Considerações sobre a autenticidade e a integridade da prova digital

Guilherme de Siqueira Pastore
Juiz de Direito no Estado de São Paulo

Resumo: A crescente relevância da tecnologia no meio social interfere diretamente na atividade probatória no processo jurisdicional, exigindo a adaptação do juízo de admissibilidade e da valoração dos elementos de prova, para que os existentes em meio eletrônico possam receber tratamento equivalente às informações documentadas em suporte físico, no tocante às exigências de confiabilidade. A falta de critérios adequados e suficientes a garantir a autenticidade e integridade das informações obtidas de fontes digitais, cuja importância se realça neste trabalho, compromete a sua força probante e pode levar a equívocos na apreciação dos fatos pelo julgador.

Palavras-chave: Direito Processual. Direito Probatório. Prova Digital. Documento Eletrônico. Banco de Dados Digital. Autenticidade. Integridade.

1. Introdução

O direito à prova, tal como se reconhece às partes do processo em contraditório, decorre diretamente do direito de ação (art. 5º, inc. XXXV, da Constituição da República) e da garantia da ampla defesa (art. 5º, inc. LV), porque do resultado da atividade probatória depende a delimitação das alegações que, tidas por verdadeiras, sustentarão a incidência normativa, atraindo as respectivas consequências jurídicas, e, por conseguinte, a prestação jurisdicional.

É inócuo alegar sem poder provar o que se alegou. Considerada, por isso, "um dos mais respeitados postulados inerentes à garantia política do devido processo legal" e "um dos fundamentais pilares do sistema processual contemporâneo" (DINAMARCO, 2017, p. 51), a adequada disciplina da produção e da valoração da prova é indispensável à realização de um processo justo.

Com efeito, embora já superada na ciência processual a equivocada noção da busca da chamada "verdade real", não se pode ignorar que haverá chances tanto maiores de se alcançar uma decisão justa, capaz de atender ao escopo magno da jurisdição — de pacificar com justiça —, quanto mais completa e precisa for a reprodução, no processo, dos fatos que lhe constituem o objeto. Não obstante, por uma "falsa suposição de que os fatos não necessitam da atenção dos juristas" (MARINONI; ARENHART, 2011, p. 25), o direito probatório frequentemente recebe atenção desproporcional à sua importância.

O descuido com a temática se tem observado, no cotidiano forense — não apenas no contexto brasileiro (*e.g.*, cf. FRIEDEN; MURRAY; LEIGH, 2011) —, pela crescente utilização de provas digitais sem atenção às suas peculiaridades, com prejuízo relevante à força probante dos elementos de convicção que se trazem aos autos e, em decorrência disso, à própria realização do direito por meio do processo, o que impõe urgente reflexão sobre o fenômeno.

2. Avanço da tecnologia e relevância da fonte de prova digital

A prova segue, pela sua própria natureza e finalidade, as alterações por que passam as relações jurídicas de direito material em que os litígios se originam, bem como a realidade que as envolve. É natural, portanto, que o marcante avanço das tecnologias nos últimos anos implique a alteração da forma pela qual se estabelecem essas relações e inspire o recurso a novos meios de acautelar informações para o futuro, acarretando então significativa mudança no perfil dos elementos que servem a reconstituir, no processo, os fatos pretéritos que se mostrem pertinentes ao desate de uma controvérsia.

A incorporação da tecnologia aos mais variados aspectos da vida tem modificado profundamente as interações humanas e a organização da sociedade, redesenhando desde a comunicação, com a substituição das cartas pelo correio eletrônico, dos telefonemas por mensagens instantâneas de texto, áudio ou vídeo etc.; até os registros – públicos ou privados – que se pretendem perenes, antes inscritos em papel com toda sorte de cautela, e hoje amplamente substituídos pelos sistemas de informática; passando, ainda, por toda espécie de atividade que, prescindindo do contato presencial antes necessário ou criando possibilidades inéditas, se vale da *internet*, por meio da qual se acessa e se transmite um volume imenso de informação, se celebram negócios jurídicos e também se praticam atos ilícitos.

