Vazamentos de dados íntimos revela falha na cadeia de custódia digital

14/03/2026

A exposição pública de conversas privadas extraídas de processos penais revela falhas na cadeia de custódia digital e aponta para a necessidade de novos padrões de governança tecnológica da prova.

Freepik

A divulgação pública de mensagens privadas extraídas de processos e procedimentos penais voltou a expor um problema recorrente no sistema de justiça brasileiro. Conversas íntimas, referências à vida sexual e até descrições anatômicas de pessoas investigadas passaram a circular fora do ambiente institucional, muitas vezes sem qualquer relevância para os fatos apurados. Mais do que episódios de constrangimento público, esses vazamentos revelam fragilidades estruturais na forma como o Estado administra a custódia de provas digitais.

Em muitos desses episódios, o material divulgado sequer diz respeito a atos diretamente relacionados ao objeto do processo penal. Trata-se de comunicações privadas que ingressaram nos autos como elementos de prova ou como dados capturados em medidas investigativas e que, em algum ponto do percurso institucional, passaram a circular fora do ambiente de custódia.

Esse fenômeno revela uma tensão própria do processo penal contemporâneo. A produção de prova digital passou a envolver volumes crescentes de dados pessoais e comunicações privadas que frequentemente ultrapassam os limites estritos do fato investigado. A Constituição estabelece, no artigo 5º, incisos X e XII, a inviolabilidade da intimidade, da vida privada e do sigilo das comunicações. Essas garantias não desaparecem quando uma pessoa passa a figurar em um processo penal.

A obtenção de comunicações privadas pode ser juridicamente legítima quando autorizada judicialmente ou vinculada à produção de prova. Contudo, a legitimidade da coleta não implica autorização para sua circulação irrestrita. Uma vez que comunicações privadas ingressam em autos judiciais, relatórios periciais ou procedimentos penais, passa a existir um dever institucional claro de custódia da informação.

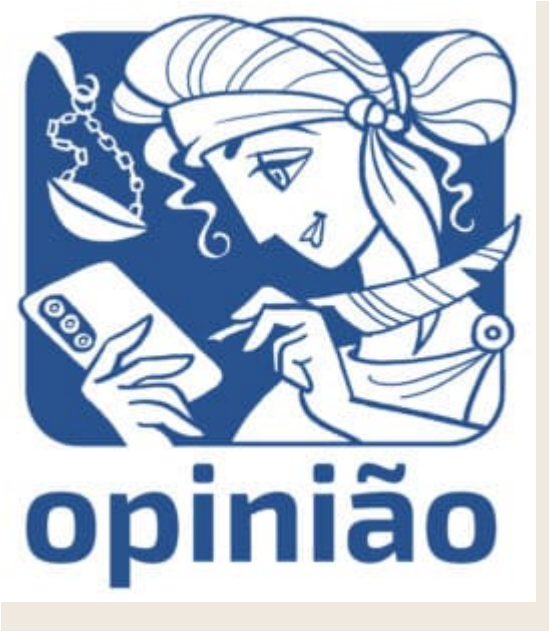
Essa obrigação possui fundamento direto no Direito Processual Penal. A Lei nº 13.964/2019 introduziu no Código de Processo Penal a disciplina da cadeia de custódia da prova, hoje prevista nos artigos 158-A a 158-F. O objetivo dessas normas é garantir a rastreabilidade da evidência desde sua coleta até sua utilização em juízo, preservando integridade, autenticidade e confiabilidade do elemento probatório.

Historicamente, a noção de cadeia de custódia foi desenvolvida para assegurar a integridade da prova e garantir que o material apresentado em juízo corresponda efetivamente àquilo que foi apreendido durante a investigação. Trata-se de um instrumento clássico de proteção ao devido processo legal e ao direito de defesa, voltado a evitar adulterações, contaminações ou manipulações indevidas do elemento probatório.

No contexto das provas digitais, contudo, essa lógica precisa ser ampliada

A cadeia de custódia passa a desempenhar também uma função de proteção de direitos fundamentais.

Spacca



Quando comunicações privadas, imagens ou informações íntimas passam a integrar procedimentos penais, o controle rigoroso sobre quem pode acessar esses dados deixa de ser apenas uma exigência probatória e passa a ser também uma medida de proteção da intimidade e da dignidade das pessoas envolvidas. A exposição pública posterior de conteúdos íntimos que nada acrescentam à apuração dos fatos pode produzir danos irreversíveis à vida pessoal e profissional dos envolvidos, danos que não são reparados por absolvições posteriores ou pelo reconhecimento da irrelevância probatória daquele material.

Em um ambiente de circulação massiva de informação, a violação da intimidade se propaga rapidamente e tende a afetar de forma particularmente intensa mulheres e pessoas expostas a estigmas sociais associados à sexualidade. Por essa razão, a cadeia de custódia digital precisa ser pensada não apenas como garantia da confiabilidade da prova, mas também como instrumento de proteção da esfera privada diante do poder punitivo do Estado.

Na era da prova digital, proteger a intimidade não depende apenas de normas jurídicas, mas de sistemas capazes de registrar e auditar cada acesso à informação sensível.

