

ARTIGO: PROVAS DIGITAIS, REALIDADE SIMULADA E OS DESAFIOS DO PROCESSO PENAL

AUTOR: GEOVANE MORAES

INTRODUÇÃO

Imagine a seguinte cena.

Você está em casa, à noite, mexendo no celular, quando chega uma mensagem de WhatsApp. A foto é do seu advogado, o nome confere, o número da OAB existe, o processo é mesmo o seu. Do outro lado da tela, a mensagem é cordial e objetiva: saiu o alvará, falta apenas uma taxa para liberação, se você fizer o PIX agora o valor entra hoje. Você olha a foto de perfil, vê o brasão da República na capa, recebe um PDF com o timbre do tribunal e até um print da movimentação processual. Tudo parece absolutamente verossímil.

Você faz a transferência.

Dias depois, descobre que o advogado nunca mandou aquela mensagem. A identidade que falou com você era inteiramente digital, montada a partir de fragmentos reais que estão espalhados pela internet. O número era falso. O rosto era verdadeiro, mas a pessoa por trás da tela não tinha qualquer vínculo com a advocacia.

Agora mude de cena.

Um motorista por aplicativo dirige à noite em uma rodovia federal. Ele exibe no painel o crachá do aplicativo, dirige um carro supostamente regular, com documentos em dia e cadastro aprovado na plataforma. Tudo em volta sugere normalidade. Em poucos minutos, uma abordagem da Polícia Rodoviária Federal desmonta essa aparência. O veículo tem registro de roubo, chassi adulterado e placas clonadas. O motorista afirma que apenas alugou o carro, apresenta contrato eletrônico, prints de

cadastro, histórico de corridas. A documentação digital, mais uma vez, conta uma história de licitude que não corresponde à realidade material.

Em outro ponto do país, uma organização criminosa simula corridas que nunca existiram. Motoristas fantasmas, passageiros que não são pessoas reais, rotas que apenas aparecem no mapa da plataforma. As corridas são registradas, os pagamentos são lançados, o prejuízo é concreto, mas o deslocamento físico nunca ocorreu. A geolocalização, base central dessa história, é montada com combinação de contas falsas e manipulação técnica.

Por fim, em um parque de exposições lotado no período junino, um vigilante negro é abordado com a família porque uma câmera de reconhecimento facial indicou que ele seria um criminoso procurado por um roubo ocorrido dez anos antes. A prisão é efetuada. As matérias de jornal falam em sucesso da tecnologia. Apenas semanas depois vem a constatação: o verdadeiro ladrão havia utilizado, no passado, os dados do vigilante quando foi detido. O sistema não errou só o rosto. Errou a vida inteira de uma pessoa.

Essas histórias não são ficção científica. São recortes de uma realidade recente, ocorrida no Brasil, em que identidades são clonadas, documentos são fabricados em ambientes digitais, rotas são manipuladas e rostos são comparados por algoritmos que erram, muitas vezes contra os mesmos corpos de sempre.

Diante desse cenário, o processo penal brasileiro precisa responder a perguntas incômodas. O que é prova em um mundo em que vozes, rostos, trajetos e documentos podem ser simulados com poucos cliques? É possível confiar em prints, relatórios de sistemas e arquivos extraídos de celulares sem qualquer controle técnico? Como agir quando a realidade digital, tão convincente na tela, não corresponde ao que de fato aconteceu?

A tese defendida neste artigo é direta. O processo penal brasileiro, assim como a maior parte dos seus operadores, ainda não possui ferramentas técnicas, base

normativa estruturada nem formação adequada para enfrentar a era das provas digitais e das realidades simuladas.

A distância entre a complexidade do mundo digital e a prática forense cotidiana se tornou um terreno perigoso, em que a aparência de verdade pode condenar inocentes ou inviabilizar investigações sérias.

Este texto desenvolve esse argumento em quatro etapas.

Primeiro, apresenta premissas teóricas mínimas sobre prova digital e cadeia de custódia. Em seguida, narra e analisa casos concretos que revelam a construção de realidades simuladas no contexto de golpes com falsos advogados, veículos roubados e clonados, fraudes em aplicativos de transporte e erros em reconhecimento facial. Depois, discute o fetichismo tecnológico e as lacunas técnicas, normativas e formativas do processo penal. Por fim, conclui mostrando por que, se nada mudar, o sistema de justiça criminal continuará julgando mundos que nunca existiram, punindo pessoas verdadeiras com base em ficções digitais.

