

A Criminalização da Invasão de Dispositivo Informático no Brasil: Tipicidade, Prova Digital e Proteção de Dados Após as Reformas de 2021 e 2023

Gustavo Henrique de Andrade Cordeiro*

Centro Universitário Eurípides de Marília (UNIVEM), Brasil.

<https://orcid.org/0000-0002-4035-1628>

Resumo: O artigo examina a criminalização da invasão de dispositivo informático no direito penal brasileiro, tendo por objeto o artigo 154-A do Código Penal e as transformações trazidas pela Lei n. 14.155/2021 e pela promulgação da Convenção de Budapeste, em 2023. O problema que orienta a investigação consiste em saber como compatibilizar a tutela penal reformada com a confiabilidade da prova digital e com o regime de proteção de dados pessoais, sem sacrificar garantias fundamentais. Adota-se o método dedutivo, partindo de premissas constitucionais e dogmáticas para conclusões específicas sobre o tipo penal, sua aplicação probatória e sua articulação normativa. A pesquisa é qualitativa, de natureza bibliográfica, documental, normativa e jurisprudencial, amparada em legislação vigente, doutrina nacional e estrangeira e julgados dos tribunais superiores posteriores à reforma de 2021. Os resultados indicam que a reforma de 2021 ampliou o alcance do tipo e suprimiu a exigência de violação de mecanismo de segurança, deslocando o problema para o terreno da prova, e que a jurisprudência do Superior Tribunal de Justiça já atribuiu ao Estado o ônus de comprovar a integridade da cadeia de custódia digital. Defende-se que a efetividade da tutela depende da aplicação sistemática desse critério, articulada à leitura integrada entre o direito penal e a proteção de dados, sob o filtro da proporcionalidade. A confiabilidade da prova e a contenção dogmática do tipo surgem, ao final, como condições de legitimidade dessa tutela no Estado Democrático de Direito.

Palavras-chave: *Crimes informáticos. Prova digital. Cadeia de custódia. Proteção de dados pessoais. Garantias fundamentais.*

* Doutor em Direito pela Instituição Toledo de Ensino (ITE). E-mail: gustavomqv@hotmail.com.



UNIVERSIDADE FEDERAL DA PARAÍBA

Programa de Pós-Graduação em Ciências Jurídicas

DOI: <https://doi.org/10.22478/ufpb.1678-2593.2026v25n58.79171>

A Criminalização da Invasão de Dispositivo Informático no Brasil: Tipicidade, Prova Digital e Proteção de Dados Após as Reformas de 2021 e 2023

Gustavo Henrique de Andrade Cordeiro

INTRODUÇÃO

A digitalização da vida cotidiana redefiniu o que significa guardar um segredo. Dados financeiros, registros de saúde, conversas privadas e arquivos profissionais migraram para dispositivos conectados, de modo que o acesso não autorizado a um único aparelho pode hoje expor camadas inteiras da existência de uma pessoa. Essa concentração informacional confere aos dispositivos informáticos um valor que ultrapassa o econômico e alcança a própria personalidade do indivíduo. Não surpreende, portanto, que a violação desses sistemas tenha deixado de ser um problema marginal para se tornar uma das frentes mais sensíveis da política criminal contemporânea.

A resposta penal brasileira a esse fenômeno, contudo, nasceu tardia e permanece em movimento. O tipo penal da invasão de dispositivo informático, introduzido em 2012, foi substancialmente reformulado em 2021, e o país aderiu à principal convenção internacional sobre o tema apenas em 2023. Diante desse arranjo normativo em transformação, coloca-se a questão central deste estudo: de que modo a tutela penal da invasão de dispositivo informático, tal como reformada, pode ser efetivada sem comprometer a confiabilidade da prova digital e os direitos fundamentais dos

investigados? A pergunta importa porque a existência do tipo, isoladamente, nada garante quanto à sua aplicação legítima.

O objetivo geral consiste em analisar a criminalização da invasão de dispositivo informático no ordenamento brasileiro à luz das reformas recentes, articulando dogmática penal, prova digital e proteção de dados. Como objetivos específicos, busca-se examinar a estrutura do tipo penal e os efeitos da Lei n. 14.155/2021; investigar os desafios da prova digital e da cadeia de custódia na persecução penal; e avaliar a relação entre o art. 154-A do Código Penal e o regime de proteção de dados pessoais, identificando os limites constitucionais da atuação estatal.

Quanto à metodologia, adota-se o método dedutivo, que parte de premissas gerais de matriz constitucional e dogmática para alcançar conclusões específicas sobre o objeto. A pesquisa é qualitativa e de natureza bibliográfica, documental, normativa e jurisprudencial, com caráter analítico e propositivo. Recorre-se à legislação vigente, à doutrina nacional e estrangeira veiculada em obras especializadas e periódicos qualificados, bem como a julgados do Superior Tribunal de Justiça e do Supremo Tribunal Federal pertinentes à prova digital e à proteção de dados.

A tipificação penal ocupa a abertura do artigo. Reconstrói-se o bem jurídico protegido, situa-se o delito no sistema do Código Penal e analisa-se a reforma de 2021, que elevou as penas e, sobretudo, suprimiu do caput a exigência de violação de mecanismo de segurança. Essa alteração, longe de ser meramente redacional, redesenha o âmbito de incidência do tipo e reabre o debate sobre os limites da intervenção penal no ambiente digital.

Na sequência, desloca-se o foco da norma para a prova. A materialidade dos crimes informáticos repousa em vestígios intangíveis e voláteis, cuja confiabilidade depende de procedimentos técnicos rigorosos. Discutem-se a cadeia de custódia introduzida pela

Lei n. 13.964/2019, o seu fundamento constitucional quando aplicada a dados digitais, os obstáculos de autoria e de cooperação internacional e a jurisprudência do Superior Tribunal de Justiça formada após a reforma de 2021 sobre o ônus da prova da integridade digital.

Por fim, o regime de proteção de dados integra as duas perspectivas anteriores. Sustenta-se que a tutela penal da invasão informática não pode ser lida isoladamente, mas em diálogo com a proteção de dados pessoais e com o direito à autodeterminação informativa. Examina-se como a eficiência investigativa, que reclama acesso a dados, deve submeter-se aos princípios da finalidade, da necessidade e da proporcionalidade.

A contribuição que se pretende oferecer está menos na descrição do tipo penal, já bastante percorrida, e mais na sua releitura à luz das reformas de 2021 e 2023 e do encontro entre direito penal, processo penal e proteção de dados. Trata-se de propor parâmetros para uma tutela ao mesmo tempo eficaz e constitucionalmente contida, em um campo no qual a tentação do excesso e o risco da impunidade caminham lado a lado.

2 A TIPIFICAÇÃO PENAL DA INVASÃO DE DISPOSITIVO INFORMÁTICO: DO TIPO DE 2012 À REFORMA DE 2021

A necessidade de adequar o direito penal a um ambiente em que a lesão a bens jurídicos passou a operar por meios eletrônicos explica a criminalização da invasão de dispositivo informático. Antes de descrever a estrutura do tipo, convém compreender qual interesse a norma protege e por que o legislador optou por uma intervenção autônoma. O bem jurídico tutelado, a transformação do tipo pela reforma de 2021 e os princípios que devem conter a expansão do direito penal informático organizam, nessa ordem, o que se segue.

2.1 Bem jurídico tutelado e inserção sistemática no Código Penal

O artigo 154-A foi inserido na Seção IV do Capítulo VI do Título I da Parte Especial do Código Penal, dedicada aos crimes contra a inviolabilidade dos segredos. Essa topografia não é acidental: o legislador associou a invasão informática à proteção da liberdade individual, e em especial da intimidade e da vida privada, bens assegurados pelo artigo 5º, inciso X, da Constituição da República (BRASIL, 1988). A localização sistemática orienta a interpretação do tipo e afasta leituras que o reduziriam a mera tutela patrimonial.

A doutrina especializada em proteção de dados oferece um quadro mais preciso desse interesse. Doneda (2019) demonstra que a privacidade evoluiu de uma pretensão de exclusão, traduzida na fórmula do direito a ser deixado só, para um poder de controle sobre as próprias informações. Essa mudança qualitativa desloca o foco do isolamento para a gestão dos dados pessoais, o que repercute diretamente sobre o conteúdo de ilicitude da invasão informática, agora compreendida como ofensa à esfera de domínio informacional do titular.

No mesmo sentido, Mendes (2018) sustenta que a Constituição brasileira abriga, ainda que de forma implícita, um direito fundamental à autodeterminação informativa, compreendido como a faculdade de o indivíduo decidir sobre a coleta e o uso de seus dados. Quando alguém invade um dispositivo alheio, não viola apenas um espaço físico simbólico, mas subtrai ao titular o controle sobre informações que o constituem como pessoa. A invasão, sob essa ótica, é uma forma de expropriação informacional.

