Podem os algoritmos racionalizar a cadeia de custódia digital?

Sob o título "Podem os algoritmos racionalizar a investigação criminal?", Marcella Mascarenhas Nardelli e Fabiana Alves Mascarenhas apresentaram o uso de "máquinas" para melhoria do desempenho da atividade investigatória (veja aqui), anotando: "*Descreve-se que a maneira viável para investigadores da polícia ou julgadores de fato sistematizarem a informação reunida é a construção de narrativas sobre o que poderia ter acontecido, que explicariam o que poderia ter causado a disponibilidade das provas. Por sua vez, defende-se ainda um método de construção de argumentos a partir da prova disponível para as hipóteses, aplicando generalizações de senso comum. O projeto de* ***software*** *— denominado AVER's —, portanto, descreve um modelo formal que combina as duas formas de base nessa perspectiva combinada*" [1].

Aproveitamos o título para inserir, no mesmo movimento, a discussão de como as máquinas podem auxiliar-nos no controle, auditabilidade e verificação da cadeia de custódia (CPP, artigo 158-A), já que, por exemplo, *"a apreensão de computadores por si só não garante integridade da informação e autenticidade da fonte de prova, estas sujeitas a adoção de métodos que consideram algoritmos criptografados destinados a reter e preservar os dados (cópias espelho e lógica e cálculo da função* ***HASH****)"*. É nesse sentido que *"a preservação da cadeia de custódia da prova é uma entre as diversas técnicas de certificação dos elementos apresentados, de modo que deverá responder aos questionamentos sobre a* ***integralidade*** *(o documento/objeto apresentado como prova se encontra da mesma forma em que foi originalmente adquirido?), a* ***espoliação*** *(houve alterações intencionais no documento/objeto durante o manuseio ou análise, ou a evidência em potencial foi destruída em antecipação a uma investigação?) e a* ***volatilidade*** *(o documento/objeto é suscetível de mudança devido a fatores mecânicos, ambientais ou de passagem de tempo?)"*[2].

2023 - www.conjur.com.br - Todos os direitos reservados.

A invasão da tecnologia no ambiente probatório é realidade constante, com a tendência cada vez mais presente de que os profissionais alheios às oportunidades disponíveis sejam ultrapassados por força da defasagem tecnológica. A nossa atividade jurídica está rodeada de dispositivos inteligentes e meios de "checagem" dos requisitos de validade e de eficácia das evidências já produzidas e das possíveis de se realizar. O desconhecimento ou o negacionismo se constituem como comportamentos dominados. O choque tecnológico precisa ser assumido por quem deseja manter ou ampliar a performance. O modelo analógico de investigação, acusação e defesa ainda opera nos casos de complexidade baixa ou média, enquanto nos de alta e maxi, a debilidade tecnológica passou a compor o contexto mínimo de atuação. Em qualquer das complexidades, associar meios digitais é fator de vantagem competitiva. O desconhecimento dos instrumentos disponíveis e o "medo" do desconhecido e sobre os "custos" precisa ser enfrentado de modo direto pelos que desejam manter condições de "jogabilidade" no processo penal 4.0.

A "jogabilidade" pressupõe paridade de armas entre as partes e julgador atento às trapaças. No campo da disparidade, já não se trata apenas da largada desvantajosa da defesa em relação à acusação, condição quase imanente que decorre da vantagem cognitiva para o acusador durante a investigação (os elementos de investigação já produzidos são conhecidos pelo acusador, mas não necessariamente pela defesa, sobretudo aqueles relacionados às diligências em execução). Trata-se agora, também, da disparidade tecnológica, que opera em *dois campos distintos: a)* obtenção e produção de provas; e, *b)* controle e checagem das provas apresentadas pelo oponente. O *primeiro* consiste na disponibilidade de acesso aos meios de obtenção e/ou produção de evidências por parte dos agentes estatais e também dos defensores providos de meios tecnológico e recursos em relação aos demais imputados e defensores carentes de meios, por ausência de orçamento e/ou desconhecimento sequer da existência. O resultado é o de que a apuração dos indicadores fáticos para atribuição de culpa se mostra desequilibrada, isto é, a ineficiência probatória pode gerar erros (falsos positivos ou negativos) por não terem sido empregas as melhores armas tecnológicas disponíveis. O *segundo* opera na lógica de que se a acusação realiza investigação valendo-se de sofisticados recursos tecnológicos, a defesa precisa dispor de *softwares* capazes de conferir acesso ao formato dos arquivos (mídias digitais), nem sempre de fácil obtenção, além de dispor, em regra, de pouco tempo disponível para auditabilidade e efetiva confrontação. O fator tempo favorece à acusação que controla a investigação, reúne os elementos e apresenta a acusação estruturada, enquanto a defesa deve responder, o prazo da resposta à acusação, indicando as provas que deseja produzir. Se o imputado não realizou trabalho anterior de *compliance*, o acesso ao material defensivo resta prejudicado, ainda mais quando o agente está preso, houve apreensão de computadores e bloqueio de patrimônio (restrição de meios financeiros ao exercício da defesa). Ademais, quando a acusação deliberadamente vale-se da tática de juntar volumes e mais volumes de dados e documentos, de forma desorganizada, com senhas não fornecidas, referências a outros processos e/ou investigações autônomas, a leitura do contexto real do caso penal resta prejudicada. A tática de dissimulação e de vantagem decorrente da *assimetria de informação* (não apresentar tudo, aguardando o movimento defensivo), por mais que viole a *Boa-fé Objetiva* e a *"Regra de Brady"*, prejudica a determinação da *Teoria do Caso* pela defesa, além de impedir a "checagem" e a "auditabilidade" de todo o material suporte da acusação.