1 PROVAS DIGITAIS E PROCESSO PENAL EM TEMPO DE REALIDADE SIMULADA

1.1 O QUE É, AFINAL, PROVA DIGITAL

Durante muito tempo, quando se falava em prova no processo penal, a imagem mais comum era a de testemunhas sentadas diante do juiz, documentos em papel, laudo pericial em poucas páginas ou um objeto apreendido exposto em audiência. Hoje, o cenário é outro. Quase toda conduta humana deixa um rastro digital. Aplicativos registram conversas, plataformas guardam históricos, sistemas armazenam acessos, câmeras produzem vídeos continuamente, bancos de dados públicos e privados acumulam informações que podem ser usadas como evidência.

Prova digital, em termos simples, é qualquer elemento probatório que existe em formato eletrônico e depende de sistemas tecnológicos para ser produzido,

armazenado, transmitido ou acessado. Isso inclui mensagens de aplicativos, e-mails, registros de acesso, arquivos de áudio e vídeo, fotos e seus metadados, dados de geolocalização, históricos de navegação, relatórios de sistemas e uma série de outros vestígios informacionais que não se encaixam exatamente nas provas clássicas.

Essa prova tem características que mudam completamente o jogo. A primeira delas é a intangibilidade. Na maior parte das vezes, ela não é palpável. Está em servidores distantes, na nuvem, em bancos de dados de empresas, em chips de celulares. A segunda é a facilidade de replicação e de alteração. Um arquivo pode ser copiado infinitas vezes, enviado a qualquer lugar do mundo em segundos, modificado de forma praticamente imperceptível. A terceira é a dependência estrutural em relação a atores privados. Boa parte do que poderia esclarecer um crime está nas mãos de plataformas que não são órgãos públicos e que respondem a legislações, políticas internas e interesses próprios.

No modelo tradicional de processo penal, muitas vezes basta olhar um documento para perceber uma rasura, observar uma arma para notar um detalhe, ouvir uma testemunha para avaliar sua segurança. Com a prova digital, esse tipo de intuição inicial é insuficiente. Um print de tela pode ter sido editado em poucos segundos. Um áudio pode ter sido montado ou otimizado artificialmente. Um relatório de sistema pode refletir uma base inteira que já foi contaminada por fraude.

A pergunta central deixa de ser apenas o que está escrito ou exibido. Passa a ser, também, como esse dado foi coletado, qual foi a metodologia de extração, quem teve acesso ao original, se houve geração de código de integridade, se o arquivo permaneceu inalterado. Sem esse olhar, o risco é tratar qualquer captura de tela ou arquivo exportado como se fosse uma fotografia neutra da realidade, quando muitas vezes é apenas uma narrativa construída.

1.2 CADEIA DE CUSTÓDIA DIGITAL: MUITO ALÉM DO ENVELOPE LACRADO

A legislação brasileira tentou reagir a esses desafios ao conferir status legal ao instituto da cadeia de custódia, especialmente a partir da Lei 13.964 de 2019, que inseriu os artigos 158 - A e seguintes no Código de Processo Penal. O conceito, de forma resumida, descreve o conjunto de procedimentos que garantem e documentam a trajetória do vestígio, do momento da coleta até sua apresentação em juízo.

Essa lógica sempre foi relativamente conhecida no campo da prova material, como drogas apreendidas, armas, manchas de sangue. O que muda, quando se fala em evidência digital, é a sensibilidade extrema do objeto. Um celular ligado e manuseado sem cuidado já pode alterar registros de forma irreversível. Um arquivo copiado sem método pode perder seu vínculo probatório com o original. E, diferentemente de um envelope lacrado, a mera impressão em papel de uma conversa de WhatsApp não preserva o conteúdo real dos dados, apenas sua aparência naquele momento.

Por isso, a cadeia de custódia digital passa por etapas que envolvem muito mais técnica do que hábito. Aprender corretamente o dispositivo, registrar as condições em que foi encontrado, realizar extração por ferramentas forenses que criam uma imagem fiel do conteúdo, gerar códigos de integridade que permitam conferir se algo foi alterado, documentar quem acessou o material, em que momento e para qual finalidade.