Essa drástica mudança de paradigma reflete na atividade probatória de modo relevante, mas sutil, porque os *meios de prova* – assim entendidos os "instrumentos ou atividades por intermédio dos quais os dados probatórios (elementos de prova) são introduzidos e fixados no processo" (GOMES FILHO, 2005, p. 308) permanecem essencialmente os mesmos, ao menos nos aspectos exteriores mais facilmente perceptíveis, enquanto as *fontes de prova* – "pessoas ou coisas das quais se possam extrair informações capazes de comprovar a veracidade de uma alegação" (DINAMARCO, 2017, p. 97) se alteram e reclamam a elaboração de novos critérios para o seu adequado exame.

Isto é, o novo cenário implica que a produção da prova no processo ainda observa o rito próprio da juntada ou depósito em juízo dos documentos, da tomada de depoimentos e dos exames e vistorias periciais para esclarecimentos de ordem técnica; mas a fonte que se acessa por esses meios, que é o traço verdadeiramente distintivo do que se chama de *prova digital*, ostenta peculiaridades merecedoras de tratamento diferenciado.

A título de exemplo, é notório que "a confiabilidade da prova documental – e a importância singular que os ordenamentos processuais lhe emprestam – assenta-se, exatamente, na *estabilidade do suporte* em que a informação é registrada" (MARINONI; ARENHART, 2011, pp. 563-564).

Ocorre que o documento produzido em meio eletrônico pode, em regra, ser alterado sem esforço, em meios de armazenamento suscetíveis de regravação. Notadamente no fluxo de dados em uma rede de computadores, como a *internet*, a informação armazenada em meio eletrônico "assume caráter temporário, é fungível e de grande volatilidade" (RAMOS, 2014, cap. 2.2), em aparente contradição com a natureza e a própria utilidade da prova documental.

Paradoxalmente, porém, cada reprodução de um documento, seja no mesmo meio ou em outro meio congruente a que transportado, poderá ser idêntica e, assim, indistinta do original, inclusive para efeitos probatórios. A conservação do original com seus atributos próprios pode, assim, exceder a vida útil de um dispositivo de armazenamento, incrementando a estabilidade documental. Já a sua

transposição para meio diverso, por outro lado, como sucede com a materialização em suporte de papel, sempre resultará em cópia, com as ressalvas que a reprodução comporta, pela eventual necessidade de confronto com o original, no meio em que produzido (MARCACINI, 1999, p. 75).

Nesse contexto, em que a atividade probatória recai sobre fontes às quais inaplicáveis diversas premissas sedimentadas no direito processual, já houve alertas para o risco de obsolescência do processo, pelo descompasso com o direito material (CABRAL, 2006, p. 99), ao que atualmente se soma, em decorrência da observação da prática forense, o receio de que os sujeitos do processo – mais especificamente, os profissionais do direito – possam inadvertidamente frustrar, seja pela postulação deficiente ou pela decisão equivocada, a satisfação de direitos legítimos.

3. Confiabilidade da prova documental em meio físico

Historicamente, a estabilidade propiciada pelos documentos, como prova pré-constituída e apta a perpetuar, sem inclinações de ordem subjetiva, a memória dos atos e fatos jurídicos, lhes rendeu tratamento especial na legislação brasileira e estrangeira, que a eles têm conferido pleno crédito (MARINONI; ARENHART, 2011, pp. 548-549), inclusive como único meio idôneo para a prova de determinados fatos, como determinava o art. 401 do Código de Processo Civil instituído pela Lei n.º 5.869, de 11 de janeiro de 1973 (CPC/73)[1].

Sobre as fontes de prova pessoais – também ditas ativas –, ao revés, pesa um estigma de desconfiança, pela pouca efetividade do depoimento pessoal para a obtenção de informações relevantes e, em especial, pelo frequente comprometimento da prova testemunhal pelo esquecimento, pelas falsas memórias, pela parcialidade ou corrupção do depoente, ou mesmo pela morte ou impossibilidade de localização da testemunha.

Assim é que, sem embargo da significativa redução da tarifação legal da prova no Código de Processo Civil em vigor, no qual não se encontra disposição equivalente ao já mencionado art. 401 do CPC/73, a cultura jurídica brasileira ainda se inclina – não sem razão – ao reconhecimento de eficácia probatória superlativa aos registros documentais.

