A fiabilidade e o disclosure da prova digital

09/12/2023

Atualmente, somos testemunhas de um avanço da tecnologia que implica numa verdadeira revolução digital. De uma inicial (e precária) digitalização, hoje vivemos a era da "plasticidade" da informação — transmitida na forma de texto, áudio, vídeo, etc. — e de novas possibilidades de interconexões que propiciam o surgimento da internet das coisas. Esse movimento disruptivo tem a potencialidade de amalgamar o mundo analógico ao virtual e fomentar o surgimento de um novo domínio: o das informações digitais. "Nele, as informações adquirem caráter universal, atemporal e plástico: elas estão por toda parte, são acessíveis a qualquer momento e podem ser lidas por variados algoritmos"[1].

Se de um lado, inicia-se a construção de uma legislação e uma doutrina especializada a respeito do tema, de outro, sabemos que o "tempo" da tecnologia anda sempre à frente de seu disciplinamento legal. Na seara penal, esse descompasso evidencia a debilidade do aparato estatal para o enfrentamento de uma criminalidade cada vez mais "tecnológica" e, ao mesmo tempo, a utilização de práticas investigativas prospectivas que implicam na transgressão do núcleo sensível da intimidade e do direito de defesa. Vivemos um embate entre uma legislação ainda construída "para o mundo físico" e a necessidade de investigar informações "em realidade virtual".

Spacca

É cada vez mais frequente a busca por provas digitais para a solução de demandas cíveis e casos criminais complexos e há quem sustente que, num futuro próximo, a prova digital possa até mesmo superar a evidência física. Em realidade, "*a partir de nossas buscas no Google ou em outros motores de buscas, se pode inferir nossos desejos, medos, preocupações, expectativas, etc. Enquanto as pessoas mentem para os seus amigos, amantes, médicos e até para elas mesmas, tendem a compartilhar informação verdadeira com o Google. Facebook, com base nos likes que outorgamos, pode prever com um alto grau de acerto a nossa religião, orientação sexual, ideológica política, etc*"[2].

Uma vez que grande parte da nossa vida está registrada em dispositivos de armazenamento digital, não há dúvida que tais instrumentos (físicos ou nas nuvens) refletem a nossa mais profunda intimidade e, ao mesmo tempo, são importantes fontes de informação. Mas a justificativa de uma persecução penal eficiente não pode frustrar expectativas legítimas e obliterar o devido processo legal em seu conjunto de princípios e regras que estruturam um processo equitativo, fomentando o uso de técnicas de mineração de dados cada vez mais sofisticas e carentes de um marco jurídico claro. Assim, qualquer investigação/instrução que tenha como suporte as provas digitais, apenas poderá seguir caso respeitada a *cadeia de custódia* e o *acesso à prova*, pois a "paridade de armas e conhecimento integral das fontes de prova obtidas durante a investigação criminal articulam-se para o concreto exercício do direito de defesa, que não fica restrito aos elementos informativos que interessam apenas à acusação"[3]. Tal conclusão é cada vez mais evidente na jurisprudência dos nossos tribunais superiores.

Em recente decisão monocrática, o ministro Toffoli[4] observou que não é possível o amplo exercício do direito de defesa sem que o investigado/acusado tenha acesso a todos os elementos de prova — já documentados — que norteiam a acusação, incluindo-se os ofícios dirigidos aos provedores de internet e operadoras de telefonia, sem os quais não seria possível o controle sobre o rastreamento dos vestígios da cadeia de custódia da prova digital:

> *"Verifica-se, portanto, que a defesa do reclamante não teve acesso a todos os elementos da prova, mormente os requeridos por meio dos ofícios dirigidos aos provedores de internet (…) e às operadoras de telefonia (…). Logo, a sequência do processo crime sem viabilizar-se o acesso do acusado às informações pretendidas, tal como apontado na inicial, impede o amplo exercício do direito de defesa.*
>
> *(…).*
>
> *Nesse contexto, independentemente das circunstâncias expostas pela autoridade reclamada, é legítimo o direito de o reclamante ter acesso aos elementos devidamente formalizados e encartados aos autos do procedimento em que é investigado, especialmente o alusivo aos ofícios dirigidos aos provedores de internet e operadoras de telefonia.*
>
> *Afinal, é fundamental à defesa saber a data de início e fim da interceptação telefônica, tendo em vista a eventual ilicitude de diálogos captados após a determinação judicial de interrupção se utilizados no contexto incriminatório, devendo a autoridade reclamada fornecer os dados sobre os prazos da medida.*
>
> *(…).*
>
> *O controle sobre o rastreamento dos vestígios, portanto, é fundamental para a reconstrução dos fatos por meio de procedimentos que assegurem a integridade dos elementos obtidos e preservados desde a fase inicial até o julgamento da ação penal.*
>
> *Uma vez quebrada a cadeia de custódia, surge o risco concreto de adulteração ou interferência nos elementos de prova, em prejuízo à apuração da verdade real, além de inviabilizar o exercício do contraditório pela defesa".*

A decisão evidencia a enorme preocupação com a chamada "*fiabilidade probatória*"[5], a qual, identificada como a "*comprovação (demonstração) da correção de um procedimento de obtenção e preservação dos elementos probatórios*" [6] é, como adverte Geraldo Prado, condição para a valoração do elemento de prova:

> *"A fiabilidade probatória refere-se ao esquema de ingresso do elemento probatório no procedimento em cujo âmbito, posteriormente, este elemento poderá ser objeto de avaliação e diz muito especificamente com a questão dos controles epistêmicos, compreendidos nesta etapa como 'controles de entrada'.*
>
> *A valoração da prova, seja para qualquer fim, por sua vez cuida da corroboração de uma hipótese e se consubstancia em um juízo de valor relativamente ao grau de convencimento alcançado pelo juiz a partir do exame de determinado elemento probatório. Lógica e cronologicamente, a questão da valoração da prova é posterior à da sua fiabilidade.*
>
> *São coisas diversas, portanto, saber se um determinado elemento probatório está em condições de ser avaliado, ou seja, se o elemento probatório pode ser objeto de avaliação, e em caso de ser 'avaliável', saber que valor o juiz lhe atribui. A primeira atividade é denominada 'fiabilidade probatória'"[7].*

Objetivando diminuir o risco intrínseco quando do exame forense de qualquer dispositivo de armazenamento digital, Pedro Eleutério e Marcio Machado, identificam quatro fases fundamentais de observância cogente: a preservação, a extração, a análise e a formalização. A preservação é a garantia de que o material colhido não será alterado. O espelhamento consiste na cópia "exata e fiel dos dados (bit a bit) contidos em um dispositivo de armazenamento computacional para outro"[8]. A extração é a "recuperação de todas as informações contidas na cópia dos dados provenientes da fase de preservação anteriormente realizada"[9]. Na análise, o perito examina as informações extraídas buscando identificar indícios relacionados ao ilícito investigado. E, a formalização, é a confecção do laudo pericial, momento em que o perito descreve "com objetividade e clareza os métodos e exames realizados para a sua própria

segurança e para a transparência do processo forense como um todo”[10].

Atualmente, vivemos uma grande discussão a respeito do melhor procedimento a ser utilizado para garantir a autenticidade e a conservação da prova digital. Isso se deve, adverte Laura Merkel, diante da sua natureza precária: *“Estas son fuentes facilmente alterables. La operación, aparentemente más trivial, podría causar modificaciones o perdidas no deseadas, socavando la credibilidade del material recogido”*[11]. Daí segue a necessidade da construção de resoluções que possam orientar a melhor prática possível.

Descendo uma camada a mais e partindo do pressuposto de que o meio de obtenção de prova cumpriu todas as exigências que garantem a sua fiabilidade, é necessário nos afastarmos de um arquétipo de valoração que introduza, *ex ante*, um prognóstico de irrefutabilidade àquilo que foi buscado. A verificabilidade ou refutabilidade da hipótese carreada pela acusação deve ser filtrada a partir do confronto dialético com a hipótese adversa construída pela defesa.