A perspectiva comparada reforça esse entendimento. Rodotà (2008) já advertia que, na sociedade da vigilância, a tutela da privacidade não se esgota na proteção de espaços íntimos, mas se

projeta sobre o fluxo permanente de dados que descreve a vida das pessoas. Em registro mais recente, Zuboff (2019) descreve um modelo econômico assentado na extração massiva de dados comportamentais, no qual o acesso não autorizado a dispositivos integra uma cadeia mais ampla de apropriação informacional. O bem jurídico protegido pelo art. 154-A insere-se, portanto, em um debate que extrapola as fronteiras nacionais.

Disso decorre uma consequência dogmática relevante. Se o interesse tutelado é a autodeterminação informativa, e não apenas o sigilo de um conteúdo específico, a gravidade da conduta deve ser medida pela intensidade da perda de controle imposta ao titular, e não exclusivamente pelo valor econômico do que foi acessado. Essa premissa, como se verá, é decisiva para avaliar a reforma de 2021 e a graduação das penas prevista nos parágrafos do dispositivo.

Convém registrar que o bem jurídico assim delineado comporta dupla dimensão. Há um aspecto individual, ligado ao controle de cada titular sobre seus dados, e um aspecto coletivo, relativo à confiança social na integridade dos sistemas informáticos. Esse segundo aspecto explica por que o legislador previu formas qualificadas quando a invasão atinge a administração pública ou serviços de interesse coletivo: a lesão, nesses casos, transcende o indivíduo e compromete a própria infraestrutura informacional da sociedade.

O dispositivo admite, ainda, a pessoa jurídica como sujeito passivo, na medida em que dados empresariais e segredos industriais também integram a esfera protegida. Tal amplitude, no entanto, não desnatura o núcleo do injusto, que permanece ancorado na tutela informacional. A identificação precisa do interesse protegido, antes de ser exercício teórico, condiciona a correta delimitação das condutas típicas e a dosimetria proporcional da pena, evitando que a sanção se descole da efetiva gravidade da lesão.

A evolução histórica do bem jurídico ajuda a compreender a

opção legislativa. Os tipos penais clássicos de proteção do segredo, concebidos para correspondências e comunicações em suporte físico, mostraram-se incapazes de abarcar a realidade dos dados eletrônicos. A criação de uma figura autônoma respondeu a essa insuficiência, reconhecendo que a informação digital ostenta valor próprio e que a sua violação produz lesão qualitativamente distinta daquela prevista nas figuras tradicionais. O art. 154-A é, nesse sentido, expressão de uma adaptação necessária do sistema penal às novas formas de agressão.

Não se trata, porém, de tutelar a tecnologia em si, mas a pessoa por trás dos dados. Mendes (2018) adverte que a autodeterminação informativa não protege o dado pela sua materialidade, e sim o indivíduo que nele se projeta. Essa precisão evita um equívoco comum, o de tratar o crime informático como ofensa a coisas, quando o que está em jogo é a liberdade do titular de governar a própria identidade informacional. A correta compreensão do interesse protegido é, por isso, condição de uma interpretação constitucionalmente adequada do tipo.

2.2 A estrutura típica e a reforma da Lei n. 14.155/2021

Introduzido pela Lei n. 12.737/2012, conhecida como Lei Carolina Dieckmann, o artigo 154-A exigia, em sua redação original, para a configuração do crime, a invasão de dispositivo mediante violação indevida de mecanismo de segurança, com pena de detenção de três meses a um ano (BRASIL, 2012). A exigência de superação de uma barreira de proteção funcionava como elemento delimitador, restringindo a tipicidade às condutas que efetivamente vencessem salvaguardas técnicas.

Esse desenho foi profundamente alterado pela Lei n. 14.155/2021, que entrou em vigor em 28 de maio de 2021 e reescreveu o caput do dispositivo. O tipo penal passou a ter a seguinte redação:

Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: Pena - reclusão, de 1 (um) a 4 (quatro) anos, e multa (BRASIL, 2021).

Duas modificações se destacam. A primeira é o agravamento da resposta penal: a pena, antes de detenção de três meses a um ano, tornou-se de reclusão de um a quatro anos, retirando o delito do rol das infrações de menor potencial ofensivo e afastando institutos como a transação penal. A segunda, de maior densidade dogmática, é a supressão da expressão violação indevida de mecanismo de segurança do núcleo do tipo. A reforma substituiu a fórmula dispositivo informático alheio por dispositivo informático de uso alheio, ampliando o alcance da norma.

A consequência é significativa. Sob a redação original, o acesso a um dispositivo desprovido de senha ou de qualquer barreira poderia escapar à tipicidade, justamente por inexistir mecanismo de segurança a ser violado. Com a nova redação, o elemento decisivo passa a ser a ausência de autorização, expressa ou tácita, do usuário, e não mais a superação de uma proteção técnica. O tipo tornou-se, nesse ponto, mais abrangente, deslocando o centro de gravidade da ilicitude da técnica empregada para o consentimento do titular.

A reforma também reorganizou as figuras qualificadas e as causas de aumento. Mantiveram-se a equiparação da conduta de quem produz ou difunde programas destinados à invasão, o aumento de pena quando da invasão resulta prejuízo econômico e a forma qualificada para os casos de obtenção de conteúdo de comunicações privadas, segredos comerciais ou informações sigilosas, com pena de reclusão de dois a cinco anos. Essa graduação, como observado, dialoga com a ideia de que a censura penal deve ser proporcional à

intensidade da lesão informacional.

É precisamente nesse ponto que o artigo objeto de releitura crítica revela a defasagem das análises que ainda se apoiam na redação de 2012. Discutir o art. 154-A sem incorporar a supressão do elemento de segurança e o novo patamar de penas significa descrever um tipo penal que não está mais em vigor. A atualização não é detalhe formal, mas condição de correção dogmática, sobretudo porque, sendo a nova lei mais gravosa, suas disposições somente alcançam condutas praticadas a partir de sua vigência, por força do artigo 5º, inciso XL, da Constituição (BRASIL, 1988).

A nova fórmula dispositivo informático de uso alheio merece atenção interpretativa. Ela abarca situações em que o agente acessa dados hospedados em servidores de terceiros ou em ambientes de armazenamento em nuvem utilizados pela vítima, ainda que o equipamento físico não lhe pertença. Assim, quem obtém credenciais e acessa o backup de um usuário em servidor remoto pratica a conduta típica, mesmo sem violar o aparelho pessoal da vítima. A reforma, nesse sentido, ajustou o tipo à arquitetura distribuída da computação contemporânea, em que os dados raramente residem em um único dispositivo.

No plano processual, a Lei n. 14.155/2021 preservou, como regra, a ação penal pública condicionada à representação, prevista no art. 154-B, ressalvada a hipótese de crime contra a administração pública, em que a ação é incondicionada. O Superior Tribunal de Justiça, ao interpretar a exigência de representação, tem dispensado rigor formal, bastando a demonstração inequívoca do interesse da vítima na persecução. Essa orientação concilia a tutela penal com o respeito à autonomia do ofendido, especialmente sensível quando a própria investigação pode reexpor o conteúdo já violado.

A supressão do elemento de segurança suscita, ainda, um debate sobre o consentimento. Se a tipicidade passa a depender da

ausência de autorização do usuário, ganham relevo as situações de autorização tácita, de revogação de consentimento e de acesso por quem outrora fora autorizado. O técnico que, autorizado a reparar um equipamento, extrapola os limites do consentimento e acessa arquivos pessoais pratica conduta típica, pois a autorização não abrangia aquela finalidade. A delimitação do alcance do consentimento torna-se, assim, questão central na aplicação do tipo reformado.

Persiste, por outro lado, a inexistência de modalidade culposa. A invasão de dispositivo informático exige dolo, de modo que a destruição acidental de dados, por imperícia ou negligência de um prestador de serviços, não configura o crime, ainda que possa gerar responsabilidade civil. Essa opção é coerente com a natureza fragmentária do direito penal, que reserva a sanção criminal às lesões dolosas mais graves, e afasta a criminalização de erros técnicos involuntários, frequentes no manejo de sistemas complexos.

O § 1º do art. 154-A equipara à invasão a conduta de quem produz, oferece, distribui, vende ou difunde dispositivo ou programa destinado a permitir a prática do crime. Trata-se de antecipação da tutela penal a um momento anterior à invasão propriamente dita, alcançando a disponibilização de ferramentas de ataque. Essa opção, embora compreensível diante da economia dos crimes informáticos, exige cautela interpretativa para não criminalizar instrumentos de uso dúbio, como programas de teste de segurança empregados legitimamente por profissionais da área.

2.3 Legalidade, intervenção mínima e os limites da expansão penal informática

A ampliação do tipo penal recoloca uma tensão clássica do direito penal. De um lado, a sociedade reclama proteção diante de condutas lesivas no ambiente digital. De outro, a expansão da tutela

penal não pode converter o art. 154-A em cláusula geral de incriminação de qualquer acesso indesejado. Os princípios da legalidade, da intervenção mínima e da fragmentariedade operam, aqui, como limites de contenção.