Não se trata de capricho. É justamente esse cuidado que permite, mais tarde, dizer com segurança ao juiz e às partes que o arquivo que está sendo analisado é o mesmo que foi encontrado, sem edições ocultas. Quando essa cadeia é quebrada, o valor probatório cai de forma drástica.

O Superior Tribunal de Justiça, em decisões recentes, reconheceu a inadmissibilidade de provas digitais produzidas sem atenção adequada à cadeia de custódia, especialmente em relação a dados de celulares. Em alguns casos, a própria condenação foi anulada porque não havia como afirmar que os arquivos apresentados correspondiam, de forma íntegra, ao conteúdo original do aparelho apreendido. No plano teórico, o recado é claro. Sem método, não há confiabilidade.

Na prática, porém, ainda é comum ver investigações lastreadas em capturas de tela realizadas de forma improvisada, acesso a aplicativos diretamente por agentes públicos, extração manual de conversas sem qualquer registro técnico. O discurso da cadeia de custódia já chegou aos livros. Ainda falta chegar às delegacias, aos laudos periciais do dia a dia e aos critérios efetivamente adotados por juízes ao valorar a prova digital.

2 HISTÓRIAS REAIS EM UM PAÍS DE REALIDADES FABRICADAS

Para além das definições abstratas, é olhando para casos concretos que a fragilidade do processo penal em relação à prova digital se torna quase palpável. Os exemplos a seguir ocorreram no Brasil e ajudam a ilustrar como se constrói, com tecnologia e informação, uma narrativa a respeito de alguém, seja para enganar, seja para acusar.

2.1 O FALSO ADVOGADO QUE SABE TUDO SOBRE O SEU PROCESSO

Um dos golpes que mais cresceram nos últimos anos envolve criminosos que se fazem passar por advogados. A mecânica é sofisticada e, ao mesmo tempo, assustadoramente simples. Os golpistas pesquisam processos em andamento nos sites de tribunais, consultam nome de partes, números de autos, órgãos julgadores, datas de audiências, valores em discussão. Em seguida, vasculham redes sociais e cadastros públicos em busca de informações sobre advogados reais: fotos, número de OAB, endereço de escritório, logotipos.

Com esse material em mãos, criam perfis em aplicativos de mensagem usando a foto do profissional, inserem o nome correto, replicam o brasão da República como imagem de capa e iniciam contato com clientes. A conversa costuma mencionar detalhes muito específicos do caso, o que dispara a sensação de autenticidade na vítima. Em alguns episódios, foram enviados PDFs imitando ofícios e decisões judiciais, com selos e carimbos aparentemente oficiais.

A Ordem dos Advogados do Brasil em São Paulo identificou milhares de relatos desse tipo. A seccional paulista ajuizou ação civil pública, apontando que, em sete meses, quase quatro mil denúncias de uso indevido de credenciais de advogados foram registradas, com mais de três quartos dos casos resultando em prejuízos financeiros. O padrão é sempre semelhante. Um cliente confia em uma identidade digital que parece sólida. A transferência é realizada. O dinheiro desaparece.

No plano do processo penal, esse cenário representa um desafio delicado. Quando a vítima procura uma delegacia, quase sempre o que leva são prints. Capturas de tela das conversas, cópia do comprovante de PIX, eventualmente o PDF recebido. Se não houver cuidado, esses prints se transformam, rapidamente, na narrativa oficial. O inquérito passa a contar a história do golpe como se fosse uma sequência de quadros estáticos, sem que se questione se houve adulteração de trechos, se o número exibido é mesmo aquele que era utilizado na época, se o PDF foi inspecionado quanto à origem.

Há outro risco ainda mais sutil. As mesmas ferramentas usadas pelos golpistas para simular uma identidade profissional podem, em tese, ser usadas para tentar incriminar um advogado verdadeiro. Uma montagem de diálogo pode sugerir que ele exigiu valores ilícitos, que orientou condutas impróprias, que se associou a práticas criminosas. Sem perícia adequada, a linha que separa a realidade da falsificação é muito mais tênue do que se imagina.