Contudo, a atuação defensiva parte de uma premissa apodíctica, ou seja, a necessidade do *disclosure* de tudo aquilo que foi coletado na fase investigativa. Não é possível agir — ou mesmo silenciar — sem conhecer. Daí segue a importância do contraditório como um mecanismo de aferição da fiabilidade probatória, na linha desenvolvida por Ferrer Bentrán:

> *“(…)*
>
> *Sin pretensión de exhaustividad, puede decirse que el principio de contradicción opera permitindo cuatro tipos de controles probatórios: 1) un control sobre la correcta aplicación de las reglas epistemológicas y jurídicas sobre la admisión de la prueba (i. e., el principio de admisión de toda prueba relevante y las excepciones estabelecidas por reglas de exclusión jurídicas); 2) la práctia de la prueba de forma contradictoria, esto es, permitiendo la intervención de las partes en la misma; 3) la posibilidad de proponer pruebas contrarias a las oferecidas por la outra parte procesal, de modo que permita vencer a éstas y/o corroborar una hipótesis fáctica distinta e incompatible; 4) la posibilidad de proponer pruebas de segundo orden (o pruebas sobre la prueba) que impugnen la fiabilidade de pruebas oferecidas por la outra parte”[12].*

É a partir do confronto de narrativas que se alcançará uma perspectiva mais dilatada quanto ao objeto do processo (a pretensão processual/acusatória trazida com a imputação), amplificando a percepção do magistrado quanto ao grau de corroboração de uma hipótese. Recordemos que na esfera processual a pretensão acusatória é construída a partir da imputação, ou seja, o conteúdo da imputação corresponde à “afirmação do fato que se atribui ao sujeito, a afirmação de um tipo penal e a afirmação da conformidade do fato com o tipo”[13]. A denúncia gesta uma hipótese a respeito de um fato — que pode ou não ter acontecido — que caberá ao magistrado julgar se ocorreu. Com efeito, trata-se de uma proposição a respeito daquilo que, na visão da acusação, pode ter ocorrido no mundo fenomênico.

A fiscalização do que foi efetivamente buscado na esfera investigatória não deve ser unicamente realizada a partir de relatórios de investigação, muitas vezes confeccionados sob uma metodologia abdutiva. O contexto da investigação está umbilicalmente ligado à formulação de hipóteses que condicionam o olhar a respeito do que é produzido. “E quem investiga, exatamente por formular a hipótese explicativa, compromete-se com a mesma e deixa de ter uma posição neutra quanto à sua confirmação e refutação”[14]. Daí advém o direito do defensor de ter acesso a todos os elementos – já documentados – que corporificam a investigação.

A aplicação da teoria do sopesamento probatório (tema que abordaremos num futuro próximo) envolve uma dificuldade sísifa, especialmente quando a atividade valorativa encontra sustentáculo em uma prova digital imperfeita, pois as peças ausentes do quebra-cabeça podem muito bem transformar a imagem de um gato em um coelho, numa forma de um mimetismo probatório sob a lupa de quem deveria conhecer o todo, mas só conhece parte dele. A adulteração do conteúdo digital (p. ex., a inconsistência do código *hash**[15]***), ou o extravio de uma parte dele, pode ser suficiente a infamar a integridade e a autenticidade das informações extraídas, afetando a sua credibilidade como elemento de convicção.

Destarte, identificando o direito à prova como um consectário do devido processo legal e um elemento indissociável aos princípios do contraditório e da ampla defesa[16], a decisão acima referenciada reforça duas pilastras fundamentais da prova digital: o respeito à cadeia de custódia e o *disclosure* de todos os elementos que corroboram a hipótese acusatória.

[1] HILGENDORF, Eric. Digitalização e direito. Orlandino Gleizer (org. e trad.). São Paulo: Marcial Pons, 2020, p. 20.

