Perícia informática é nova 'prova-chave' do processo penal, diz professora espanhola

07/09/2025

Em meio à consolidação das vidas das pessoas no meio digital, a perícia informática torna-se a nova "prova-chave" do processo penal. A avaliação é da processualista espanhola **Lorena Bachmaier Winter**, professora catedrática da Universidade Complutense de Madrid e especialista em provas digitais.

Spacca

Winter também é professora do *campus* madrileno da Universidade Saint Louis (sediada nos EUA), perita do Conselho da Europa — organização que atua na defesa dos direitos humanos e da democracia naquele continente — e membro do grupo de experts em política criminal da Comissão Europeia, instituição que representa e defende os interesses da UE.

A professora esteve no Brasil no final de agosto para dar a palestra "A prova na era digital: um novo paradigma?", no 31º Seminário Internacional de Ciências Criminais do Instituto Brasileiro de Ciências Criminais (IBCCRIM), que acontece em São Paulo.

Em entrevista à revista eletrônica **Consultor Jurídico**, a professora traçou um panorama sobre as transformações do processo penal, que, segundo ela, sofrerá uma mudança de enfoque no mundo inteiro, à medida que enfrenta fenômenos relacionados à sociedade digital e à tecnologia.

Na visão de Winter, o Direito Penal é cada vez menos repressivo e mais preventivo, mas as medidas de prevenção, fomentadas por sistemas de vigilância em massa baseados em algoritmos, criam a categoria das "pessoas de interesse" — indivíduos identificados como "pré-suspeitos" devido ao risco de se associarem a atividades criminosas.

Além disso, segundo ela, as medidas de Direito Administrativo, que estão fora do escopo das garantias do processo penal, tendem a ser punitivas e igualmente intrusivas.

À **ConJur**, a professora também explica como não há um tratamento uniforme para as provas digitais na UE. Alguns países têm regulamentações bem definidas sobre o tema, mas outros ainda contam com normas desatualizadas ou incompletas.

Na Espanha, a legislação traz apenas regras isoladas sobre segurança e preservação de provas. Isso foi desenvolvido e exigido em processos criminais com base nas orientações do Supremo Tribunal daquele país. A Corte costumava ser rigorosa, mas recentemente flexibilizou os

requisitos para admissão de provas digitais: agora, presume-se que elas são autênticas, mas isso pode ser contestado pela defesa de forma fundamentada.

Para a UE, Winter acredita que uma regulamentação uniforme, detalhada e harmonizada "sem dúvida facilitaria muito o intercâmbio de provas digitais para fins de prova criminal", até para evitar insegurança jurídica e custos com perícias.

Ela ainda ressalta que "a manutenção da cadeia de custódia não tem um fim em si mesma, mas tem um valor instrumental". Esse procedimento garante a "indenidade" da prova, mas não sua validade.

Nos sistemas jurídicos de alguns países, a quebra da cadeia de custódia não impede a admissão da prova digital, mas traz dúvidas sobre sua autenticidade, o que pode ser levado em conta pelo juiz ao avaliá-la. Já outros países tendem a excluir a prova em caso de violação da cadeia de custódia.

Leia a seguir a entrevista:

ConJur — *Como as provas digitais são tratadas na Espanha e na Europa? As regras são muito distintas?*
Lorena Bachmaier Winter — Essa é uma questão que analisamos no desenvolvimento de um projeto que dirigi no *European Law Institute* (ELI), com o objetivo de elaborar uma proposta legislativa sobre provas eletrônicas, em particular, as de natureza transfronteiriça. Como consequência desse projeto, e também de um projeto anterior (dirigido pela Universidade de Bolonha, na Itália, e financiado pela União Europeia), pudemos confirmar que, no âmbito da UE, não há harmonização legislativa quanto a esse tema.

Enquanto alguns ordenamentos jurídicos contêm regulamentações muito precisas — como é o caso da Lei de Processo Penal espanhola, conhecida como Lecrim, que foi objeto de uma reforma muito acertada em 2015 —, em outros ordenamentos jurídicos as regulamentações legais não foram atualizadas ou revelam-se ainda incompletas.

Apesar disso, como quase todos os Estados-membros da UE são signatários da Convenção de Budapeste e de seus protocolos adicionais, há um certo grau de aproximação jurídica.