2.2 O CARRO ROUBADO QUE RODA NO APLICATIVO COM DOCUMENTAÇÃO PERFEITA

Em outro conjunto de casos, a realidade fabricada aparece sob a forma de aparente regularidade. Um exemplo emblemático se repete em diferentes estados. Motoristas abordados em rodovias, conduzindo veículos que constam como roubados ou clonados, alegam ter alugado ou comprado o carro de maneira legítima. Quando mostram o celular, exibem contratos eletrônicos, conversas em aplicativos, prints de

cadastros aprovados em plataformas de transporte, histórico de corridas com passageiros.

No papel, ou melhor, na tela, tudo parece coerente. O veículo está registrado como ativo em um aplicativo conhecido. A foto corresponde ao modelo. O CRLV aparece no formato digital. As conversas com o suposto locador indicam um negócio aparentemente comum. Em alguns episódios tornados públicos, no entanto, as investigações revelaram esquemas em que organizações criminosas utilizavam contas no sistema gov.br para efetuar transferências fraudulentas de veículos, emitindo documentos em nome de laranjas ou mesmo em nome de vítimas que desconheciam completamente a operação.

O resultado é um cenário em que o automóvel, embora fisicamente roubado, circula sob um manto digital de aparente licitude. Em um eventual processo por receptação ou associação criminosa, tanto a acusação quanto a defesa podem tentar se apoiar nessas provas digitais. De um lado, o Ministério Público pode argumentar que o preço muito abaixo da tabela e as circunstâncias do negócio indicam dolo ou, ao menos, indiferença quanto à origem ilícita. De outro, o motorista pode sustentar que confiou justamente na regularidade documental e na aprovação do cadastro do aplicativo como sinais de boa fé.

Se o júízo se contentar em olhar apenas a superfície desses dados, corre o risco de dar à narrativa digital um peso probatório que ela não merece. Será que os cadastros foram feitos com documentos legítimos? Será que a aprovação no aplicativo foi precedida de uma verificação minimamente séria ou se tratou de um mero envio de fotos facilmente manipuláveis? Houve, por parte da plataforma, qualquer checagem junto a bancos públicos sobre restrição do veículo? Sem resposta técnica para essas perguntas, a prova digital permanece mais próxima de uma cenografia sofisticada do que de um reflexo confiável dos fatos.

2.3 CORRIDAS QUE NUNCA EXISTIRAM E ROTAS QUE SÓ ACONTECEM NO MAPA

A Operação Rota Falsa, deflagrada pela Polícia Civil do Rio de Janeiro em 2025, é talvez o exemplo mais claro de como uma realidade digital completa pode ser fabricada sem que nada corresponda, de verdade, ao mundo físico. O grupo investigado criou centenas de contas falsas de motoristas e passageiros em uma grande plataforma de transporte. Em muitas dessas contas, imagens geradas ou manipuladas com auxílio de inteligência artificial eram usadas para enganar o sistema de verificação de identidade.

As corridas registradas no aplicativo não passavam de simulações. Passageiros fictícios solicitavam viagens que eram aceitas por motoristas igualmente inexistentes. A rota era traçada, o aplicativo registrava deslocamentos, o sistema calculava o valor devido. A empresa arcava com pagamentos, acreditando remunerar profissionais por trajetos efetivamente realizados. No mapa, a cidade era percorrida em múltiplos itinerários. Nas ruas, nenhum desses deslocamentos ocorria.

Esse tipo de fraude mostra como a geolocalização, tão frequentemente tratada como prova quase absoluta em processos penais, pode ser manipulada. Somando contas falsas, uso de ferramentas de simulação de GPS e manipulação de rotas, é possível construir uma linha do tempo digital para qualquer pessoa. Em um contexto de investigação criminal, isso abre portas tanto para álibis fabricados quanto para imputações forjadas.

Se um investigado apresenta extratos de corridas para demonstrar que estava dirigindo em determinada região, e não no local do crime, a análise não pode se limitar à leitura acrítica do relatório da plataforma. É preciso examinar a origem dessas contas, cruzar dados com antenas de telefonia, verificar se houve conexão do aparelho em redes compatíveis com aquele trajeto, identificar pontos de contradição. A prova digital só ganha densidade quando se confronta com outros vestígios. Isolada, pode ser apenas parte do enredo criado por quem quer enganar o sistema.

2.4 O ROSTO QUE O ALGORITMO CONFUNDE E O CORPO QUE VAI PARA A PRISÃO

Os casos brasileiros de reconhecimento facial que resultaram em prisão de pessoas inocentes revelam um aspecto ainda mais perturbador da realidade simulada.

