

QUANDO A INVESTIGAÇÃO INVADE O SISTEMA: HACKING ESTATAL, PROVA DIGITAL E OS LIMITES DA LEGALIDADE

WHEN THE INVESTIGATION INVADES THE SYSTEM: STATE HACKING, DIGITAL EVIDENCE, AND THE LIMITS OF LEGALITY

DOI: <https://doi.org/10.5281/zenodo.22921393>

Resumo: A expansão das técnicas de investigação digital deslocou a persecução penal da apreensão do suporte físico para o acesso oculto e remoto a dispositivos e sistemas. *Hacking* estatal e infiltração por *malware* oferecem alto potencial investigativo, mas também podem alcançar comunicações, arquivos, câmeras, microfones e localização, alterando o próprio ambiente em que a prova é produzida. Este editorial sustenta que a inovação não pode operar sem reserva legal, transparência técnica, contraditório efetivo e cadeia de custódia auditável. A ausência de disciplina específica, inclusive no espaço ainda não preenchido pela chamada LGPD Penal, não autoriza poderes ilimitados nem decisões baseadas em confiança institucional. Propõem-se parâmetros concretos para autorização, execução, preservação e controle dessas medidas, distinguindo a capacidade de descobrir informação da legitimidade de convertê-la em prova confiável.

Palavras-chave: *hacking* estatal; *malware*; prova digital; cadeia de custódia; direitos fundamentais.

Abstract: The expansion of digital investigative techniques has moved criminal prosecution beyond the seizure of physical devices toward covert and remote access to systems and data. State hacking and malware infiltration may produce substantial investigative gains, but they can also reach communications, files, cameras, microphones, and location data while altering the very environment in which evidence is generated. This editorial argues that innovation cannot operate without statutory authorization, technical transparency, effective adversarial participation, and an auditable chain of custody. The absence of a specific framework, including the regulatory gap associated with the proposed Criminal Data Protection Law, does not authorize unlimited investigative powers or decisions based on institutional trust. The article proposes concrete parameters for authorizing, conducting, preserving, and reviewing these measures, distinguishing the capacity to discover information from the legitimacy of converting it into reliable evidence.

Keywords: State hacking; malware; digital evidence; chain of custody; fundamental rights.

1. Introdução

A investigação criminal já não depende apenas da apreensão do aparelho que contém a informação. A conexão em rede, a computação em nuvem e a circulação de dados permitem que o Estado procure, à distância e de modo oculto, aquilo que antes exigia acesso físico. Essa transformação é compreensível diante da criminalidade organizada e transnacional, mas não é juridicamente

neutra. O aumento da capacidade técnica estatal não elimina a necessidade de uma autorização legal; ao contrário, torna mais urgente que a lei defina o que pode ser feito, contra quem, por quanto tempo e sob quais controles.

O *hacking* estatal explora vulnerabilidades para ingressar remotamente em um dispositivo ou sistema. A infiltração por *malware* instala programa não autorizado e pode abrir um

backdoor, isto é, um mecanismo de acesso excepcional que permite consultar e transmitir informações. A instalação pode decorrer de um comportamento induzido do usuário ou da inserção de um dispositivo físico. Uma vez instalado, o programa pode continuar operando sem conexão permanente, aguardando posterior transmissão por internet, *Bluetooth* ou retirada de um suporte. A técnica, portanto, não se limita a “ler” um arquivo: pode alcançar dados na origem, buscar conteúdos armazenados, acompanhar atividades, captar áudio e vídeo e obter localização.

Essa amplitude repercute diretamente sobre a privacidade, a inviolabilidade do domicílio e das comunicações, a autodeterminação informativa e a integridade dos sistemas informáticos. Também modifica a relação entre investigação e prova. Uma busca tradicional delimita, ao menos em tese, um local e um objeto; uma intrusão remota pode converter o dispositivo inteiro em campo de exploração. Uma interceptação passiva acompanha o fluxo comunicacional; o *malware* pode capturar o dado antes do envio ou no destino, internamente ao sistema. A diferença de invasividade não é um detalhe técnico. Ela impede que se trate a nova técnica como simples variação de meios já regulados.