Tal singular relevância dos documentos explica o tratamento minucioso da sua produção e da sua valoração pela lei, uma vez que, embora inerentemente mais segura em comparação com outros meios, a prova documental sabidamente se expõe ao erro, à falsificação, ao perecimento e a toda ordem de utilização inescrupulosa.

Para este fim, a par das exigências de forma solene para determinados atos e das disposições sobre o teor de instrumentos particulares, o cuidado legislativo com a prova documental se observa, exemplificativamente, na disciplina dos pormenores do conteúdo e do momento da lavratura das escrituras públicas, quanto ao que deve ser declarado, como as declarações devem ser conferidas pelos subscritores, quem deve assinar o instrumento público e de que modo os presentes devem se identificar para a prática do ato (art. 215, §§ 1º, 2º e 5º, do Código Civil).

[1] "Art. 401. A prova exclusivamente testemunhal só se admite nos contratos cujo valor não exceda o décuplo do maior salário mínimo vigente no país, ao tempo em que foram celebrados."

Cautela semelhante se revela na exigência de que as certidões dos documentos produzidos ou armazenados em juízo, para que façam a mesma prova que os originais, sejam extraídas pelo próprio escrivão ou sob a sua vigilância (art. 216 do Código Civil e art. 425, inc. I, do Código de Processo Civil); bem como de que os telegramas e as cópias autenticadas por tabelião sejam conferidos com os originais na hipótese de lhes ser impugnada a autenticidade (arts. 222 e 223 do Código Civil).

No aspecto da valoração, a lei ainda cuidou de explicitar algumas noções intuitivas, que na falta de disposição normativa poderiam ser facilmente extraídas das regras de experiência comum, como a de que a declaração constante de documento apenas se presume verdadeira em relação ao signatário (art. 219 do Código Civil e art. 412 do Código de Processo Civil), ou de que, a fim de evitar o uso de documentos antedatados para prejudicar direitos, a data do documento particular não é oponível a terceiros, até que verificada, por dado externo e objetivo – a exemplo da morte de um dos subscritores ou da inscrição em registro público –, a impossibilidade de data diversa (art. 409, parágrafo único, do Código de Processo Civil).

Em síntese, as precauções adotadas pela lei em relação aos documentos permitem extrair ao menos duas premissas que interessam ao tratamento da prova digital: primeiro, que o conteúdo de um documento tem a sua força probante condicionada à sua origem e, em vista dela, à credibilidade que possa merecer o que nele se inscreveu; e, segundo, que a fidelidade das informações, quando não se tem acesso direto ao original, depende da fé de quem as transporta para a forma documental que ingressará nos autos do processo. Este último enfoque é o que, de forma mais direta, interessa à apuração da autenticidade e da integridade, no paralelo que se exporá a seguir.

4. Confiabilidade da prova digital: requisitos de autenticidade e integridade

As premissas estabelecidas a respeito da prova inscrita em suporte físico não se distanciam do que se deve almejar em relação à prova digital. Procedendo-se à adequada decomposição analítica dos documentos em seu aspecto intrínseco, correspondente ao conteúdo, e o seu suporte material, como manifestação concreta e sensível (MARINONI; ARENHART, 2011, p. 255), nota-se que a evolução tecnológica tende sempre a propiciar o uso de novos suportes, sem, contudo, desnaturar a essência nem a finalidade do registro de um fato, que caracterizam a prova em função de seu conteúdo (MARCACINI, 1999, pp. 75-76) e, portanto, inspiram igual prudência no reconhecimento da sua eficácia.

Não é dizer que o suporte do documento seja indiferente. Os seus atributos distintos ensejaram, desde o início, intenso debate a respeito da fidedignidade da prova digital e resistência à sua admissão. E tal resistência não é inédita: no curso da evolução do direito processual, a informática não é a primeira mudança de paradigma imposta pela disseminação de novas tecnologias. Em retrospectiva, os obstáculos que a prova digital enfrentou na prática forense, quanto à sua confiabilidade, foram considerados previsíveis, à vista das semelhantes ressalvas que os tribunais opuseram à fotografia, ainda no século XIX, e às gravações de conversas, já no início do século XX (GOODE, 2009, p. 4).

