ameacas-deransomware-no-mundo-aponta-estudo-134683/. Acesso em: 14 set. 2026.