Por outro lado, há muita troca de informações entre a comunidade de informáticos das diferentes forças policiais de cada Estado, de modo que se espalhou uma prática bastante semelhante em relação aos protocolos que eles seguem para análise de dados e, em particular, para a cadeia de custódia. As maiores divergências podem ser encontradas principalmente na gravação remota de sistemas eletrônicos.

Uma regulamentação jurídica detalhada e harmonizada sem dúvida facilitaria muito o intercâmbio de provas digitais para fins de prova criminal. Estamos trabalhando nesse sentido, embora ainda haja certa resistência por parte de alguns Estados-membros em aceitar uma normativa europeia probatória.

ConJur — *As provas digitais representam um novo paradigma no Direito Probatório ou no processo penal em geral?*

Lorena Bachmaier Winter — As regras tradicionais sobre provas documentais não se ajustam às particularidades das provas digitais, nem na forma como são adquiridas, nem em sua conservação ou produção.

No futuro, a sociedade digital e a expansão dos sistemas de vigilância em massa e de prevenção extensiva gerarão uma mudança de enfoque no processo penal. Tendo em vista as dimensões que a coleta de informações adquiriu e as possibilidades tecnológicas de vigilância em massa, é natural nos perguntarmos se não está se introduzindo de forma sub-reptícia um sistema alternativo ou adicional de prevenção — e até mesmo de punição — de delitos, permeando as estruturas processuais.

Em muitos âmbitos, a fronteira entre prevenção e repressão tende a diminuir, pois, por um lado, o Direito Penal foi da repressão para a prevenção e, por outro, as medidas de Direito Administrativo tendem a ter um caráter punitivo. Isso, sem dúvida, tem um impacto sobre os direitos fundamentais, mas também sobre a própria concepção do processo penal.

Embora esse tipo de processo tenha sido tradicionalmente concebido como um marco de garantias para proteger o indivíduo de intromissões indevidas do Estado e para impedir o uso abusivo do *ius puniendi*, podemos observar hoje medidas igualmente intrusivas fora do escopo do Direito Penal e, portanto, fora das garantias previstas pelo processo penal.

Ao mesmo tempo, o uso de amplas medidas preventivas também levou ao surgimento de uma nova categoria de pessoas — as chamadas "pessoas de interesse". Elas não chegam a se qualificar como suspeitas para processos criminais, mas considera-se que devem ser mantidas sob um "radar de controle". Isso naturalmente nos leva a perguntar como determinados indivíduos se tornam "pré-suspeitos" ou "suspeitos preventivos" e, acima de tudo, quais são seus direitos nessa esfera de "justiça preventiva", voltada a fins de segurança.

A situação atual na luta contra certos tipos de crime mostra que determinadas pessoas apresentam um risco potencial de se vincularem a atividades criminosas e que os sistemas de vigilância em massa baseados em algoritmos as identificam como pessoas de interesse ou "pré-suspeitos". Uma vez classificadas pelo algoritmo nessa categoria, elas podem estar sujeitas a vigilância permanente, justamente para coletar inteligência e realizar uma análise mais específica dos riscos potenciais. A "pessoa de interesse" é, então, colocada sob vigilância policial ou de inteligência e, a partir daí, resta apenas um passo para a persecução penal: a análise de todos esses dados digitais para gerar indícios suficientes para iniciar o processo criminal.

ConJur — *O Superior Tribunal de Justiça vem traçando algumas diretrizes sobre a devida documentação da cadeia de custódia de provas digitais no Brasil. Mas ainda não há uma lei específica ou outras normativas sobre o tema. E os órgãos de persecução penal têm dificuldade de resguardar a prova digital. Qual a situação na Espanha e na Europa?*
Lorena Bachmaier Winter — A Lecrim não contém uma regulamentação completa sobre a cadeia de custódia das diferentes provas, apenas regras isoladas sobre a segurança e a preservação das provas. Mas não significa que isso não tenha sido desenvolvido e exigido em processos criminais.