A resistência inicial é superada, como de fato o foi em todos os casos mencionados, pela crescente familiaridade com a tecnologia, bem como, no caso da prova digital, pelo avanço legislativo que se verificou desde as primeiras advertências sobre a obsolescência do direito processual diante da tecnologia, dispensando o esforço interpretativo antes

necessário que as informações armazenadas em meio eletrônico fossem admitidas como prova e valoradas pelo seu conteúdo.

Na ordem jurídica brasileira, trata-se, principalmente, da Medida Provisória n.º 2.200-2, de 2001, de efeitos perenizados pela Emenda à Constituição n.º 32, de 24 de agosto de 2001, que instituiu a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, outorgando expresso reconhecimento aos documentos eletrônicos produzidos naqueles moldes[2]; bem como da Lei n.º 11.419, de 19 de dezembro de 2006, que disciplinou a informatização do processo digital e, reconhecendo a assinatura digital como garantia de autenticidade das informações (art. 1º, § 2º, inc. III[3], e art. 2º, § 2º[4]), passou a admitir a conservação dos autos em meio exclusivamente eletrônico, desde que garantida a integridade dos dados[5]; e, finalmente, do Código de Processo Civil editado em 2015, que passou a tratar da prova digital, embora com ambiguidades e imprecisões.

Também a Lei n.º 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet no Brasil, ao cuidar de aspectos do tráfego de dados na *internet*, acabou por tocar questões pertinentes à informática em geral e ao direito à prova, embora, por escaparem ao âmbito declarado da sua incidência, não tenham sido objeto de regulação minuciosa, dando ensejo à crítica no sentido de que "o Marco Civil acabou por se tornar uma norma incompleta e passível de sofrer prováveis problemas interpretativos" (MARCACINI, 2015, pp. 469-470).

Na verdade, a dificuldade em relação à prova digital se inverteu: a onipresença da tecnologia, fora do restrito âmbito processual, e a crescente familiaridade dos profissionais do direito com as fontes de prova que frequentemente interessam ao processo – basta pensar nos históricos de conversas travadas por meio de aplicativos de celular, reproduzidos por imagem da tela do dispositivo –, somados à legislação lacunosa, têm resultado na prevalência da confiança individual e subjetiva em cada específica fonte de prova, muitas vezes superficial e alheia às suas características técnicas, em detrimento de análise objetiva dos riscos que a atividade probatória envolve.

O que muitas vezes se negligencia, como efeito desse crescente conforto com a prova digital, é que documentos eletrônicos em sentido estrito e outras informações armazenadas em meio eletrônico são também suscetíveis de falsidade, não apenas ideológica, mas também material. Conforme já se apontou no início, uma sequência de dados armazenada em meio eletrônico pode, desde que o meio comporte regravação ou que a informação seja transportada a outro meio que a comporte, ser alterada, o que pode ser difícil ou mesmo impossível de detectar, pelas próprias peculiaridades do suporte:

---

[2] "Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória."

3 "§ 2º Para o disposto nesta Lei, considera-se:
[...]
III – assinatura eletrônica as seguintes formas de identificação inequívoca do signatário:
a) assinatura digital baseada em certificado digital emitido por Autoridade Certificadora credenciada, na forma de lei específica;
b) mediante cadastro de usuário no Poder Judiciário, conforme disciplinado pelos órgãos respectivos."

[4] "§ 2º Ao credenciado será atribuído registro e meio de acesso ao sistema, de modo a preservar o sigilo, a identificação e a autenticidade de suas comunicações."

[5] "§ 1º Os autos dos processos eletrônicos deverão ser protegidos por meio de sistemas de segurança de acesso e armazenados em meio que garanta a preservação e integridade dos dados, sendo dispensada a formação de autos suplementares."

> *Não há bits falsos. Isto equivale a afirmar que, enquanto no mundo físico, a materialidade do meio em que se propagam as mensagens permite uma série de mecanismos de verificação de sua autenticidade (exame grafotécnico, análise da tinta, do papel em que impressa a mensagem, como papel-moeda, marca d'água, etc.), no meio virtual isto é impossível. (CABRAL, 2006, p. 102).*

As imagens da tela de um computador pessoal ou de um aparelho de telefonia celular, a seu turno, podem ser compostas sem qualquer especial exigência de habilidade em editores de imagens, ou mesmo em sítios eletrônicos que facilitam a criaçãointeiramente nova de uma reprodução visualmente indistinta de uma conversa autêntica. Há numerosas aplicações de *internet* para este fim, facilmente encontradas por intermédio de qualquer sistema de busca, que aqui não se listam para evitar a promoção de software não verificado, potencialmente malicioso.