[2] POLANSKY, Jonathan A. Garantías Constitucionales del Procedimiento Penal en el entorno digital. Buenos Aires: Hammurabi, 2020, p. 21. Daí segue a importância do Big Data: "(…) determinadas fontes online conseguem fazer com que as pessoas admitam coisas que não admitiriam em nenhum outro lugar. Elas agem como um soro digital da verdade. Pense nas buscas do Google. Lembre-se das condições que tornam as pessoas mais honestas. Online? Sim. Sozinha? Sim. Ninguém conduzindo a pesquisa? Sim. (…). Mesmo que esteja mentindo para si mesmo, ainda assim o Google pode saber a verdade". (STEPHENS-DAVIDOWITZ, Seth. Todo mundo mente: Big Data, nossos dados e o que a internet nos diz sobre quem realmente somos. Wendy Campos (tradutor). Rio de Janeiro: Alta Books, 2018, p. 130).

[3] PRADO, Geraldo. A cadeia de custódia da prova no processo penal, 2ª. ed., Rio de Janeiro: Marcial Pons, 2021, p. 175.

[4] STF, Rcl 62566/PR, j. em 24/11/2023.

[5] PRADO, Geraldo. A cadeia de custódia da prova no processo penal, 2ª. ed., Rio de Janeiro: Marcial Pons, 2021, p. 144. Em sentido semelhante, Thamay e Tamer observam que: "A utilidade da prova digital passa necessariamente pela observância de três fatores principais (i) autenticidade; (ii) integridade; e (iii) preservação de cadeia de custódia. E, ao se falar em utilidade, quer se dizer que é o respeito a esses três fatores ou qualidades da atividade probatória digital que vai permitir que ela seja utilizada sem questionamentos válidos ou minimamente hábeis a desconstituir seu valor agregado". (THAMAY, Rennan; TAMER, Mauricio. Provas no Direito Digital. Conceito da prova digital, procedimentos e provas digitais em espécie. São Paulo: Thomson Reuters Brasil, 2020, p. 39).

[6] PRADO, Geraldo. A cadeia de custódia da prova no processo penal, 2ª. ed., Rio de Janeiro: Marcial Pons, 2021, p. 146.

[7] Ibid., p. 144. Em artigo correlato, o autor ressalta: "A auditabilidade da prova digital que viabilize a sua rastreabilidade, reconstituindo-se as etapas com a confirmação da integridade e autenticidade da informação colhidas, revela-se condição *sine qua non* de validade jurídica do ato probatório". (PRADO, Geraldo. A cadeia de custódia da prova digital: desafios decorrentes das novas tecnologias. In. Homenagem ao Ministro Rogerio Schietti. 10 anos de STJ. São Paulo: Migalhas, p. 380).

[8] ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira. Desvendando a Computação Forense. São Pauo: Novatec, 2019, p. 61.

[9] Ibid., p. 69.

[10] Ibid., p. 79.

[11] MERKEL, Laura. Derechos humanos e investigaciones policiales. Una tensión constante. Madrid: Marcial Pons, 2022, p. 75.

[12] FERRER BELTRÁN, Jordi. La valoración racional de la prueba. Madrid: Marcial Pons, 2007, p. 88.

[13] BADARÓ, Gustavo, p. 68.

[14] BADARÓ, Gustavo, p. 147.

[15] "O que torna esse tipo de função [função unidirecional hash] extremamente utilizada para a verificação de integridade de dados computacionais é o fato de que uma simples alteração na informação de entrada do algoritmo gerará uma sequência de bits (valor hash) completamente diferente. Assim, se o conteúdo de um arquivo é submetido a uma função unidirecional e, em seguida, seu conteúdo é alterado em um único bit e submetido novamente à mesma função, duas sequências de bits completamente diferentes serão obtidas como resultado da função de autenticação, (…). Dessa forma, utilizando esse conceito, é possível se criar mecanismos seguros para a detecção de alteração em um conteúdo digital". (ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira. Desvendando a Computação Forense. São Pauo: Novatec, 2019, p. 152).

[16] BEDAQUE, José Roberto dos Santos. Poderes instrutórios do juiz, 7ª, ed. rev., atual., e ampl., São Paulo: Editora Revista dos Tribunais, 2013, p. 25.

Fonte: https://conjur.jumps.com.br/2023-dez-09/a-fiabilidade-e-o-disclosure-da-prova-digital/