O Supremo Tribunal da Espanha vem definindo há anos o que entende por "cadeia de custódia":

> *"A cadeia de custódia é um conjunto de atos destinados a coletar, transferir e preservar as provas e os vestígios obtidos no curso de uma investigação criminal, atos esses que devem obedecer a uma série de requisitos, a fim de garantir a autenticidade, a inalterabilidade e a indenidade das fontes de prova. A integridade da cadeia de custódia garante que, desde o momento em que os vestígios relacionados ao crime são coletados até se tornarem provas concretas no momento do julgamento, o que estará sujeito à imediação, à publicidade e ao contraditório das partes e ao julgamento do tribunal é o mesmo" (decisão de 2015).*

A manutenção da cadeia de custódia não tem um fim em si mesma, mas tem um valor instrumental. A única coisa que ela garante é a indenidade da prova desde o momento em que é coletada até sua análise, o que, em caso de violação, pode afetar a credibilidade da análise, mas não sua validade.

Em termos de provas eletrônicas, os protocolos seguidos são principalmente os desenvolvidos pela Rede Europeia de Institutos de Ciência Forense (ENFSI), que são muito semelhantes às normas da Organização Internacional para Padronização (ISO), às normas da Associação Espanhola de Normalização (UNE) ou às diretrizes elaboradas pelo Escritório das Nações Unidas sobre Drogas e Crime (UNODC).

Todos esses protocolos são muito semelhantes e estabelecem um sistema de gerenciamento de documentos desde o momento inicial da aquisição da prova até sua valoração no julgamento, registrando detalhadamente as ações que foram realizadas nos dados ou suportes eletrônicos e documentando quem as realizou, sempre preservando a cópia espelhada. Obviamente, na prática, esse processo de documentação variará, dependendo do tipo de acesso aos dados digitais (remoto ou *in situ*, com ou sem um computador aberto, se o computador ou terminal está ou não conectado a uma rede etc.).

As normas internacionais também estabelecem que o registro e a análise de computadores apreendidos devem ser realizados, se possível, em um laboratório forense. O Comissariado Geral da Polícia Científica da Espanha e sua unidade tecnológica seguem as recomendações dos Laboratórios Forenses da Organização Internacional de Polícia Criminal (Interpol).

A partir da aceitação de que os protocolos para preservar a cadeia de custódia são essenciais para garantir a autenticidade das provas, inclusive as eletrônicas, surge a questão das consequências probatórias da quebra da cadeia de custódia.

Alguns sistemas jurídicos — aqueles que baseiam a admissibilidade da prova na confiabilidade da fonte da prova — tenderão a excluir essa prova e impedir que ela seja valorada no julgamento.

Nos ordenamentos jurídicos em que a admissibilidade da prova não é determinada pela sua confiabilidade, mas a exclusão da prova é baseada apenas na sua ilicitude vinculada à proteção dos direitos fundamentais, uma violação das regras da cadeia de custódia não levará

imediatamente à inadmissibilidade da prova eletrônica.

Entretanto, como tal violação introduz dúvidas sobre a autenticidade da prova eletrônica, isso deve ser levado em conta pelo juiz ao valorar a prova. Como no caso de uma testemunha que se sabe ter faltado com a verdade a respeito de algumas informações: o testemunho não é excluído, mas essa perda de credibilidade deve ser levada em conta na hora de avaliá-lo.

O Supremo Tribunal da Espanha começou com uma posição muito rigorosa ao avaliar capturas de tela de mensagens do WhatsApp como prova, afirmando que a prova digital deve ser tratada com todas as cautelas, dada a sua natureza potencialmente manipulável (decisão de 2015), até, mais recentemente, flexibilizar notavelmente os requisitos para sua admissão, reduzindo o *standard* probatório que até então exigia um mínimo de confiabilidade técnica (decisões de 2025). Deixou-se de exigir que o proponente da prova demonstrasse rigorosamente a confiabilidade da prova digital, para, agora, presumir sua autenticidade, salvo impugnação expressa e tecnicamente fundamentada por parte da defesa.

De certa forma, é o mesmo que já se fazia com documentos manuscritos: eles são considerados autênticos, a menos que essa autenticidade seja contestada e seja apresentado algum elemento de prova (pericial) indicando que o documento pode ser falsificado. E quando é invocado o argumento de que a prova digital é altamente manipulável, não se pode ignorar que os documentos escritos também são. Além disso, a prova pericial informática para determinar a autenticidade do documento digital costuma ser mais confiável do que a prova de caligrafia.