A lei não passou integralmente ao largo desse risco, ao preceituar que qualquer reprodução mecânica ou eletrônica tem o valor do original, se não for impugnada (art. 225 do Código Civil[6]), e que as fotografias digitais, assim como a forma impressa das mensagens eletrônicas, fazem prova do que reproduzem até a impugnação, cabendo, neste caso, a "autenticação eletrônica" ou a realização de perícia (art. 422, §§ 1º e 3º, do Código de Processo Civil). Igualmente se admitiu o valor probatório dos documentos "produzidos eletronicamente e juntados aos processos eletrônicos com garantia da origem e de seu signatário" (art. 11, *caput*, da Lei n.º 11.419, de 2006), bem assim dos extratos digitais de bancos de dados, desde que atestada a conformidade com o original pelo emitente, sob as penas da lei (art. 425, inc. V, do CPC).

O regramento legal é longe de exaustivo, e deve ser compatibilizado, na jurisdição criminal, com a necessidade de exame pericial do corpo de delito, independentemente de impugnação (art. 158 do Código de Processo Penal[7]), mas permite entrever que, para a atribuição de força probante a documentos eletrônicos e outras informações extraídas de meios digitais, "é fundamental avaliar o grau de segurança e de certeza que se pode ter, sobretudo quanto à sua *autenticidade*, que permite identificar a sua autoria, e à sua *integridade*, que permite garantir a inalterabilidade do seu conteúdo" (DIDIER JÚNIOR; BRAGA; OLIVEIRA, 2016, p. 221-222).

Vale destacar que tais parâmetros – autenticidade e integridade – são expressamente previstos pela legislação processual para o registro de atos processuais eletrônicos (art. 195 do Código de Processo Civil[8]) e podem ser estendidos, seja por analogia, seja pela própria finalidade da prova, a todo e qualquer registro eletrônico que se pretenda utilizar com força probante no processo.

A verificação da presença desses requisitos depende estritamente do suporte em que os dados são armazenados, da forma como são produzidos, da finalidade a que se

[6] "Art. 225. As reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão."

[7] "Art. 158. Quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado."

[8] "Art. 195. O registro de ato processual eletrônico deverá ser feito em padrões abertos, que atenderão aos requisitos de autenticidade, integridade, temporalidade, não repúdio, conservação e, nos casos que tramitem em segredo de justiça, confidencialidade, observada a infraestrutura de chaves públicas unificada nacionalmente, nos termos da lei."

destinam e, sobretudo, do estado da técnica. O essencial, portanto, é que se tenha sempre presente a sua imprescindibilidade e, em caso de dúvida fundada, haja o recurso à prova pericial para que o exercício da jurisdição não seja induzido em erro por elementos que não tenham aptidão ou idoneidade para retratar a realidade.

Não obstante, algumas diretrizes podem, diante do cenário atual, ser traçadas visando à utilidade imediata e a fundamentar o exame de evoluções futuras, para tanto distinguindo-se entre os instrumentos, que como documentos em sentido estrito comportam a assinatura, em alguma forma, dos que concorrem para a sua formação; e os documentos em sentido amplo, que podem, com maior ou menor concurso das pessoas a que digam respeito, ser captados ou mantidos por terceiros idôneos, ou ainda gerados automaticamente por sistemas de informática.

a. A técnica aplicável aos documentos em sentido estrito e semelhantes

Entendem-se como documentos em sentido estrito os escritos que veiculam declarações, originados portanto em uma pessoa, com uma finalidade própria, que assim se ligam ao respectivo autor. São, por exemplo, os contratos, a correspondência eletrônica, peças processuais etc. Também em função da autoria, a eles se assemelham outros registros textuais que, embora não se prestem a perpetuar a memória de um ato ou fato jurídico, têm por conteúdo a produção humana em um suporte relativamente estável, a exemplo do *software*.