2. Potencial investigativo não é legitimidade probatória

O potencial investigativo dessas ferramentas é real. Elas podem revelar informações inacessíveis por métodos convencionais e ampliar a capacidade de reconstrução de fatos complexos. Mas descobrir mais não significa provar melhor, e obter informação não significa obtê-la legitimamente. O dado alcançado por uma intrusão pode ser relevante e, ainda assim, resultar de medida sem habilitação normativa, de autorização genérica ou de procedimento incapaz de demonstrar sua autenticidade. A utilidade estratégica da técnica não substitui a legalidade da operação nem a confiabilidade do resultado.

A distinção é decisiva porque o sistema-alvo pode ser alterado pela própria intervenção. A operação pode modificar registros, produzir novos arquivos, interromper processos, contaminar metadados ou dificultar a reconstrução do estado original do dispositivo. Mesmo quando não há intenção de adulterar, a presença do agente técnico no ambiente digital introduz uma variável que precisa ser identificada, controlada e documentada. O Estado não pode apresentar como espelho neutro um sistema que ele próprio acessou e potencialmente transformou.

A questão não é demonizar a tecnologia, mas recusar a ideia de que sua eficiência cria autorização. A ausência de regulamentação específica para a segurança pública e a persecução penal, tal como ressaltado no texto-base, não pode ser convertida em licença para acessos desmedidos. A Lei Geral de Proteção de Dados estabeleceu uma estrutura geral de proteção de dados pessoais, mas excluiu de seu âmbito as operações destinadas exclusivamente à segurança pública e à investigação e repressão de infrações penais, nos termos de seu art. 4º, III. O espaço reservado aos debates sobre a chamada LGPD Penal permanece, assim, uma lacuna que não deve ser preenchida por analogias expansivas contra direitos fundamentais.

Em matéria de intrusão estatal, a reserva legal cumpre dupla função. Ela habilita uma ingerência que, sem norma, não pode ser presumida; e limita o poder habilitado por meio de pressupostos, duração, finalidade e fiscalização. Não basta uma decisão judicial que empregue expressões amplas como “acesso integral” ou

“monitoramento do dispositivo”. Quanto maior a capacidade da ferramenta, maior deve ser a precisão da autorização. A ordem judicial não pode delegar ao operador a definição posterior do objeto, do alcance e da duração da medida.

3. A prova digital exige uma lógica de desconfiança

A confiabilidade do resultado começa antes da análise pericial. Como observa **Caio Badaró Massena** (2023, p. 19), a prova digital é uma “fonte de prova cujo manejo é delicado, por apresentar alto grau de vulnerabilidade a erros (conscientes ou não), e para a qual se exige, na maior parte dos casos, intervenção técnica”. A afirmação vale com especial força para dados obtidos por *hacking* ou *malware*: a defesa precisa saber qual vulnerabilidade foi explorada, que componente foi instalado ou acionado, quais operações foram executadas e que vestígios foram deixados no dispositivo.

A cadeia de custódia não é formulário posterior para conferir aparência de regularidade ao que já foi produzido. Ela deve contar a história do elemento desde a decisão que autorizou a medida, passando pela seleção do alvo, pela configuração da ferramenta, pela coleta, pela transmissão, pelo armazenamento, pela extração e pela apresentação em juízo. A documentação precisa registrar quem realizou cada ato, quando, com qual equipamento, versão e configuração, sob quais parâmetros e com que resultado. *Logs*, metadados, *hashes*, imagens forenses e registros de acesso devem ser preservados de modo a permitir a verificação independente, sem confundir a existência de um arquivo com a prova de sua integridade.

Gustavo Badaró (2024, p. 8) sintetiza a relação entre método e valor probatório ao afirmar: “É imprescindível que o método empregado garanta a integridade do dado digital e, com isso, a força *probandi* do conteúdo probatório por ele representado”. A integridade, aqui, não é atributo abstrato do arquivo. É a conclusão possível quando o método de obtenção, conservação e análise pode ser explicado, repetido e criticado. Se a operação foi invasiva, a exigência metodológica não diminui, aumenta.

Por isso, a cadeia deve incorporar também a lógica da desconfiança. Não se trata de presumir fraude de cada agente público, mas de reconhecer a vulnerabilidade estrutural do vestígio digital e a assimetria de informação entre acusação e defesa. O próprio Estado controla a ferramenta, os registros técnicos e, muitas vezes, a seleção do material que chega aos autos. A confiança pessoal entre agentes não substitui uma trilha verificável. A prova deve ser confiável porque pode ser auditada, e não porque a acusação afirma que foi corretamente produzida.