Mesmo assim, para evitar a insegurança jurídica e os custos periciais subsequentes, é desejável que as regras sobre a cadeia de custódia sejam regulamentadas de maneira uniforme, pois isso permitiria, justificadamente, fundamentar uma "presunção de autenticidade" da prova digital, dando-lhe maior valor devido à sua comprovada confiabilidade técnica. Isso é o que se busca na proposta do ELI para uma diretiva da UE. No momento, a Comissão Europeia está muito interessada em avançar na tramitação de um instrumento legislativo desse tipo, mas há alguns Estados-membros que se opõem radicalmente, como a Suécia.

ConJur — *O avanço da inteligência artificial (IA) generativa ameaça as práticas consolidadas quanto a esse tema?*
Lorena Bachmaier Winter — Seria arriscado responder a essa pergunta por uma perspectiva científica, pois não temos experiência e conhecimento suficientes para saber ou até mesmo levantar hipóteses sobre como o surgimento da IA generativa alterará a prática probatória atual.

O que está comprovado é que, à medida que os sistemas de IA generativa avançam, o mesmo acontece com os programas para reconhecer o que é gerado por IA e o que é gerado por um ser humano.

A velocidade das mudanças tecnológicas nos obriga a estar atentos a essa nova realidade, e somente por meio de treinamento adequado em tecnologia da informação (TI) ou, na sua falta, com o apoio apropriado de uma equipe de especialistas em TI poderemos ajustar os processos probatórios aos novos desafios impostos pelo mundo digital dominado pela IA.

O que pode ser dito com segurança é que, à medida que nossas vidas se tornam "digitais", a perícia informática se torna a nova "prova-chave" do processo penal.

ConJur — *No Brasil, é comum que policiais acessem mensagens e outros dados de celulares de pessoas presas em flagrante mesmo sem autorização. Mas nem sempre as provas obtidas são anuladas. Como isso é tratado na Espanha e na Europa?*
Lorena Bachmaier Winter — A decisão de 4 de outubro de 2024 do Tribunal de Justiça da União Europeia sobre o acesso a dados de um dispositivo móvel exige não apenas uma base jurídica suficiente, mas também a autorização judicial, que garanta que uma interferência grave em um direito fundamental cumpra os requisitos de adequação, necessidade e proporcionalidade. Especificamente, essa sentença afirma:

> *"Em particular, a fim de garantir que o princípio da proporcionalidade seja respeitado em cada caso concreto por meio da ponderação de todos os elementos pertinentes, é essencial que, quando o acesso das autoridades nacionais competentes aos dados pessoais implicar o risco de uma interferência grave nos direitos fundamentais do titular do interessado, esse acesso seja submetido ao controle prévio de um tribunal ou um órgão administrativo independente.*
>
> *Esse controle prévio exige que o órgão jurisdicional ou a entidade administrativa independente responsável pela realização do controle prévio disponha de todos os poderes e ofereça todas as garantias necessárias para conciliar os diferentes interesses legítimos e direitos concorrentes. No caso específico de uma investigação criminal, esse controle exige que o tribunal ou órgão esteja em condições de ponderar adequadamente, por um lado, os interesses legítimos relacionados às necessidades da investigação no âmbito da luta contra o crime e, por outro, os direitos fundamentais de respeito à vida privada e à proteção dos dados pessoais daqueles cujos dados são afetados pelo acesso."*

No ordenamento jurídico espanhol, o acesso a telefones celulares e dispositivos de armazenamento de dados está sujeito a autorização judicial. Excepcionalmente, a Lecrim permite que, em casos de urgência em que se aprecie um interesse constitucional legítimo que torne imprescindível esse acesso, ele possa ser realizado pela polícia, comunicando ao juiz em um prazo máximo de 24 horas, explicando os motivos da urgência que os levou a agir sem esperar pela autorização judicial. O juiz deve decidir em 72 horas se revoga ou confirma a autorização desde que a medida foi adotada.

Na ausência de tais circunstâncias especiais de urgência, as autoridades e os agentes procederão à apreensão do telefone celular e à proteção dos dados contidos no dispositivo.

Fonte: https://conjur.jumps.com.br/2025-set-07/pericia-informatica-e-nova-prova-chave-do-processo-penal-diz-professora-espanhola/