A supressão da exigência de violação de mecanismo de segurança torna esses limites ainda mais relevantes. Sem a barreira técnica como filtro, cabe à interpretação assegurar que apenas condutas dotadas de efetiva lesividade ingressem no âmbito do tipo. O elemento subjetivo cumpre função decisiva: a norma exige dolo e finalidade específica de obter, adulterar ou destruir dados, ou de instalar vulnerabilidades para vantagem ilícita, de modo que acessos acidentais, autorizados ou destituídos dessa finalidade permanecem atípicos.

O alcance internacional do problema acentua a necessidade de coerência. A Convenção de Budapeste, promulgada no Brasil pelo Decreto n. 11.491/2023, define o acesso ilegal a sistemas informáticos como conduta a ser criminalizada pelos Estados signatários, mas faculta a exigência de que a infração seja cometida com violação de medidas de segurança (BRASIL, 2023a). O legislador brasileiro, ao reformar o tipo em 2021, seguiu caminho inverso ao da faculdade prevista no tratado, optando por um tipo mais aberto, o que reforça o papel da dogmática na delimitação do injusto.

A literatura processual penal de matriz comparada oferece subsídios para essa contenção. Greco e Gleizer (2019), ao analisarem a infiltração online e o acesso oculto a sistemas no direito alemão, demonstram que o avanço das técnicas de investigação digital deve vir acompanhado de exigências estritas de legalidade e de reserva de jurisdição, sob pena de erosão de garantias. A lição é transponível ao plano material: quanto mais amplo o tipo, mais rigorosa deve ser a sua aplicação.

Há, ainda, um risco de sobreposição típica que a doutrina vem assinalando. Com a reforma de 2021, condutas praticadas no ambiente digital podem tangenciar simultaneamente o art. 154-A, o furto mediante fraude eletrônica e o estelionato, também alterados pela mesma lei. A delimitação precisa do bem jurídico, retomada no item anterior, é o que permite distinguir a invasão informática, voltada ao controle sobre dados, de figuras orientadas à proteção do patrimônio, evitando-se concursos artificiais e bis in idem.

Em síntese, a tipificação penal da invasão de dispositivo informático constitui instrumento legítimo de tutela, mas a sua aplicação reformada exige redobrada cautela interpretativa. A questão, todavia, não se resolve no plano da norma incriminadora. Ainda que perfeitamente tipificada a conduta, a punição depende da demonstração da autoria e da materialidade, o que conduz ao terreno mais árduo da prova digital, examinado a seguir.

A tensão com o princípio da taxatividade também merece registro. Tipos penais abertos, ainda que constitucionalmente toleráveis, exigem do intérprete um esforço adicional de delimitação, sob pena de a indeterminação converter-se em insegurança jurídica. No caso do art. 154-A reformado, a ausência do elemento de segurança transfere para a finalidade específica e para a ausência de autorização o ônus de circunscrever o injusto, o que recomenda interpretação estrita dessas elementares e rejeição de leituras expansivas que alcancem meros acessos inconvenientes.

Sob a ótica da harmonização internacional, a Convenção de Budapeste e seus protocolos adicionais oferecem um vocabulário comum para a definição das condutas e para a cooperação entre Estados. A coerência entre o tipo interno e os parâmetros convencionais não é mera deferência ao direito internacional, mas fator de eficácia, pois facilita o auxílio mútuo e reduz divergências que, na prática, inviabilizam a responsabilização de agentes situados no

exterior. A contenção dogmática do tipo, portanto, dialoga com a sua inserção em um sistema normativo mais amplo.

A intervenção mínima impõe que se questione, em cada caso, se a resposta penal é realmente necessária. Boa parte das condutas lesivas no ambiente digital pode ser adequadamente enfrentada por mecanismos preventivos, contratuais ou administrativos, reservando-se a tutela penal às hipóteses de maior gravidade. A inflação de tipos penais informáticos, sem correspondente capacidade de aplicação, produz o efeito perverso das leis simbólicas, que aparentam proteção sem efetivamente conferi-la e que terminam por erodir a confiança no sistema de justiça.

A esse risco soma-se o da seletividade. Greco e Gleizer (2019) observam que o aparato investigativo digital, quando desacompanhado de limites estritos, tende a recair de modo desigual sobre determinados grupos, ampliando assimetrias preexistentes. A contenção do tipo penal e o rigor na obtenção da prova funcionam, também por isso, como instrumentos de igualdade, evitando que a expansão da tutela informática se converta em vigilância seletiva travestida de eficiência.

Há quem situe a invasão informática no âmbito de um direito penal voltado à proteção de bens supraindividuais, como a segurança dos sistemas e a confiança nas comunicações eletrônicas. Essa leitura, todavia, deve ser recebida com reservas, pois a diluição do bem jurídico em interesses difusos tende a flexibilizar as exigências de lesividade e a ampliar indevidamente o alcance do tipo. Mantém-se preferível ancorar o injusto na esfera informacional do titular, preservando a função garantística do conceito de bem jurídico.

3 PROVA DIGITAL, CADEIA DE CUSTÓDIA E OS DESAFIOS DA PERSECUÇÃO PENAL

Se a tipificação resolve o problema da previsão legal, a persecução penal enfrenta o problema da prova. Nos crimes informáticos, a materialidade repousa em vestígios eletrônicos cuja fragilidade técnica desafia os instrumentos tradicionais de investigação. A natureza da prova digital e da cadeia de custódia, o seu fundamento constitucional e os obstáculos de autoria que projetam a investigação para o plano internacional ocupam, nessa ordem, a análise que se segue.

3.1 A natureza volátil da prova digital e a cadeia de custódia

A prova digital possui características que a distinguem da prova material clássica. Saad, Rossi e Partata (2024) observam que o atributo digital não decorre do simples uso de um dispositivo, mas da circunstância de a informação relevante estar vinculada à manipulação eletrônica de dados, o que lhe confere natureza imaterial, volátil e facilmente alterável. Um vestígio digital pode ser modificado, copiado ou apagado sem deixar marcas visíveis, o que torna a sua integridade um problema central.

Essa fragilidade explica a centralidade da cadeia de custódia, conjunto de procedimentos destinados a documentar a história cronológica do vestígio, desde a coleta até o descarte. A Lei n. 13.964/2019 incorporou expressamente o instituto ao Código de Processo Penal, nos artigos 158-A a 158-F, estabelecendo etapas de reconhecimento, isolamento, fixação, coleta, acondicionamento e armazenamento (BRASIL, 2019). A função desses procedimentos é assegurar que o elemento apresentado em juízo é o mesmo que foi coletado, sem adulterações intermediárias.

A literatura forense estrangeira fornece o substrato técnico dessa exigência. Casey (2011) descreve a integridade e a autenticidade como pilares da forense digital, recomendando o uso de cópias-espelho e de funções de verificação criptográfica, como o cálculo de valores hash, para demonstrar que os dados não sofreram alteração. A mera apreensão de um equipamento, sem esses cuidados, é insuficiente para garantir a confiabilidade da fonte de prova.

O caso Carolina Dieckmann, ocorrido em 2012, ilustra de modo eloquente os desafios dessa investigação. A invasão do computador pessoal da atriz e a divulgação não autorizada de imagens íntimas expuseram a ausência, à época, de tipificação penal específica e a dificuldade das autoridades em responsabilizar os autores. A ampla repercussão do episódio acelerou a tramitação do projeto que resultou na Lei n. 12.737/2012, demonstrando como um caso concreto pode catalisar a resposta legislativa. O episódio revelou, ainda assim, que a criação do tipo, por si, não eliminava os obstáculos probatórios.

Com efeito, ainda que se disponha hoje de tipo penal reformado e de regramento legal da cadeia de custódia, persiste a necessidade de perícia técnica especializada e de operadores capacitados. Vaz (2012), em estudo pioneiro sobre o tema, já alertava para a inadequação de transpor mecanicamente à prova digital o procedimento probatório concebido para vestígios físicos, defendendo a sistematização de um regime próprio. A confiabilidade da prova, em suma, não é pressuposta, mas construída por meio de procedimentos verificáveis.

O Código de Processo Penal, ao disciplinar a cadeia de custódia, estruturou-a em etapas sucessivas que vão do reconhecimento e isolamento do vestígio ao seu acondicionamento e armazenamento, com registro documental de cada transferência de posse. Transposta ao ambiente digital, essa lógica reclama adaptações próprias: a coleta deve preservar metadados, a duplicação deve gerar cópias idênticas e verificáveis e cada manipulação deve ser registrada, de modo a

permitir a reconstrução integral do trajeto do dado, desde a apreensão até a análise pericial.