Essa exigência alcança a admissibilidade. Os estudos sobre a cadeia de custódia da prova digital destacam que, no processo penal, “deve-se comprovar a sua autenticidade, integridade e confiabilidade, qual seja, a sua mesmidade” (**Saad Netto; Avolio; Borri**, 2026, p. 18). A mesmidade significa demonstrar que o elemento examinado é o mesmo que foi obtido, e que o percurso entre obtenção e julgamento não ocultou acréscimos, supressões ou transformações relevantes. Se o método é incapaz de assegurar esse mínimo, a discussão não é apenas sobre peso probatório: é sobre a aptidão do material para ingressar validamente no processo.

4. Parâmetros para uma autorização responsável

Uma disciplina adequada não precisa prever o nome comercial de cada tecnologia, mas deve fixar limites materiais e procedimentais que resistam à obsolescência técnica. O primeiro parâmetro é a delimitação objetiva do fato investigado. A medida deve indicar a hipótese concreta, sua conexão com a pessoa atingida e a finalidade probatória que justifica a intrusão. A delimitação subjetiva deve identificar os sujeitos, o dispositivo ou sistema, o local de execução e o meio técnico autorizado. Não é admissível transformar uma ordem dirigida a um investigado em autorização para explorar dados de terceiros indistintamente.

O segundo parâmetro é a necessidade, acompanhada de subsidiariedade e proporcionalidade. A decisão deve explicar por que a informação não pode ser obtida por meio menos invasivo e por que o grau de acesso é compatível com a gravidade do fato. Um catálogo legal de crimes, eventualmente graduado conforme a gravidade, pode impedir que a técnica excepcional se torne instrumento ordinário. A excepcionalidade não decorre apenas da dificuldade operacional da investigação; decorre do impacto sobre direitos fundamentais.

O terceiro parâmetro é temporal. A autorização deve estabelecer prazo máximo, condições de renovação e cessação imediata quando alcançada a finalidade ou desaparecida a necessidade. O monitoramento não pode permanecer aberto por inércia administrativa. Cada extensão deve ser justificada com base no que foi efetivamente produzido, e não em uma expectativa genérica de que novos dados talvez surjam.

O quarto parâmetro é a transparência técnica sob controle judicial. A ordem e os relatórios de execução devem indicar a ferramenta empregada, sua versão, seus módulos, suas permissões, o modo de instalação, as alterações possíveis no sistema e as medidas adotadas para reduzi-las. A documentação não precisa expor vulnerabilidades de modo irresponsável, mas deve ser suficiente para que o juiz e a perícia defensiva compreendam o funcionamento relevante da operação. O segredo operacional não pode cobrir a própria confiabilidade do resultado.

O quinto parâmetro é o registro integral. Devem ser preservados os comandos, logs, metadados, horários, identificadores,

transferências e incidentes, inclusive os resultados exculpatórios, inconclusivos ou estranhos ao objeto da autorização. A seleção unilateral de trechos favoráveis à acusação impede o contraditório. Quando houver dados de terceiros ou material protegido por sigilo, devem existir regras de separação, retenção, descarte e restrição de divulgação, com controle documentado de cada decisão.

A tecnologia pode
reforçar a qualidade
da prova quando
acompanha
governança, capacitação
e padronização. Sem
essas condições,
ferramentas de
validação, inteligência
artificial ou registros
tecnológicos não
funcionam como
garantias automáticas
de verdade; apenas
deslocam o ponto em
que a prova precisa ser
controlada.

5. Contraditório efetivo e auditoria independente

O acesso defensivo não pode começar apenas quando a acusação escolhe o que juntar. A defesa deve receber elementos necessários para testar a autenticidade e a integridade do resultado: imagem ou cópia forense pertinente, documentação da ferramenta, registros de execução, metadados e informações sobre limitações conhecidas. O acesso deve ser tecnicamente utilizável, com tempo e meios para exame por profissional habilitado. Sem isso, o contraditório se reduz à possibilidade formal de contestar uma narrativa já filtrada pelo órgão que realizou a intrusão.