Em Salvador, por exemplo, o episódio do vigilante negro preso durante as festas juninas de 2022 ganhou repercussão nacional. Ele foi abordado ao entrar no Parque de Exposições com a família porque o sistema de câmeras inteligentes indicou que seu rosto correspondia ao de um criminoso procurado.

A narrativa inicial seguiu o padrão das notícias oficiais: mais um foragido capturado graças à tecnologia. O que não foi dito com a mesma ênfase é que, anos antes, o verdadeiro autor do crime havia fornecido os dados do vigilante quando foi preso, criando um vínculo indevido entre o rosto de um e a ficha de outro. O algoritmo, alimentado com uma base já contaminada por essa confusão, apenas reproduziu e amplificou o erro. O resultado concreto foram vinte e seis dias de prisão injusta, com dano à honra, à vida familiar e ao trabalho daquela pessoa.

No Rio de Janeiro, a história do educador Danillo Félix Vicente de Oliveira ilustra outro aspecto grave. Ele foi reconhecido por fotografia em um inquérito, chegou a ficar preso por quase dois meses, e depois foi absolvido quando a vítima admitiu o engano. Mesmo assim, a mesma imagem voltou a ser utilizada em outro procedimento, levando o mesmo cidadão a ter de provar sua inocência mais de uma vez. A fotografia passou a funcionar quase como um personagem recorrente, reaparecendo em diferentes processos sob a roupagem de prova.

Em ambos os casos, a realidade digital que se formou sobre aqueles corpos não corresponde à verdade. A foto no sistema, o índice gerado pelo algoritmo, o relatório exibindo um suposto acerto, tudo isso produz a sensação de certeza. Para o operador do direito que não domina minimamente o funcionamento das ferramentas, a tentação é grande. O sistema acusou, logo deve ser verdadeiro.

Essa confiança deslocada tem consequências diretas sobre o princípio da presunção de inocência. Quando se parte da premissa de que o laudo tecnológico é

neutro e confiável, o ônus de demonstrar o erro acaba recaindo sobre a pessoa acusada. Em vez de o Estado provar, de forma robusta, a autoria, é o indivíduo que se vê na posição de desconstruir um relatório técnico que poucos entendem.

Nesse movimento, o processo penal deixa de ser um instrumento de contenção do poder punitivo para se tornar, muitas vezes, mera chancela de decisões algorítmicas opacas.

3 PROVA DIGITAL, NARRATIVA E FETICHISMO TECNOLÓGICO

Os quatro blocos de casos analisados têm algo em comum. Em todos eles, existe uma história sendo contada em linguagem digital. O perfil do falso advogado, o contrato eletrônico do veículo, o histórico de corridas inexistentes, o relatório de reconhecimento facial. Em cada situação, um conjunto de elementos técnicos compõe uma narrativa que parece coerente.

O problema é que o processo penal, se não tomar cuidado, passa a julgar a narrativa e não o fato. Em vez de perguntar o que de fato aconteceu, quem fez o quê, em que circunstâncias, com quais consequências, o sistema de justiça corre o risco de perguntar apenas se aquilo que se apresenta como dado digital é internamente consistente. Se o perfil tem foto, nome e número, se o contrato está bem escrito, se a rota parece verossímil no mapa, se o relatório exhibe percentual de acerto elevado.

Esse deslocamento é alimentado por um fetichismo tecnológico. No imaginário contemporâneo, a tela tem aura de evidência. O print do celular, o e-mail impresso, a página do sistema representam, para muitos, algo mais confiável do que a memória humana. Quando se soma a isso a presença de termos técnicos, como log, hash, geolocalização, reconhecimento facial, cria-se um ambiente em que a aparência de sofisticação substitui a discussão sobre método.

Sem perceber, juízes, promotores, delegados e advogados podem tratar um print de WhatsApp como se fosse documento público dotado de fé, um arquivo

extraído manualmente de um celular como se fosse resultado de procedimento pericial rigoroso, um relatório de sistema emitido por empresa privada como se tivesse passado por validação independente.