Essa característica comum permite que tais documentos – instrumentos negociais, correspondência, código para operação de computadores ou qualquer equivalente – sejam assinados pelos seus autores, à semelhança do que sucede com os documentos físicos, mas com os atributos próprios da tecnologia, a lhes garantir redobrada segurança quanto à autenticidade e à integridade.

A assinatura digital, tal como hoje reconhecida pela lei, é produto de sofisticada técnica elaborada a partir da criptografia assimétrica, que recebe tal denominação por não se basear em um segredo comum (do qual dois interlocutores se valem para, substituindo um signo por outro, segundo padrão uniforme, ofuscar uma mensagem), como nas raízes históricas da prática.

Em breve resumo, essa forma de criptografia atua a partir de um conjunto de chaves, compostas de uma sequência de caracteres gerada por computador, a partir de elementos aleatórios e fórmulas matemáticas avançadas que viabilizam a sua correlação. Com elas, permite-se que, a partir da chave pública (assim chamada porque passível de ampla divulgação, sem prejuízo à segurança do mecanismo), qualquer pessoa ou dispositivo possa codificar conteúdo que apenas poderá ser decifrado pela chave privada (cuja posse é reservada ao emissor do par), bem como identificar a chave pública associada ao conteúdo codificado com a chave privada, tudo sem ter acesso a ela; por conseguinte, sem poder acessar conteúdo destinado ao seu detentor de forma protegida nem simular a autoria do código cifrado, que se relaciona exclusivamente à chave pública correspondente.

Uma vez aplicada essa espécie de criptografia sobre determinado conteúdo, a alteração de qualquer mínima unidade de informação – um *bit* que seja, ainda que em metadados que não repercutam diretamente no seu teor – torna impossível que a decodificação resulte no que se assinou ou mesmo algo próximo, dada a assimetria das

chaves utilizadas no algoritmo; antes produzindo conteúdo ilegível, no caso de texto, ou inteiramente imprestável, no caso de *software*.

Mais comum, porém, é aplicar a assinatura aos chamados *hashes*, *digests* ou *checksums*, que são produtos de algoritmos capazes de reduzir grandes quantidades de dados a uma sequência menor, usualmente de tamanho determinado, alcançada de modo unidirecional. Ou seja, submetido um conjunto de dados a um determinado algoritmo, que resume fragmentos de conteúdo distintos a uma representação igual, de modo a reduzi-los, resulta uma sequência de caracteres própria para identificar o documento, que não é única, pela própria natureza, mas suficientemente distintiva para evitar confusão ou adulteração em um mesmo contexto. Com isso, vincula-se ao autor do documento o *hash* e, se o documento a conferir produzir o mesmo código, quando submetido ao mesmo algoritmo, ter-se-á a certeza da integridade do conteúdo, isento de qualquer mínima modificação.

Esta visão geral, que não se pretende exaustiva do aspecto técnico pelo próprio escopo do trabalho, permite compreender que, com elevadíssimo grau de confiabilidade, o documento assinado digitalmente, por par de chaves de criptografia assimétrica, ostenta as garantias de autenticidade (porque identificável, pelo par de chaves, o autor da assinatura) e de integridade (porque inalterável o documento sem que a assinatura fique prejudicada).

É importante ter em conta que os pares de chaves podem ser emitidos por qualquer pessoa, em qualquer dispositivo, mas a identidade do seu detentor pode ser verificada pelo próprio interessado, obtendo diretamente a chave pública de seu interlocutor, ou a partir de entidades públicas ou privadas de certificação, que se incumbem de atestar que uma determinada chave pertence a uma dada pessoa. É o que se alcançou, no Brasil, sobretudo para fins oficiais, com a criação pela Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, disciplinada pela Medida Provisória n.º 2.200-1, de 2001, já antes mencionada.

Delineado o cenário ideal, contudo, surgem ao menos quatro ordens de problemas na aplicação prática.

O primeiro é que a emissão de certificados digitais por autoridades certificadoras integrantes da ICP-Brasil ainda é um mecanismo custoso e normalmente limitado aos âmbitos de obrigatoriedade na interação com órgãos públicos, como na escrituração fiscal de empresas de porte relevante e no processo eletrônico. Não é algo corrente, que se utilize, por exemplo, no trato negocial ou nas relações de consumo, o que limita severamente a sua utilidade cotidiana – e a esse respeito não há muito de que cogitar, no estudo da técnica jurídica.