2023 - www.conjur.com.br - Todos os direitos reservados.

É nesse contexto que se inserem as discussões acerca da cadeia de custódia da prova. Mormente em relação às provas digitais, por conta da facilidade de manipulação (fake news, *deep fake* etc.), a cadeia de custódia é indispensável. Como advertido por Janaina Matida: *"é preciso que a cadeia de custódia das provas não se reduza à cadeia de aproveitamento de irregularidades. A promessa de um processo penal acusatório seriamente comprometido com a presunção de inocência só pode ser satisfeita quando o que acontece em investigação preliminar também seja objeto de nossas reflexões. A determinação adequadamente fatos, considerando o compromisso com a redução dos riscos de se condenar inocentes próprio do processo penal, não pode ser atingida enquanto a investigação preliminar seja conservada como um reino de arbitrariedades e surpresas contra a defesa, favores e condescendências para a acusação"* [3].

Se a acusação obtém ou produz evidências por meio de tecnologia não disponível no mercado ou ainda com custos relevantes, a negativa de acesso e disponibilidade dos *softwares* à defesa, impede a verificação da observância da *cadeia de custódia digital* (por ausência a de meios tecnológicos). A oferta, sem custos, à defesa, dos mecanismos utilizados para fins de *acesso* ao conteúdo, *auditabilidade* e *verificação* do material é condição de validade e de eficácia da prova. Deve-se conceder acesso e/ou licença de uso do programa ou *software*, durante todo o processo, para defensores públicos e privados, sem qualquer custo.

A paridade de armas tecnológicas pressupõe a possibilidade efetiva (e não potencial, a depender de recursos privados) de *contraditório significativo* sobre a qualidade, credibilidade e confiabilidade dos meios e dos trajetos empregados. Do contrário, não se trata de vantagem tecnológica, mas de subtração das condições mínimas do dever de "informação" sobre o conteúdo da prova produzida, violadora do *devido processo legal e da presunção de inocência*. Não se pode ignorar que o ônus da prova pertence exclusivamente ao acusador, o qual abrange também o ônus de provar que é lícita a prova produzida.

Ao mesmo tempo em que não se pode proibir o uso da tecnologia no ambiente processual, é vedado que a vantagem tecnológica circunstancial impeça o exercício da ampla defesa. A postura de exigir acesso, apontar a impossibilidade do exercício da defesa, deve ser demonstrada ao julgador, porque no ambiente 4.0, as coordenadas pressupõem adequação de meios, sob pena de não se instaurar o contraditório significativo, obstando a participação da defesa na construção do provimento jurisdicional. A indicação expressa e circunstanciada dos *softwares* e bancos de dados utilizados na investigação estão contidos no conceito de *cadeia de custódia digital*, já que surgiram do esforço investigativo (em fontes fechadas e abertas) realizado pelos agentes da investigação. Por isso, o cumprimento do ônus acusatório da *cadeia de custódia digital* engloba o trajeto investigativo, não se confundido com o resultado apresentado no "Relatório da Investigação". Será preciso demonstrar: a) quem; b) quando; c) como; d) onde; e) por que; f) para que; g) o que; e, h) com que motivação. A responsabilidade pelos métodos utilizados, o controle da "pescaria probatória", do "compartilhamento espúrio" de dados e informações agregados de investigações autônomas, por exemplo, precisa estar documentada de modo a autorizar a identificação dos indicadores democráticos da epistemologia da prova. A inobservância abre espaço para discussão sobre a "quebra" da cadeia de custódia digital, o reconhecimento da ilicitude e/ou invalidade do material apresentado[4].