A doutrina e a prática forense convergem para a adoção de padrões técnicos reconhecidos, como as normas internacionais de tratamento de evidências digitais, que orientam a identificação, a coleta e a preservação dos dados. Tais referências não possuem força normativa autônoma no processo penal, mas funcionam como parâmetros de boa técnica cuja inobservância pode ser invocada para questionar a fiabilidade da prova. A ausência de protocolos uniformes, entretanto, ainda gera insegurança e decisões divergentes nos tribunais, o que reforça a tese de Vaz (2012) quanto à conveniência de um regime probatório específico.

A volatilidade dos dados impõe urgência à coleta. Registros de conexão, dados de geolocalização e conteúdos em servidores podem ser apagados em curto intervalo, seja por rotinas automáticas de exclusão, seja por ação deliberada do investigado. Daí a importância de medidas de preservação imediata, que congelem o estado dos dados enquanto se obtém a autorização para o seu acesso. A ausência de tais mecanismos, ou a sua utilização sem respaldo legal, compromete a investigação ou contamina a prova obtida.

Saad, Rossi e Partata (2024) sustentam que essas peculiaridades reclamam requisitos próprios, que o procedimento concebido para vestígios físicos não contempla integralmente. A simples analogia com a busca e apreensão tradicional ignora que o dado digital pode ser copiado sem subtração do original, replicado em múltiplos locais e alterado sem rastro aparente. Reconhecer a especificidade da prova digital não é capricho teórico, mas exigência de segurança jurídica, sobretudo diante da expansão do tipo penal operada em 2021.

A documentação minuciosa de cada operação técnica integra a própria essência da prova digital. O registro do método empregado,

das ferramentas utilizadas e dos valores de verificação obtidos permite que terceiros reproduzam e auditem o resultado, conferindo à perícia o atributo de reprodutibilidade que se espera de um procedimento de pretensão científica. A ausência desse registro converte o laudo em mera afirmação de autoridade, insuscetível de controle, o que é incompatível com o contraditório técnico.

3.2 O fundamento constitucional da cadeia de custódia da prova digital

A cadeia de custódia costuma ser tratada como questão técnica ou meramente procedimental. Geraldo Prado, todavia, oferece leitura que a eleva ao plano constitucional. Em sua obra sobre o tema, o autor demonstra que a rastreabilidade da prova é condição para o controle epistêmico da jurisdição penal, isto é, para que se possa verificar racionalmente como a prova foi obtida e por que ela sustenta determinada conclusão (PRADO, 2021).

Esse controle não é um luxo metodológico, mas decorrência das garantias do contraditório, da ampla defesa e da paridade de armas. Prado (2014) sustenta que a quebra da cadeia de custódia, sobretudo nas provas obtidas por métodos ocultos, compromete a possibilidade de a defesa fiscalizar a origem e a integridade do material, esvaziando o contraditório de seu conteúdo substancial. Quando aplicada à prova digital, essa exigência ganha contornos próprios, pois a volatilidade dos dados amplia as oportunidades de manipulação não detectável.

A jurisprudência do Superior Tribunal de Justiça tem reconhecido as consequências processuais da inobservância desses procedimentos. No julgamento do Habeas Corpus n. 160.662/RJ, a Corte assentou que a ausência de preservação da integralidade da prova obtida por meios telemáticos viola o contraditório e a ampla

defesa. Em precedentes mais recentes, o Tribunal reafirmou que a ausência de demonstração da cadeia de custódia digital pode comprometer a fiabilidade do material e repercutir na sua valoração, como no Recurso em Habeas Corpus n. 143.169/RJ.

Discute-se, na doutrina, se a violação da cadeia de custódia conduz à inadmissibilidade da prova ou se opera apenas no plano da valoração. Prado (2021) tende a vincular a questão ao exame de corpo de delito e à admissibilidade, ao passo que parte da literatura prefere situá-la na aferição do peso probatório. Independentemente da solução adotada, há consenso quanto a um ponto: a falha na rastreabilidade enfraquece a prova e impõe ônus argumentativo à acusação.

Desse modo, a cadeia de custódia da prova digital não é exigência burocrática, mas projeção das garantias constitucionais sobre o terreno técnico. A sua observância protege tanto o investigado, contra condenações fundadas em material inseguro, quanto a própria persecução penal, cuja legitimidade depende da confiabilidade dos elementos que a sustentam. A perícia, nesse contexto, deve ser oficial, independente e tecnicamente idônea, sob pena de fragilizar todo o edifício probatório.

A controvérsia entre admissibilidade e valoração tem consequências práticas distintas. Se a quebra da cadeia de custódia conduzir à inadmissibilidade, a prova é excluída do processo e não pode fundamentar a decisão. Se for tratada como problema de valoração, a prova permanece nos autos, porém com peso reduzido. A escolha entre essas vias não é neutra: a primeira tutela com mais vigor as garantias do investigado, ao passo que a segunda confere maior flexibilidade ao julgador, com o risco de relativizar as exigências de integridade quando a prova for incriminadora.

Precedentes do Superior Tribunal de Justiça formados após a reforma de 2021 já oferecem resposta prática a essa controvérsia. No

julgamento do Agravo Regimental no Recurso em Habeas Corpus n. 143.169/RJ, a Quinta Turma, por maioria, declarou inadmissíveis as provas extraídas de computadores apreendidos por ausência de documentação da coleta, do armazenamento e da análise, atribuindo ao Estado o encargo de demonstrar a integridade do material (BRASIL, 2023b). No Agravo Regimental no Habeas Corpus n. 828.054/RN, a mesma Turma reafirmou que a extração de dados de aparelho celular sem metodologia forense documentada torna a prova inadmissível, e não apenas fragilizada (BRASIL, 2024a). O Habeas Corpus n. 738.418/SP, julgado pela Sexta Turma, acrescentou a exigência de que o próprio procedimento adotado permita testar a confiabilidade dos dados extraídos (BRASIL, 2024b). Mais recentemente, no Agravo Regimental no Habeas Corpus n. 943.895/PR, a Quinta Turma consolidou o entendimento de que o ônus de provar a observância da cadeia de custódia do vestígio digital recai sobre o Estado, nas figuras da polícia e do Ministério Público, e não sobre o investigado (BRASIL, 2025). Essa linha decisória permite afirmar, com apoio em precedente reiterado e não apenas em construção doutrinária, que a falha na cadeia de custódia digital opera no plano da admissibilidade, e não apenas no da valoração: a prova cuja integridade o Estado não consegue demonstrar não ingressa validamente no processo.

Sobressai, ainda, a exigência de que a perícia em prova digital seja oficial, independente e tecnicamente idônea. A delegação da análise a entes privados interessados, ou a sua realização sem condições de contraditório, fragiliza o controle epistêmico defendido por Prado (2021) e compromete a paridade de armas. A independência do exame pericial, nesse domínio, não constitui formalidade dispensável, mas garantia de que a reconstrução dos fatos não será capturada por uma das partes nem fundada em material cuja origem não se possa auditar.

O controle epistêmico defendido por Prado (2014) pressupõe que a defesa possa refazer, ao menos em tese, o caminho percorrido pela prova. Quando esse caminho é opaco, a presunção de inocência resta enfraquecida, pois a acusação se beneficia de um material cuja origem não pode ser questionada. A cadeia de custódia, ao tornar rastreável cada etapa, devolve à defesa a possibilidade de fiscalização e restaura o equilíbrio entre as partes, condição de um processo penal de feição acusatória.

Essa exigência não deve, todavia, ser confundida com formalismo estéril. O que se busca não é o cumprimento ritual de formalidades, mas a garantia substancial de integridade e autenticidade da prova. Uma falha meramente formal, sem repercussão sobre a fiabilidade do dado, não possui o mesmo peso de uma quebra que torne impossível verificar se o material foi manipulado. A jurisprudência tem caminhado para essa distinção, avaliando, no caso concreto, a aptidão da falha para comprometer a confiabilidade do elemento probatório.

3.3 Autoria, anonimato e cooperação internacional: a Convenção de Budapeste

Mesmo assegurada a integridade do vestígio, remanesce o problema talvez mais difícil: a identificação da autoria. O uso de redes privadas virtuais, de servidores intermediários e de ferramentas de anonimização dificulta a individualização do agente, frequentemente situado em jurisdição diversa daquela em que se produziram os efeitos do crime. A persecução penal depara-se, assim, com uma criminalidade que ignora fronteiras.

Cavalcante Vieira e Rodrigues Santos (2025) destacam que a investigação criminal apoiada em tecnologias digitais exige não apenas capacitação técnica dos órgãos estatais, mas também salvaguardas contra a expansão desproporcional da vigilância. Os autores chamam

a atenção para o risco de que instrumentos como o policiamento preditivo e a coleta massiva de dados convertam a eficiência investigativa em ameaça às liberdades, o que reforça a necessidade de balizas jurídicas claras na obtenção da prova digital.