Nesse contexto cresce internacionalmente o interesse por soluções tecnológicas destinadas a fortalecer a cadeia de custódia digital. Entre elas destaca-se o uso de sistemas baseados em registros distribuídos.

A tecnologia conhecida como *blockchain* possui características particularmente relevantes para a gestão de evidências digitais. Trata-se de um livro-razão distribuído no qual cada registro é encadeado criptograficamente ao anterior por meio de funções *hash*. Cada bloco incorpora o *hash* do bloco precedente, formando uma sequência cronológica de registros cuja alteração retroativa se torna computacionalmente impraticável.

Essa arquitetura permite a criação de registros imutáveis de eventos.

Em aplicações voltadas à cadeia de custódia digital, o documento sensível não precisa ser armazenado diretamente na *blockchain*. Em geral utiliza-se uma arquitetura híbrida. O arquivo permanece em repositórios seguros fora da cadeia, enquanto o sistema registra na *blockchain* o *hash* criptográfico do documento e os metadados de cada interação.

Cada acesso ao arquivo pode gerar automaticamente um registro contendo identificação do usuário autenticado, marca temporal verificável, *hash* do documento acessado e natureza da operação realizada, como visualização, cópia ou transferência.

Esse registro passa então a integrar uma cadeia de blocos permanentemente auditável.

O resultado prático é a criação de uma trilha técnica imutável sobre a circulação da informação. Diferentemente de logs administrativos tradicionais, esses registros não podem ser apagados ou alterados sem comprometer a integridade da cadeia. Embora os procedimentos atuais de extração forense já contem com um elemento técnico altamente relevante de preservação da prova — o registro de *hash* criptográfico do material coletado —, que desempenha papel essencial na demonstração de sua integridade e autenticidade, esse mecanismo atua sobretudo no plano da conservação do conteúdo extraído. Trata-se de uma salvaguarda importante, consolidada e indispensável para a cadeia de custódia, pois permite verificar se os dados examinados permanecem idênticos àqueles originalmente obtidos.

Ainda assim, o *hash*, por si só, não oferece rastreabilidade plena sobre a circulação institucional posterior dessas informações, especialmente quanto à identificação de quem acessou o conteúdo, em que momento, sob qual autorização e para qual finalidade.

É nesse ponto que o sistema sugerido apresenta ganho adicional: ao registrar de forma imutável e auditável cada evento de acesso, visualização, cópia, transferência ou compartilhamento de documentos sensíveis, ele amplia a cadeia de custódia da esfera estritamente pericial da integridade para a esfera institucional da governança da informação. Com isso, além de preservar a autenticidade técnica da prova, o modelo proposto reforça a prevenção, a auditoria e a responsabilização em

hipóteses de vazamento ou uso indevido de dados íntimos obtidos em investigações.

Aplicado ao contexto do processo penal, um sistema desse tipo permitiria reconstruir com precisão a sequência de acessos institucionais a documentos sensíveis. Caso determinado conteúdo viesse a público de forma indevida, seria possível identificar quais agentes tiveram acesso ao material e em qual ordem temporal.

Nenhuma tecnologia elimina completamente o risco de vazamentos

Um agente ainda poderia reproduzir manualmente um conteúdo ou registrar imagens externas de um documento. Ainda assim, a existência de registros criptográficos imutáveis altera profundamente o ambiente institucional.

Primeiro porque amplia a capacidade de investigação de vazamentos. Segundo porque produz um efeito preventivo relevante. Quando cada acesso deixa um rastro auditável permanente, o incentivo para o uso indevido da informação diminui.

Esse debate aponta para possíveis evoluções normativas e institucionais. A legislação processual poderia reconhecer explicitamente a cadeia de custódia digital como requisito obrigatório na gestão de evidências eletrônicas sensíveis. Sistemas utilizados por tribunais, órgãos de persecução penal e comissões parlamentares poderiam ser obrigados a implementar mecanismos de registro imutável de acesso a documentos classificados como sensíveis.

Também seria possível desenvolver protocolos nacionais de governança de evidências digitais alinhados a padrões internacionais de preservação, auditoria e integridade da informação.

Vazamentos recorrentes de dados íntimos extraídos de ambientes institucionais não representam apenas episódios de constrangimento público. Eles revelam fragilidades na arquitetura informacional do próprio sistema de justiça.

Quando conversas privadas sobre sexualidade, características corporais ou aspectos íntimos que nada acrescentam à apuração dos fatos passam a circular fora do ambiente institucional, a questão deixa de ser apenas política ou midiática. Surge um problema estrutural de gestão da prova digital no processo penal.

Se hoje existem tecnologias capazes de registrar de forma verificável cada acesso a um documento sensível, a persistência desses vazamentos deixa de ser um simples acidente informacional. Ela passa a indicar uma lacuna institucional que o próprio sistema de justiça precisará enfrentar.

Fonte: https://conjur.jumps.com.br/2026-mar-14/vazamentos-de-dados-intimos-revela-falha-na-cadeia-de-custodia-digital/