A auditoria independente é o complemento institucional desse acesso. Em casos de maior invasividade, a perícia não deve depender exclusivamente da equipe que operou o *malware* ou conduziu o *hacking*. Um órgão pericial independente, ou profissional escolhido sob controle judicial, deve poder verificar a cadeia, reproduzir etapas relevantes, avaliar a ferramenta e apontar alterações ou limites que comprometam a conclusão. A repetibilidade não exige que toda operação seja recriada em um ambiente idêntico, mas que o caminho técnico seja suficientemente documentado para permitir escrutínio real.

É um adequado critério de orientação, a consideração de que “a inovação nunca pode se sobrepor à justiça em si. Ao contrário disso, ela deve potencializá-la, sempre respeitando os direitos fundamentais, para que a confiança da sociedade nas instituições seja fortalecida” (Neves; Rosa, 2025, p. 31). A tecnologia pode reforçar a qualidade da prova quando acompanha governança, capacitação e padronização. Sem essas condições, ferramentas de validação, inteligência artificial ou registros tecnológicos não funcionam como garantias automáticas de verdade; apenas deslocam o ponto em que a prova precisa ser controlada.

A conclusão é de contenção, não de imobilismo. O Estado pode investigar no ambiente digital, mas não pode fazer do dispositivo alheio um território sem fronteiras jurídicas. Como lembram **Nereu Giacomolli e Luiz Eduardo Cani** (2024, p. 6), “Os custos operacionais jamais justificam a supressão dos direitos e das garantias fundamentais”. A legitimidade probatória exige que a busca por eficiência se submeta a uma habilitação legal expressa, a uma decisão judicial específica, à necessidade demonstrada, a prazo definido, a registro integral, à preservação técnica e ao contraditório.

Em síntese, *hacking* estatal e *malware* não devem ser avaliados apenas pelo que conseguem descobrir. Devem ser avaliados pelo modo como ingressam no sistema, pelo que podem alterar, pelo que registram, pelo que preservam e pelo que permitem à defesa verificar. A cadeia de custódia auditável é a ponte entre a capacidade investigativa e a prova judicialmente confiável.

Sem reserva legal, transparência técnica, acesso defensivo e fiscalização independente, a inovação pode produzir informação; não produz, por si só, legitimidade probatória.

Como citar (ABNT Brasil)

INSTITUTO BRASILEIRO DE CIÊNCIAS CRIMINAIS. Quando a investigação invade o sistema: hacking estatal, prova digital e os limites da legalidade. *Boletim IBCCRIM*, São Paulo, v. 34, n. 407, p. 2-5, 2026. DOI: 10.5281/

zenodo.22921393. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/3613. Acesso em: 1 out. 2026.

Referências

BADARÓ, Gustavo Henrique Righi ivahy. Os *standards* metodológicos de produção na prova digital e a importância da cadeia de custódia. *Boletim IBCCRIM*, São Paulo, v. 29, n. 343, p. 7-9, 2024. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1325. Acesso em: 21 set. 2026.

GIACOMOLLI, Nereu; CANI, Luiz Eduardo. O acesso autorizado a aparelhos smart: burla ao agente infiltrado digital? *Boletim IBCCRIM*, São Paulo, v. 30, n. 352, p. 4-6, 2024. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1435. Acesso em: 21 set. 2026.

MASSENA, Caio Badaró. A propósito da cadeia de custódia das provas digitais no Processo Penal: breves notas sobre lógica da desconfiança, assimetria informacional e direito de defesa. *Boletim IBCCRIM*, São Paulo, v. 31, n. 368,

p. 19-21, 2023. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/506. Acesso em: 21 set. 2026.

NEVES, Luiz Gabriel Batista; ROSA, Hiuston César dos Santos. Tecnologia e prova digital: desafios e propostas para a cadeia de custódia no judiciário. *Boletim IBCCRIM*, São Paulo, v. 34, n. 398, p. 29-31, 2025. DOI: 10.5281/zenodo.17914684. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/2654. Acesso em: 21 set. 2026.

SAAD NETTO, Cláudio; AVOLIO, Luiz Francisco Torquato; BORRI, Luiz Antonio. A cadeia de custódia da prova digital: dissensos e consensos entre teoria e prática. *Boletim IBCCRIM*, São Paulo, v. 34, n. 403, p. 18-21, 2026. DOI: 10.5281/zenodo.19697006. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/2761. Acesso em: 21 set. 2026.