Foi nesse cenário que a adesão à Convenção de Budapeste adquiriu relevância prática. Promulgada pelo Decreto n. 11.491/2023, após aprovação congressional por meio do Decreto Legislativo n. 37/2021, a Convenção sobre o Crime Cibernético oferece um marco de cooperação internacional para a obtenção de provas eletrônicas armazenadas em outros países e para a harmonização das legislações nacionais (BRASIL, 2023a). O tratado disciplina o acesso ilegal, a interceptação ilícita e a interferência em dados e sistemas, além de prever mecanismos de auxílio mútuo entre os Estados.

A relevância do instrumento decorre da própria natureza transnacional dos crimes informáticos. Sem cooperação, a investigação esbarra na soberania de outros Estados e na localização física de servidores. Bujosa Vadell, Bustamante Rúa e Toro Garzón (2021), em estudo comparado entre Espanha e Colômbia, demonstram que a prova digital obtida por vigilância secreta suscita problemas comuns de admissibilidade e de valoração nos diversos ordenamentos, o que torna a convergência normativa um pressuposto de eficácia.

É preciso, no entanto, evitar leituras ingênuas. A cooperação internacional não dispensa o controle de legalidade interno, nem autoriza que dados obtidos no exterior ingressem no processo à margem das garantias nacionais. A Convenção é instrumento de eficiência, mas a sua aplicação permanece submetida aos parâmetros constitucionais brasileiros, em especial à reserva de jurisdição e à proteção de dados, tema que articula esta análise da prova com a discussão sobre proteção de dados que vem a seguir.

A cooperação internacional, embora indispensável, esbarra em entraves estruturais. Os pedidos de auxílio jurídico mútuo e as cartas

rogatórias frequentemente tramitam com lentidão incompatível com a volatilidade dos dados, que podem ser apagados antes de obtida a autorização. A localização de servidores em jurisdições diversas e a diversidade de regimes jurídicos agravam o problema, tornando a harmonização promovida pela Convenção de Budapeste um instrumento de eficiência valioso, ainda que insuficiente por si só para superar todos os obstáculos da investigação transnacional.

No plano interno, o Marco Civil da Internet já estabelecia deveres de guarda de registros e parâmetros para o fornecimento de dados mediante ordem judicial. A adesão à Convenção de Budapeste soma-se a esse arcabouço, sem o substituir, e exige leitura harmônica que preserve a reserva de jurisdição. A obtenção de prova no exterior, em qualquer hipótese, deve respeitar as garantias do ordenamento brasileiro, sob pena de ilicitude por contaminação dos elementos derivados, conforme a lógica das proibições de prova.

A dimensão transnacional também desafia a noção tradicional de competência. Quando o agente, a vítima e o servidor situam-se em países distintos, a definição do foro e da lei aplicável torna-se complexa, exigindo critérios de conexão que a legislação interna nem sempre fornece de modo claro. A Convenção de Budapeste oferece parâmetros de cooperação, mas não suprime as dificuldades decorrentes da soberania, que permanece como limite à atuação direta de autoridades estrangeiras em território nacional.

Bujosa Vadell, Bustamante Rúa e Toro Garzón (2021) demonstram, na comparação entre ordenamentos, que a admissibilidade da prova digital obtida no exterior depende da compatibilidade entre os padrões de obtenção e as garantias do foro. Transposta ao Brasil, a lição impõe que a prova produzida sob regime estrangeiro seja filtrada pelas exigências constitucionais internas antes de ser valorada, evitando-se que a cooperação internacional sirva de via oblíqua para a flexibilização de garantias.

Acrescente-se que a identificação do agente, mesmo quando tecnicamente possível, raramente é definitiva. O uso de credenciais alheias, a infecção de dispositivos por terceiros e a atuação coordenada de grupos dificultam a imputação individual. Por isso, a prova da autoria deve resultar de um conjunto convergente de elementos, e não de um único indício técnico, sob pena de condenações fundadas em inferências frágeis sobre quem, de fato, operava o sistema no momento do crime.

4 ENTRE O DIREITO PENAL E A PROTEÇÃO DE DADOS: A TUTELA INTEGRADA DA PRIVACIDADE

A invasão de dispositivo informático situa-se na interseção entre o direito penal e o regime de proteção de dados pessoais. Tratar esses campos isoladamente conduz a respostas incompletas. A proteção de dados como direito fundamental, a articulação entre o art. 154-A e a Lei Geral de Proteção de Dados e os limites de proporcionalidade que disciplinam o acesso a dados na persecução penal organizam a análise que se segue.

4.1 Proteção de dados como direito fundamental e autodeterminação informativa

A proteção de dados pessoais consolidou-se, no constitucionalismo contemporâneo, como expressão autônoma da dignidade da pessoa humana e dos direitos da personalidade. No Brasil, esse reconhecimento culminou na Emenda Constitucional n. 115/2022, que inscreveu a proteção de dados entre os direitos e garantias fundamentais. Trata-se de movimento que confirma a leitura

doutrinária anterior, segundo a qual a tutela dos dados já decorria do sistema constitucional.

Doneda (2019) descreve esse percurso como a passagem da privacidade à proteção de dados, na qual o foco se desloca da defesa de uma esfera íntima para a regulação do tratamento da informação pessoal ao longo de todo o seu ciclo. A proteção de dados, nessa acepção, não proíbe o uso da informação, mas o submete a princípios e garantias, conferindo ao titular instrumentos de controle. A invasão informática, por subtrair esse controle de forma abrupta e clandestina, atinge o cerne do interesse protegido.

A literatura brasileira já explorava essa passagem antes mesmo da consolidação legislativa do tema. Oliva e Pessoa (2016) analisam os bancos de dados que armazenam informações de consumidores brasileiros e descrevem, a partir da figura do panóptico pós-moderno, como a pessoa se converte em mercadoria informacional quando submetida a um controle continuado sobre os próprios dados sem ter disso pleno conhecimento. A leitura, construída para o direito do consumidor, ilumina por analogia a invasão de dispositivo informático: também aqui o titular perde o controle sobre um fluxo de informações que o descreve, ainda que a vigilância decorra de um ato ilícito pontual, e não de um regime contratual de coleta.

Sarlet, Mendes e Doneda (2021) sistematizam os fundamentos desse direito fundamental, articulando a autodeterminação informativa, a transparência e a finalidade como vetores de um regime jurídico próprio. A autodeterminação informativa, conceito de matriz germânica incorporado ao debate brasileiro, traduz a prerrogativa de o indivíduo decidir, em princípio, sobre a revelação e o uso de seus dados, prerrogativa que a invasão de dispositivo informático nega frontalmente.

A doutrina estrangeira ilumina o ponto. Rodotà (2008) já sublinhava que a proteção de dados é condição de exercício da

liberdade em uma sociedade que opera por meio de informações, e não apenas garantia de segredo. A privacidade deixa de ser um direito de exclusão para tornar-se um direito de participação na circulação dos próprios dados. Sob essa perspectiva, a tutela penal da invasão informática integra um sistema mais amplo de proteção da pessoa no ambiente digital.

Compreendido o bem jurídico nesses termos, torna-se evidente que a resposta penal é apenas uma das peças de um arranjo normativo. A prevenção de incidentes, a imposição de deveres de segurança e a responsabilização administrativa e civil compõem, ao lado da sanção penal, um sistema integrado de proteção. É essa articulação que o item seguinte procura precisar.

O reconhecimento da proteção de dados como direito fundamental autônomo precedeu, na jurisprudência, a sua positivação expressa. Em 2020, ao apreciar o compartilhamento massivo de dados de usuários de telefonia, o Supremo Tribunal Federal, na Ação Direta de Inconstitucionalidade n. 6.387, afirmou a existência de um direito fundamental à proteção de dados pessoais decorrente do sistema constitucional. A Emenda Constitucional n. 115/2022 veio, posteriormente, consolidar esse entendimento no próprio texto da Constituição, inscrevendo a proteção de dados no rol dos direitos fundamentais.

Essa trajetória confirma que a tutela dos dados não é criação da legislação ordinária, mas concretização de um direito de matriz constitucional. A invasão de dispositivo informático, ao violar esse direito, agride não apenas a vítima individual, mas também o modelo de proteção que a ordem jurídica erigiu. A leitura penal do art. 154-A deve, por isso, ser informada pela estatura constitucional do bem jurídico, o que repercute tanto na interpretação do tipo quanto na ponderação que orienta as medidas de investigação.

A consagração da proteção de dados como direito fundamental repercute sobre a interpretação de toda a legislação infraconstitucional. Tanto o art. 154-A quanto a Lei Geral de Proteção de Dados passam a ser lidos à luz desse direito, que funciona como vetor hermenêutico e como parâmetro de validade. Normas e práticas que esvaziem o controle do titular sobre seus dados tornam-se constitucionalmente suspeitas, o que confere à proteção de dados uma força expansiva sobre o conjunto do ordenamento.