O segundo problema decorre do primeiro: são correntes outros métodos de autenticação, alguns equivalentes, outros mais singelos; alguns idôneos, outros não.

De um lado, a infraestrutura oficial não esgota as possibilidades, antes coexistindo com o emprego de mecanismos de criptografia assimétrica e de certificação fora do âmbito da ICP-Brasil. Os outros instrumentos não podem ser desprezados, porque da mesma forma propiciam a verificação de autoria (autenticidade) e de conteúdo conforme à expressão do autor (integridade), cabendo apenas ter clareza quanto à finalidade de cada aspecto do mecanismo para lhe assegurar a força probante. Se emitidos os certificados por entidade idônea, valendo-se da mesma tecnologia, ou se os litigantes prescindirem da intermediação, reconhecendo a titularidade das chaves utilizadas na assinatura, ou ainda se por outros

meios se puder provar o uso de um determinado par de chaves por uma pessoa[9], não há por que recusar eficácia probatória ao documento assinado digitalmente, ainda que fora da macroestrutura eleita pelo Estado para negócios oficiais.

De outro lado, é também frequente, para o fim de autenticação, o envio de correspondência a um endereço de correio eletrônico, ou de mensagem de texto (SMS) a uma linha de telefonia móvel, contendo um código a ser fornecido ao prestador de serviços na própria plataforma, com o escopo de provar que o usuário de um determinado sistema é o titular da linha ou o detentor do endereço de e-mail, e assim atestar a autoria do que ele venha a produzir nesse ambiente. Concorre para essa finalidade o registro da origem de um acesso a um serviço ou aplicação, pelo endereço do Protocolo de *Internet* (IP) e pela porta lógica de origem da conexão, que em tese permitiria, pela consulta aos registros do provedor de conexão à *internet*[10], identificar o autor de dado conteúdo. Mesmo no setor público, a Lei n.º 11.419, de 2006, expressamente faculta a assinatura "mediante cadastro de usuário no Poder Judiciário" (art. 1º, § 2º, inc. III, alínea "b"), sem o uso de certificado digital.

Todos esses métodos propiciam, em alguma extensão, a garantia de autenticidade dos documentos – como correspondência entre o autor indicado em uma declaração e o seu efetivo emitente –, mas não preservam, sem outras cautelas, a integridade dos dados, assim entendida a inalterabilidade do conteúdo, para oportuna prova do seu teor oponível ao próprio autor. Não se pode, só por isso, dizer que sejam inidôneos ou inadmissíveis: é apenas necessário ter consciência das suas limitações, para que a valoração da prova não pressuponha uma característica que o documento não reveste.

A conclusão é diversa a respeito de métodos que, espelhando impropriamente a lógica de documentos físicos, não oferecem segurança alguma, a exemplo da reprodução digitalizada de assinatura manuscrita em documento originalmente digital, que alguns rotulam, a nosso juízo equivocadamente, como assinatura eletrônica. Trata-se, na verdade, de mera imagem digital, que pode ser inserida em qualquer documento por quem detenha uma cópia sua, cópia que pode inclusive ser extraída de um documento no qual já aposta, para eventual reprodução em outros. Em alguns casos, com que já deparamos no exercício da jurisdição, chega-se a copiar, junto com a assinatura, o selo de autenticação da firma por notário público em outro documento[11], o que evidentemente caracteriza falsidade, da qual não se pode inferir qualquer efeito jurídico que não o sancionatório da ilegalidade, prejudicando a verificação de autenticidade a que a assinatura se presta, em qualquer meio.

No mais, o derradeiro problema que se anunciou é o emprego inadequado da assinatura digital, mesmo quando produzida por certificado digital. Merecem destaque dois exemplos do manejo equivocado: a ocultação da assinatura, substituída pela verificação em um sítio na internet presumivelmente confiável, e a materialização do documento digital em suporte físico, em especial para juntada aos autos de processo físicos, denominados pela lei de "convencionais" (art. 439 do Código de Processo Civil).