Em alguns momentos, as cortes superiores reagem, exigindo respeito à cadeia de custódia, afastando provas colhidas sem método, alertando para o perigo de condenações lastreadas exclusivamente em reconhecimento fotográfico ou facial. Esses movimentos, contudo, ainda convivem com uma prática diária em que o imprevisto é regra.

A prova digital não é, por natureza, melhor ou pior do que as provas tradicionais. Ela é diferente. Exige perguntas específicas. Quando não se sabe quais perguntas fazer, o operador do direito tende a se refugiar em dois extremos igualmente perigosos. Ou rejeita tudo de forma genérica, sob o argumento de que tudo pode ser manipulado, ou aceita quase tudo, por acreditar que a tecnologia, por ser complexa, deve ser confiável. Nem uma coisa, nem outra, atende ao ideal de um processo penal orientado pela busca honesta da verdade possível.

4 UM PROCESSO PENAL ANALÓGICO DIANTE DE CRIMES DIGITAIS

Se o problema fosse apenas teórico, bastaria reescrever alguns capítulos manuais. O desafio é mais profundo. Ele é normativo, técnico e, sobretudo, formativo.

Do ponto de vista da legislação, há ilhas de avanço. O Marco Civil da Internet e a Lei Geral de Proteção de Dados estabeleceram diretrizes importantes sobre obtenção e uso de informações na rede. A positivação da cadeia de custódia no Código de Processo Penal é um passo significativo. Ainda assim, falta uma disciplina mais específica e detalhada sobre a prova digital, que estabeleça parâmetros mínimos para admissibilidade, produção e valoração em matéria penal.

Enquanto isso não ocorre, o resultado é um mosaico fragmentado. Em uma comarca, prints de conversas são tratados como prova plena. Em outra, são vistos com

desconfiança e demandam confirmação por outros meios. Em alguns casos, dados extraídos de celulares sem qualquer documentação técnica são aceitos. Em outros, são declarados nulos. O mesmo vale para registros de geolocalização e relatórios emitidos por plataformas. A jurisprudência oscila, não apenas entre tribunais, mas às vezes dentro do mesmo colegiado.

No plano técnico, a distância entre o ideal e a realidade de muitas instituições é evidente. A extração correta de dados de um smartphone exige softwares específicos, treinamento, laboratório, tempo. A análise cruzada de geolocalização pede conhecimento de redes, antenas, protocolos. A avaliação crítica de um algoritmo de reconhecimento facial pressupõe compreensão básica de como são formados os bancos de dados, de qual é a taxa de falsos positivos, de como o viés aparece nas estatísticas.

Grande parte das delegacias, entretanto, ainda opera com estrutura limitada, sem laboratório forense digital adequado, sem equipe especializada em número suficiente, sem acesso contínuo a ferramentas atualizadas. Em muitos estados, há concentração de peritos em capitais, o que dificulta a análise de casos em regiões mais afastadas. Verifica-se um hiato entre a sofisticação das práticas criminosas e os meios concretos disponíveis para enfrentá-las dentro da legalidade.

No centro de tudo isso está o fator humano. O currículo tradicional dos cursos de Direito raramente contempla disciplinas de segurança cibernética, ciência de dados, inteligência artificial ou mesmo fundamentos de tecnologia da informação. A grande maioria dos operadores do processo penal formou-se em um ambiente acadêmico em que prova era sinônimo de depoimento, documento físico e laudo pericial clássico. Muitos sequer tiveram contato, na graduação, com debates mais recentes sobre algoritmos, plataformas, vigilância em massa.

Não se trata de exigir que juízes se tornem engenheiros de software, nem que promotores ou defensores se metamorfoseiem em peritos de informática. O que se exige é que tenham formação mínima que lhes permita formular as perguntas certas,

identificar inconsistências básicas, desconfiar de laudos tecnicamente fracos, valorizar adequadamente o trabalho pericial sério, saber quando é necessário um exame mais aprofundado e quando a prova apresentada não atende a um padrão minimamente aceitável.

Sem essa base, a tendência é que o processo penal se torne excessivamente dependente de relatórios produzidos por terceiros, muitas vezes sem possibilidade real de escrutínio. Essa dependência é perigosa, porque desloca o poder de decisão para fora do espaço jurídico, entregando a atores privados ou algoritmos proprietários uma parcela significativa da reconstrução dos fatos.