Doneda (2019) ressalta que esse direito não se confunde com a propriedade sobre os dados, mas se traduz em um feixe de garantias relativas ao seu tratamento. O titular não é dono da informação no sentido patrimonial, e sim sujeito de direitos quanto ao modo como ela é coletada, usada e compartilhada. Essa concepção afasta leituras mercantis e reforça a vinculação da proteção de dados à dignidade da pessoa, o que tem consequências diretas sobre a gravidade atribuída à invasão informática.

4.2 A articulação entre o art. 154-A, a LGPD e o direito de proteção de dados no processo penal

A Lei n. 13.709/2018, Lei Geral de Proteção de Dados Pessoais, estabeleceu um regime jurídico voltado à disciplina do tratamento de dados, com fundamento expresso na proteção de direitos fundamentais. O seu artigo 1º delimita o objeto e a finalidade da norma:

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

A relação entre a Lei Geral de Proteção de Dados e o art. 154-A é de complementaridade, não de identidade. Enquanto a norma penal reprime, de forma subsidiária, a conduta mais grave do agente invasor, a Lei Geral impõe a controladores e operadores deveres de segurança cuja inobservância pode ensejar responsabilização administrativa e civil. Uma mesma invasão pode, assim, desencadear consequências em planos distintos: a punição de quem invade e a responsabilização de quem, por negligência, deixou de proteger adequadamente os dados.

Há, entretanto, um ponto de fricção frequentemente negligenciado. A própria persecução penal constitui tratamento de dados pessoais e, como tal, deve observar os princípios da finalidade, da necessidade e da segurança. Gleizer, Montenegro e Viana (2021) defendem a existência de um direito de proteção de dados aplicável ao processo penal e à segurança pública, de modo que a atividade investigativa não está imune às garantias que ela própria busca tutelar. O Estado que investiga a violação de dados não pode, ao fazê-lo, violar dados de forma desproporcional.

A doutrina processual de matriz alemã reforça essa exigência. Wolter (2018) articula a proteção de dados com a teoria das proibições de prova, sustentando que a dignidade da pessoa e a separação informacional de poderes impõem limites à coleta e ao uso de informações na persecução penal. A consequência é clara: dados obtidos com afronta a esses limites não podem legitimar a condenação, ainda que materialmente relevantes.

A Lei Geral de Proteção de Dados, é certo, prevê hipóteses de tratamento para o cumprimento de obrigação legal e para o exercício regular de direitos em processos. Tais previsões não convertem a lei em obstáculo à investigação, mas estabelecem balizas para que o acesso a dados ocorra de modo legítimo. A leitura integrada das duas normas afasta tanto a tese de que a proteção de dados inviabiliza a

persecução quanto a tese oposta, de que a persecução autoriza o acesso irrestrito.

A própria Lei Geral de Proteção de Dados, apesar disso, excluiu de seu âmbito de aplicação o tratamento de dados realizado para fins exclusivos de segurança pública e de investigação e repressão de infrações penais, nos termos de seu art. 4º, inciso III (BRASIL, 2018). Essa exclusão criou um vácuo normativo de difícil justificação: justamente a atividade estatal mais apta a interferir nos direitos dos titulares ficou desprovida de disciplina legal específica, à espera de uma legislação própria que ainda não foi editada.

O direito comparado oferece modelo para o preenchimento dessa lacuna. Na União Europeia, a Diretiva (UE) 2016/680 disciplina o tratamento de dados pessoais para fins de prevenção e repressão penal, estabelecendo princípios e garantias específicos para a atuação das autoridades competentes (UNIÃO EUROPEIA, 2016). A ausência, no Brasil, de um regime equivalente acentua a importância de aplicar, por força constitucional, os princípios da finalidade, da necessidade e da proporcionalidade à persecução penal, suprindo interpretativamente o silêncio do legislador (GLEIZER; MONTENEGRO; VIANA, 2021).

A complementaridade entre a norma penal e a Lei Geral de Proteção de Dados não elimina zonas de tensão. A persecução de uma invasão informática pode exigir o acesso a dados de terceiros não investigados, como provedores e contatos da vítima, o que suscita o problema do tratamento de dados de pessoas alheias ao fato. A delimitação rigorosa do objeto da investigação é, nesse ponto, indispensável para que a apuração de uma violação não se converta em fonte de novas violações.

Wolter (2018) fornece a chave teórica para enfrentar esse risco ao articular proteção de dados e proibições de prova. Para o autor, a coleta de informações que afronte o núcleo intangível da personalidade não pode ser convalidada por sua utilidade probatória,

pois há um patamar de proteção que se impõe mesmo diante do interesse na elucidação dos fatos. Essa perspectiva oferece um critério substancial, e não meramente procedimental, para a exclusão de provas obtidas com violação desproporcional de dados.

Sob o aspecto institucional, a Lei Geral de Proteção de Dados criou autoridade administrativa incumbida de fiscalizar o tratamento de dados e de orientar os agentes. Embora sua competência não alcance a persecução penal, a atuação dessa autoridade contribui para a difusão de uma cultura de segurança que reduz a incidência de incidentes. A prevenção promovida no âmbito administrativo e a repressão exercida no âmbito penal compõem, assim, faces complementares de uma mesma política de proteção da informação.

A exigência de governança não é estranha à reflexão sobre sistemas informáticos em geral. Moraes e Carini (2020) sustentam que a confiança em sistemas de inteligência artificial depende de mecanismos de governança ética capazes de tornar o funcionamento do sistema auditável e responsivo a quem é afetado por suas decisões. O mesmo requisito de auditabilidade, adaptado à investigação penal, é o que a jurisprudência do Superior Tribunal de Justiça exige da cadeia de custódia digital: um procedimento cuja metodologia possa ser reconstruída e testada por terceiros, e não apenas afirmada pela autoridade que a executou.

4.3 Persecução penal, acesso a dados e proporcionalidade

A investigação dos crimes informáticos demanda, quase sempre, acesso a dados pessoais, registros de conexão e conteúdos digitais, elementos indispensáveis à demonstração da autoria e da materialidade. O ponto sensível está em compatibilizar essa

necessidade investigativa com a preservação dos direitos dos titulares. A proporcionalidade emerge, então, como critério reitor.

Em outro trabalho, Saad, Rossi e Partata (2024) sustentam que a obtenção de provas digitais reclama disciplina jurídica própria, com previsão de hipóteses, requisitos e procedimentos específicos que balizem as decisões judiciais autorizadoras. A ausência de parâmetros claros transfere ao julgador uma margem de discricionariedade incompatível com a sensibilidade dos direitos em jogo, sobretudo quando se trata de acesso oculto e remoto a dispositivos.

O Supremo Tribunal Federal enfrentou faceta correlata do problema no Recurso Extraordinário n. 1.055.941/SP, ao tratar do compartilhamento, com órgãos de persecução, de dados protegidos por sigilo. A Corte admitiu o compartilhamento, mas o condicionou a balizas e a deveres de preservação, reconhecendo que a eficiência da persecução não suspende a proteção dos dados, mas convive com ela sob condições. O precedente confirma que o acesso estatal a informações sensíveis exige justificação e controle.

A doutrina comparada adverte para os riscos da deriva vigilantista. Zuboff (2019) demonstra como a lógica da coleta total de dados, própria do capitalismo de vigilância, tende a normalizar formas de monitoramento que, transpostas ao Estado, ameaçam a autodeterminação informativa. Cavalcante Vieira e Rodrigues Santos (2025), na mesma linha, alertam que a incorporação acrítica de tecnologias de vigilância à segurança pública pode subverter a relação entre eficiência e garantias.

A proporcionalidade, nesse contexto, opera em três planos. No plano da adequação, a medida investigativa deve ser apta a produzir a prova buscada. No plano da necessidade, deve ser a menos gravosa entre as disponíveis, evitando-se a coleta indiscriminada. No plano da proporcionalidade em sentido estrito, o sacrifício imposto ao titular dos dados deve ser compensado pela relevância do interesse

perseguido. A inobservância de qualquer desses planos contamina a legitimidade da prova.

Fecha-se esta análise com uma constatação. A tutela da invasão de dispositivo informático não se realiza apenas no momento da punição, mas ao longo de toda a cadeia que vai da prevenção à valoração da prova. A proteção de dados não é adversária da persecução penal: é a sua condição de legitimidade. Eficiência e garantia, longe de se excluírem, reclamam-se mutuamente em um Estado Democrático de Direito.

A aplicação concreta da proporcionalidade revela-se particularmente delicada no acesso a dados armazenados em telefones celulares. O aparelho contemporâneo concentra a totalidade da vida digital do indivíduo, de modo que a sua devassa indiscriminada equivale a uma medida de amplitude desproporcional. A exigência de autorização judicial fundamentada e de delimitação do objeto da diligência funciona, nesse contexto, como contenção indispensável, evitando que a apreensão de um dispositivo se converta em vigilância retrospectiva e ilimitada sobre a pessoa.