2023 - www.conjur.com.br - Todos os direitos reservados.

É nesse sentido que o ponto de partida de Marcella Mascarenhas e Fabiana Mascarenhas serve-nos de ponto de chegada [5]. Algoritmos, por operarem comparando e compondo dados, podem, sem dúvida, racionalizar a cadeia de custódia. Obviamente, alguns ajustes são necessários: a) é preciso criar um *checklist* oficial da cadeia de custódia digital (o qual deve ser incluído no CPP, pois o atual regramento dos artigos 158-A a 158-F parece-nos insuficiente para tratar da prova digital), em conformidade com manuais já desenvolvidos, mas que precisam ser amplamente discutidos na comunidade jurídica, técnico-especializada (peritos nas respectivas áreas de formação) e sociedade civil; b) é preciso que esses critérios sejam convertidos em dados analisáveis (texto, imagem ou som de qualidade) pelos algoritmos; c) esses dados devem ser os mais completos, claros e nítidos (qualidade do dado) possíveis; d) a verificação da cadeia de custódia é reserva jurisdicional, de modo que o trabalho realizado por algoritmos policiais e ministeriais usurparia indevidamente a jurisdição, logo só pode pertencer ao Judiciário; e) toda a atividade precisa ser supervisionada pelo juiz natural; f) eventuais resultados negativos (insuficiência, violação, ausência ou incompletude) servem para inadmitir a prova, ao mesmo tempo que os positivos ainda se submetem ao contraditório (não implicam na admissão automática da prova); g) toda decisão sobre cadeia de custódia deve ser fundamentada (artigo 93, IX, CRFB; artigo 315, §2º, CPP) e, no caso de avaliação por algoritmo, tal circunstância deve constar expressamente na decisão para que as partes possam controlar; e g) eventual inconsistência entre a avaliação pelo algoritmo e o controle das partes (verificação do trabalho, com conferência entre informações da cadeia de custódia e o *checklist* oficial) deve implicar na inadmissão da prova. É o que estamos fazendo na Plataforma **RoadMapCrime** (em breve).

[1] NARDELLI, Marcella Mascarenhas; MASCARENHAS, Fabiana Alves. Podem os algoritmos racionalizar a investigação criminal. **Consultor Jurídico**, São Paulo, 19 mar. 2021. Disponível em: https://www.conjur.com.br/2021-mar-19/limite-penal-podem-algoritmos-racionalizar-investigacao-criminal.

[2] PRADO, Geraldo. Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital. **Consultor Jurídico**, São Paulo, 21 jan. 2021. Disponível em: https://www.conjur.com.brhttps://www.conjur.com.br/wp-content/uploads/2023/09/artigo-geraldo-prado.pdf.

[3] MATIDA, Janaina. A cadeia de custódia é condição necessária para a redução dos riscos de condenações de inocentes. **Boletim IBCCRIM**, n. 331, jun. 2020, p. 8.

[4] PRADO, Geraldo. Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital. **Consultor Jurídico**, São Paulo, 21 jan. 2021. Disponível em: https://www.conjur.com.brhttps://www.conjur.com.br/wp-content/uploads/2023/09/artigo-geraldo-prado.pdf

2023 - www.conjur.com.br - Todos os direitos reservados.

: "violada a cadeia de custódia da prova digital incide imperiosa proibição de valoração da prova assim obtida. É o corpo de delito que se converte em algo juridicamente imprestável à luz do direito fundamental à integridade dos sistemas informáticos e o igualmente fundamental direito à confidencialidade, princípios constitucionais implícitos assim como o é o direito fundamental à autodeterminação informativa."

[5] NARDELLI, Marcella Mascarenhas; MASCARENHAS, Fabiana Alves. Podem os algoritmos racionalizar a investigação criminal. **Consultor Jurídico**, São Paulo, 19 mar. 2021. Disponível em: https://www.conjur.com.br/2021-mar-19/limite-penal-podem-algoritmos-racionalizar-investigacao-criminal: "Tanto a adequada definição da hipótese fática a ser sustentada pela acusação em juízo — a qual indicará todas as questões de fato subjacentes à pretensão acusatória —, quanto a confiabilidade do conjunto probatório que servirá de base para a decisão judicial dependem, em grande medida, que a investigação criminal se desenvolva de forma racional e a partir de parâmetros acertados. Os rumos da atividade de busca e coleta de elementos informativos na fase preliminar condicionarão, por certo, a confiabilidade do juízo de fato que terá lugar na etapa processual."

Date Created
02/04/2021

2023 - www.conjur.com.br - Todos os direitos reservados.