CONCLUSÃO

Ao longo deste texto, foram apresentados casos concretos que poderiam, sem qualquer exagero, compor o roteiro de uma série de ficção jurídica. Um advogado que não é advogado, mas convence clientes de que representa seus interesses. Carros roubados que circulam com documentação digital aparentemente impecável, inclusive em aplicativos de transporte. Corridas que nunca saíram do papel, mas aparecem em mapas, relatórios e extratos como se tivessem cruzado cidades inteiras. Rostos confundidos por sistemas de reconhecimento facial, que geram prisões e processos contra pessoas que nada têm a ver com os crimes imputados.

A diferença em relação à ficção está em um detalhe incômodo. Tudo isso aconteceu de verdade.

Essas histórias revelam um ponto de ruptura entre o nosso processo penal, ainda muito marcado por uma lógica analógica, e o mundo em que hoje os conflitos se desenrolam, povoado de identidades digitais, bases de dados dinâmicas e sistemas algorítmicos. A prova digital, em vez de ser um simples novo formato da velha prova, é um campo que exige linguagem própria, protocolos específicos, infraestrutura técnica, peritos especializados e operadores do direito com outra formação intelectual.

No Brasil, alguns sinais de mudança aparecem na legislação e na jurisprudência. A previsão legal da cadeia de custódia, as decisões que anulam provas digitais colhidas sem método, as críticas crescentes ao reconhecimento fotográfico e facial mal conduzidos, tudo isso indica que há consciência, em níveis distintos, do tamanho do desafio. Ainda assim, é impossível afirmar, com honestidade, que o sistema esteja preparado.

Normas gerais, por si só, não bastam. Sem investimento real em laboratórios, em equipamentos, em pessoal qualificado, a prova digital continuará a ser produzida e analisada de forma improvisada. Sem uma reforma profunda na formação de delegados, promotores, magistrados, defensores e advogados, a tecnologia seguirá envolta em uma aura de neutralidade que ela não possui. Sem protocolos claros para uso de ferramentas como reconhecimento facial, o risco de reproduzir e ampliar injustiças, especialmente contra grupos vulneráveis, permanecerá alto.

A conclusão é dura, mas necessária. O processo penal brasileiro, em sua configuração atual, e a maioria dos que o operam ainda não dispõem de ferramentas técnicas, de arcabouço normativo específico e, principalmente, de conhecimento suficiente para enfrentar, com segurança, a era das provas digitais e das realidades simuladas.

Se nada for feito, a tendência é que se repitam, com frequência cada vez maior, as histórias aqui narradas. Pessoas reais continuarão sendo esmagadas por narrativas digitais falsas ou por sistemas que confundem seus rostos, seus dados, seus trajetos. Golpistas seguirão explorando a ingenuidade tecnológica de vítimas e instituições. Investigações sérias podem ser comprometidas por provas frágeis, fáceis de contestar, ou, pior, por provas manipuladas que ninguém sabe como desmontar.

Prevenir esse futuro exige reconhecer que o problema não é apenas técnico, mas também político e cultural. Exige abandonar a crença confortável de que a verdade está na tela apenas porque ali aparece com nitidez. Exige retomar o compromisso do processo penal com a busca responsável da verdade possível, desta

vez em um ambiente em que a verdade pode ser imitada com uma fidelidade assustadora.

Enquanto não houver esse esforço conjunto de atualização normativa, estrutura pericial e formação de operadores, continuaremos vivendo em um cenário em que o sistema de justiça criminal corre o risco diário de condenar pessoas de carne e osso com base em mundos que só existiram na memória de um servidor, em uma rota de GPS falsificada ou na superfície lisa de uma tela de celular.



Observação sobre

PLÁGIO

Autor: Geovane Moraes

Curso: Jus21

Coordenação Pedagógica: Rayanna Fernandes

Todo o conteúdo deste artigo e da produção científica, incluindo textos e imagens, está protegido por direitos autorais do autor. É estritamente proibida qualquer forma de plágio, reprodução, cópia ou utilização parcial ou integral do material sem autorização prévia e expressa do autor, independentemente de haver finalidade lucrativa. O descumprimento dessa norma poderá implicar em sanções civis e criminais, conforme previsto na legislação vigente. O presente trabalho foi desenvolvido com base em revisão bibliográfica, a fim de reunir, analisar e discutir contribuições teóricas relevantes sobre o tema abordado.