Questão correlata é a do desbloqueio compelido de dispositivos. França (2023), em análise comparativa entre os sistemas brasileiro e estadunidense, examina a tensão entre a segurança pública e o direito de não produzir prova contra si mesmo, demonstrando que obrigar o investigado a fornecer senha ou dado biométrico pode colidir com o princípio *nemo tenetur se detegere*. A solução desse impasse exige ponderação cuidadosa, incompatível com automatismos que sacrifiquem garantias em nome da eficiência investigativa.

Doutrina e jurisprudência têm convergido para a exigência de fundamentação reforçada nas decisões que autorizam o acesso a dados. Não basta a invocação genérica do interesse na investigação; é preciso indicar a relação entre os dados buscados e os fatos apurados, bem como justificar a extensão temporal e material da medida. Essa

exigência concretiza a proporcionalidade e permite o controle posterior da decisão, tanto pela defesa quanto pelas instâncias revisoras, conferindo racionalidade ao emprego dos meios de obtenção de prova digital.

Os mesmos autores alertam, ainda, para o risco de naturalização da vigilância. À medida que tecnologias de monitoramento se incorporam à rotina investigativa, tende-se a tratar como ordinário aquilo que deveria permanecer excepcional. Resistir a essa naturalização é tarefa que cabe ao controle judicial e à doutrina, encarregados de reafirmar que a regra é a proteção dos dados e a exceção é o seu acesso, e não o contrário, sob pena de inversão da lógica constitucional.

A advertência de Zuboff (2019) sobre a lógica extrativista dos dados encontra eco na atuação estatal quando esta incorpora, sem filtros, as ferramentas de coleta desenvolvidas no mercado. O Estado que se vale dessas tecnologias herda também os seus riscos, podendo converter a investigação criminal em instrumento de monitoramento difuso. A proporcionalidade, nesse cenário, cumpre função de antídoto, ao exigir que cada acesso seja justificado, delimitado e submetido a controle, preservando a excepcionalidade que deve caracterizar a intervenção estatal na esfera informacional.

5 CONSIDERAÇÕES FINAIS

Reformado em 2021, o artigo 154-A do Código Penal já não depende primordialmente da amplitude do tipo para operar com efetividade: depende de que o vestígio digital que sustenta a acusação tenha sua integridade demonstrada pelo Estado, e não presumida em seu favor. É essa distribuição do ônus da prova, e não a supressão da exigência de violação de mecanismo de segurança, que hoje decide se

a invasão informática resulta em condenação ou em absolvição por insuficiência probatória. A jurisprudência do Superior Tribunal de Justiça formada entre 2023 e 2025 já consagrou esse critério, ainda que a doutrina especializada continue por vezes a discuti-lo como se estivesse em aberto.

Partiu-se da pergunta sobre como compatibilizar a tutela penal reformada do art. 154-A com a confiabilidade da prova digital e com os direitos fundamentais dos investigados. Mediante método dedutivo e pesquisa bibliográfica, documental, normativa e jurisprudencial, examinaram-se a estrutura do tipo após a Lei n. 14.155/2021, os fundamentos técnicos e constitucionais da cadeia de custódia digital e a articulação entre a norma penal e o regime de proteção de dados pessoais. A pesquisa incorporou, nesse percurso, a linha jurisprudencial do Superior Tribunal de Justiça posterior à reforma, que a literatura consultada ainda não havia sistematizado de modo integrado à dogmática do art. 154-A.

Confirmou-se que a Lei n. 14.155/2021 promoveu mais do que um agravamento de penas. Ao suprimir do caput a exigência de violação de mecanismo de segurança e ao substituir a referência a dispositivo alheio por dispositivo de uso alheio, a reforma deslocou o centro da ilicitude da técnica de invasão para a ausência de autorização do titular, ampliando o alcance do tipo e tornando obsoletas as análises ainda apoiadas na redação de 2012. Essa ampliação, contudo, não eliminou o problema da lesividade: transferiu-o inteiramente para o momento da prova, onde a finalidade específica exigida pelo tipo e a ausência de autorização precisam ser demonstradas por elementos técnicos verificáveis, e não presumidas a partir da mera constatação do acesso.

Demonstrou-se, na sequência, que essa transferência de peso para a prova encontrou resposta jurisprudencial concreta. A cadeia de custódia digital, regrada pela Lei n. 13.964/2019, deixou de ser tratada

pelo Superior Tribunal de Justiça como formalidade cuja falha apenas reduz o peso do material: no Agravo Regimental no Recurso em Habeas Corpus n. 143.169/RJ, no Agravo Regimental no Habeas Corpus n. 828.054/RN, no Habeas Corpus n. 738.418/SP e, de modo consolidado, no Agravo Regimental no Habeas Corpus n. 943.895/PR, a Corte atribuiu ao Estado o ônus de comprovar a integridade do vestígio digital como condição de admissibilidade, não de mera valoração. A consequência prática é que a ausência de metodologia forense documentada, por si só, inviabiliza a prova, independentemente de o investigado demonstrar concretamente a manipulação do material.

Evidenciou-se, por fim, que essa exigência probatória converge com o regime de proteção de dados pessoais. A persecução penal do art. 154-A constitui, ela própria, tratamento de dados, e submete-se aos princípios da finalidade, da necessidade e da proporcionalidade mesmo à falta de disciplina legal específica para a segurança pública. A exigência de auditabilidade que a literatura sobre governança de sistemas informáticos formula para a inteligência artificial e a leitura da proteção de dados como poder de controle sobre a própria informação, e não como mero segredo, convergem no mesmo ponto: um procedimento cuja integridade não possa ser reconstruída e testada por terceiros não gera prova válida, seja qual for o rótulo dado ao vício.

A resposta à pergunta de pesquisa é, portanto, direta: a tutela penal da invasão de dispositivo informático se efetiva não pela amplitude do tipo, mas pela imposição, já jurisprudencialmente consolidada, de que o Estado demonstre a integridade da cadeia de custódia digital como pressuposto de admissibilidade da prova. O critério operativo decorrente é preciso: toda extração de dados de dispositivo informático destinada a instruir persecução penal fundada no art. 154-A deve ser acompanhada de laudo pericial que identifique

o método empregado, a ferramenta utilizada e o valor de verificação criptográfica do material original e da cópia analisada; a ausência de qualquer desses elementos, verificada em juízo, torna a prova inadmissível, independentemente de o investigado comprovar manipulação concreta. Esse critério não amplia garantias além do que a jurisprudência já assegura: torna-o verificável e replicável por qualquer operador, inclusive fora do âmbito dos tribunais superiores.

A objeção mais forte a esse critério é de ordem prática: exigir laudo pericial completo, com valor de verificação criptográfica e metodologia documentada, em toda investigação de invasão informática pode inviabilizar a persecução de casos de menor complexidade técnica, sobretudo em comarcas sem estrutura de perícia digital, e favorecer sistematicamente investigados com maior capacidade de impugnação técnica. A objeção procede quanto ao diagnóstico, mas não quanto à conclusão. A limitação de recursos periciais é problema de política de segurança pública, a ser enfrentado por investimento em capacitação e equipamento, e não motivo para relativizar a exigência de integridade da prova em favor da eficiência. Admitir prova digital sem metodologia verificável para compensar a carência estrutural do Estado inverteria a lógica constitucional: transformaria uma deficiência da acusação em ônus do investigado, exatamente o resultado que a jurisprudência do Superior Tribunal de Justiça já rejeitou.

Propõe-se ao Conselho Nacional do Ministério Público a edição de diretriz, no âmbito da atuação criminal dos Ministérios Públicos estaduais e do Distrito Federal, condicionando o oferecimento de denúncia fundada em prova extraída de dispositivo informático à juntada de laudo técnico que identifique o método de extração, a ferramenta utilizada e o valor de verificação criptográfica do material original e da cópia periciada, nos termos consolidados pelo Superior Tribunal de Justiça no Agravo Regimental no Habeas Corpus n.

943.895/PR. A diretriz não cria requisito novo: torna exigível, na fase de oferecimento da denúncia, o que os tribunais superiores já exigem na fase de admissibilidade da prova, evitando o desgaste de ações penais construídas sobre material que a própria jurisprudência do Superior Tribunal de Justiça tende a invalidar.

Data de Submissão: 18/06/2026

Data de Aprovação: 31/08/2026

Processo de Avaliação: *double blind peer review*

Editor Geral: Prof. Dr. Herry Charriery da Costa Santos

Editora Adjunta: Profa. Dra. Hirdan Katarina de Medeiros Costa

Assistente Editorial: Anna Karoline Tavares Marsicano de Brito

Assistente Editorial: Iasmim Barbosa Araujo

REFERÊNCIAS

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Senado Federal, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 22 maio 2026.

BRASIL. Decreto-Lei n. 2.848, de 7 de dezembro de 1940. Código Penal. Diário Oficial da União: Rio de Janeiro, 31 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 22 maio 2026.

BRASIL. Decreto n. 11.491, de 12 de abril de 2023a. Promulga a Convenção sobre o Crime Cibernético, firmada em Budapeste, em 23 de novembro de 2001. Diário Oficial da União: Brasília, DF, 13 abr. 2023. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm. Acesso em: 22 maio 2026.

BRASIL. Lei n. 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Diário Oficial da União: Brasília, DF, 3 dez. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 22 maio 2026.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 22 maio 2026.

BRASIL. Lei n. 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. Diário Oficial da União: Brasília, DF, 24 dez. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 22 maio 2026.

BRASIL. Lei n. 14.155, de 27 de maio de 2021. Altera o Decreto-Lei n. 2.848/1940 para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet. Diário Oficial da União: Brasília, DF, 28 maio 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 22 maio 2026.

BRASIL. Superior Tribunal de Justiça. Agravo Regimental no Habeas Corpus n. 828.054/RN. Relator: Min. Joel Ilan Paciornik, 5ª Turma, julgado em 23 abr. 2024a. Disponível em: <https://www.stj.jus.br>. Acesso em: 21 ago. 2026.

BRASIL. Superior Tribunal de Justiça. Agravo Regimental no Habeas Corpus n. 943.895/PR. Relator: Min. Joel Ilan Paciornik, 5ª Turma, julgado em 3 set. 2025. Disponível em: <https://www.stj.jus.br>. Acesso em: 21 ago. 2026.

BRASIL. Superior Tribunal de Justiça. Agravo Regimental no Recurso em Habeas Corpus n. 143.169/RJ. Relator: Min. Messod Azulay Neto; Relator para acórdão: Min. Ribeiro Dantas, 5ª Turma, julgado em 7 fev. 2023b. Disponível em: <https://www.stj.jus.br>. Acesso em: 21 ago. 2026.

BRASIL. Superior Tribunal de Justiça. Habeas Corpus n. 160.662/RJ. Relatora: Min. Assusete Magalhães, 6ª Turma, julgado

em 18 fev. 2014. Disponível em: <https://www.stj.jus.br>. Acesso em: 22 maio 2026.

BRASIL. Superior Tribunal de Justiça. Habeas Corpus n. 738.418/SP. Relator: Min. Otávio de Almeida Toledo, 6ª Turma, julgado em 19 dez. 2024b. Disponível em: <https://www.stj.jus.br>. Acesso em: 21 ago. 2026.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade n. 6.387 MC-Ref/DF. Relatora: Min. Rosa Weber, Tribunal Pleno, julgado em 7 maio 2020. Disponível em: <https://portal.stf.jus.br>. Acesso em: 22 maio 2026.

BRASIL. Supremo Tribunal Federal. Recurso Extraordinário n. 1.055.941/SP. Relator: Min. Dias Toffoli, Tribunal Pleno, julgado em 4 dez. 2019. Disponível em: <https://portal.stf.jus.br>. Acesso em: 22 maio 2026.

BUJOSA VADELL, Lorenzo M.; BUSTAMANTE RÚA, Mónica M.; TORO GARZÓN, Luis O. La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 7, n. 2, p. 1347-1384, maio/ago. 2021. Disponível em: <https://doi.org/10.22197/rbdpp.v7i2.482>. Acesso em: 22 maio 2026.

CASEY, Eoghan. *Digital evidence and computer crime: forensic science, computers, and the internet*. 3rd ed. Waltham: Academic Press, 2011.

CAVALCANTE VIEIRA, Ana Beatriz; RODRIGUES SANTOS, Hugo Leonardo. Investigação criminal e tecnologias digitais: algumas reflexões sobre o policiamento preditivo e a admissibilidade de provas digitais. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 11, n. 1, e1072, jan./abr. 2025. Disponível em: <https://doi.org/10.22197/rbdpp.v11i1.1072>. Acesso em: 22 maio 2026.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

FRANÇA, Rafael Francisco. Balancing self-incrimination and public safety: a comparative analysis of compelled smartphone unlocking in Brazilian and U.S. legal systems. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 9, n. 3, p. 1371-1420, set./dez. 2023. Disponível em: <https://doi.org/10.22197/rbdpp.v9i3.867>. Acesso em: 22 maio 2026.

GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. O direito de proteção de dados no processo penal e na segurança pública. São Paulo: Marcial Pons, 2021.

GRECO, Luís; GLEIZER, Orlandino. A infiltração online no processo penal: notícia sobre a experiência alemã. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 5, n. 3, p. 1483-1518, set./dez. 2019. Disponível em: <https://doi.org/10.22197/rbdpp.v5i3.278>. Acesso em: 22 maio 2026.

MENDES, Laura Schertel. Habeas data e autodeterminação informativa: dois lados da mesma moeda. *Revista Direitos Fundamentais & Justiça*, Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez. 2018.

MORAIS, Fausto Santos; CARINI, Lucas. Governança ética para construção de confiança em sistemas de inteligência artificial. *Prim@ Facie*, João Pessoa, v. 19, p. 1-26, 2020. Disponível em: <https://periodicos.ufpb.br/index.php/primafacie/article/view/48406>. Acesso em: 21 ago. 2026.

OLIVA, Afonso Carvalho de; PESSOA, Flávia Moreira Guimarães. Bancos de dados e a proteção do consumidor brasileiro: o panóptico pós-moderno. *Prim@ Facie*, João Pessoa, v. 15, n. 28, p. 1-43, 2016. Disponível em: <https://doaj.org/article/f7cebd50b606423da0533f67b6c4a7bf>. Acesso em: 21 ago. 2026.

PRADO, Geraldo. Prova penal e sistema de controles epistêmicos: a quebra da cadeia de custódia das provas obtidas por métodos ocultos. São Paulo: Marcial Pons, 2014.

PRADO, Geraldo. A cadeia de custódia da prova no processo penal. 2. ed. Rio de Janeiro: Marcial Pons, 2021.

RODOTÀ, Stefano. A vida na sociedade de vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SAAD, Marta; ROSSI, Helena Costa; PARTATA, Pedro Henrique. A obtenção das provas digitais no processo penal demanda uma disciplina jurídica própria? Uma análise do conceito, das características e das peculiaridades das provas digitais. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 10, n. 3, e1071, set./dez. 2024. Disponível em: <https://doi.org/10.22197/rbdpp.v10i3.1071>. Acesso em: 22 maio 2026.

SARLET, Ingo Wolfgang; MENDES, Laura Schertel; DONEDA, Danilo (org.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021.

UNIÃO EUROPEIA. Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais. Jornal Oficial da União Europeia, L 119, p. 89-131, 4 maio 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016L0680>. Acesso em: 22 maio 2026.

VAZ, Denise Provasi. Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório. 2012. Tese (Doutorado em Direito) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2012.

WOLTER, Jürgen. O inviolável e o intocável no direito processual penal: reflexões sobre dignidade da pessoa humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal. São Paulo: Marcial Pons, 2018.

ZUBOFF, Shoshana. The age of surveillance capitalism: the fight for a human future at the new frontier of power. New York: PublicAffairs, 2019.

The Criminalization Of Computer Device Intrusion In Brazil: Criminal Typicity, Digital Evidence And Data Protection After The 2021 And 2023 Reforms

Gustavo Henrique de Andrade Cordeiro

Abstract: This article examines the criminalization of computer device intrusion under Brazilian criminal law, focusing on Article 154-A of the Penal Code and the changes introduced by Law No. 14,155/2021 and by the 2023 enactment of the Budapest Convention. The guiding research problem is how to reconcile the reformed criminal provision with the reliability of digital evidence and with the personal data protection regime, without sacrificing fundamental guarantees. The study adopts the deductive method, moving from constitutional and doctrinal premises to specific conclusions about the offence, its evidentiary application and its normative articulation. The research is qualitative, bibliographic, documentary, normative and case-law based, grounded in current legislation, domestic and foreign scholarship and decisions of the higher courts. The findings indicate that the 2021 reform broadened the scope of the offence and removed the requirement of breaching a security mechanism, shifting the core difficulty to the evidentiary domain. It is concluded that the effectiveness of this protection depends on a constitutionally grounded digital chain of custody and on an integrated reading of criminal law and data protection, under the filter of proportionality. The reliability of evidence and the doctrinal containment of the offence emerge, ultimately, as conditions for the legitimacy of this protection under the rule of law.

Keywords: *Computer crimes. Digital evidence. Chain of custody. Personal data protection. Fundamental guarantees.*

DOI: <https://doi.org/10.22478/ufpb.1678-2593.2026v25n58.79171>

Content sob license *Creative Commons*: Attribution-Noncommercial-Nonderivative 4.0 International (CC BY-NC-ND 4.0)