---

[9] A prova indireta é utilizada para esse fim com êxito na ordem jurídica dos Estados Unidos da América, com base na Regra 901(b)(4) da legislação alcunhada de *Federal Rules of Evidence*. A esse respeito, cf. FRIEDEN; MURRAY; LEIGH, 2011, p. 11.

[10] Os conceitos relativos à internet são aqui referidos na terminologia da Lei n.º 12.695, de 2014 (Marco Civil da Internet no Brasil), sem consideração pelo rigor técnico, de modo a evitar confusão desnecessária no âmbito da discussão, em que a lei vige como posta.

[11] TJSP, 4ª Turma Cível e Criminal do Colégio Recursal 52ª Circunscrição Judiciária – Itapecerica da Serra, Recurso Inominado Cível n.º 1003745-98.2018.8.26.0176, rel. Juiz Guilherme de Siqueira Pastore, julgado em 22/02/2019.

No primeiro caso, o documento é mantido em meio digital, mas, ao invés de se manter íntegro, é alterado para que, às suas margens, conste uma observação de que é autêntico e pode ser verificado em determinado endereço, mediante a inserção de um certo código. Isto é, rompe-se a garantia de integridade do documento pela alteração, ainda que automatizada. Em raras situações, preserva-se íntegro o documento, mas ele é exibido dentro de um enquadramento que faz menção à assinatura. Em nenhum caso, porém, o *hash* assinado é repassado ao usuário, que assim não pode conferir pelos próprios meios a validade da assinatura digital. Esse é, por exemplo, o funcionamento do portal e-SAJ, utilizado pelo Tribunal de Justiça de São Paulo, que na averbação adverte que o documento é cópia do original assinado.

Embora compreensíveis as razões de ordem prática que levam a tanto, seja pela maior facilidade proporcionada ao usuário que não tem familiaridade com a tecnologia, seja pela preservação de dados pessoais atrelados à assinatura digital no âmbito da ICP-Brasil, a solução engendrada prejudica a maior vantagem da assinatura digital, de permitir ao destinatário final a autenticação do específico e exato documento que tem consigo, assegurando que foi assinado pelo detentor da chave, e que nenhum erro de sistema possa atestar tal circunstância equivocadamente. Nesse caso, não é a assinatura, mas a confiança no próprio sistema que sustenta a força probante do documento.

Mais perigoso, porém, é o segundo caso, no qual o equívoco consiste em tomar como prova a materialização do documento digital, que, como já se advertiu no início deste texto, é mera cópia, que não se deve preferir ao original, pela possibilidade de adulteração ou perda acidental das suas características. A própria lei contribui para a aplicação errônea da técnica, ao dispor que a utilização do documento depende da sua conversão à forma impressa e determinar a verificação da sua autenticidade.[12]

À vista de todo o exposto até aqui, é elementar que "o valor probante do documento eletrônico deve ser sempre aferido no ambiente em que ele foi gerado" (RINALDI, 2016, p. 638). Desta forma, a única interpretação possível da disposição normativa, que não anula os benefícios da tecnologia na garantia de autenticidade e integridade da prova, é a de que, *ainda que* integrado aos autos físicos, para melhor compreensão do acervo probatório e garantia do contraditório, o documento digital deve ter a sua autenticidade verificada *no meio digital* e assim certificada pelo escrivão, sem prejuízo de permanecer disponível, *no original*, para verificação independente das partes e, se o caso, exame pericial.

Adotadas estas cautelas, o documento digital oferece segurança superior ao seu semelhante físico, não merecendo, portanto, a resistência que inicialmente se lhe opôs. Caso se tomem pelo valor de face, contudo, soluções tecnicamente insustentáveis, o documento digital não conferirá segurança quanto à sua autenticidade e integridade, não merecendo, então, admissão para fins probatórios.

[12] "Art. 439. A utilização de documentos eletrônicos no processo convencional dependerá de sua conversão à forma impressa e da verificação de sua autenticidade, na forma da lei."

b. Outras informações armazenadas em meio eletrônico

Além dos documentos digitais em sentido estrito, já tratados no tópico anterior, existe um grande volume de outras informações armazenadas eletronicamente[13], de potencial interesse para fins probatórios. Na legislação brasileira, o fundamento normativo que melhor se ajusta ao seu tratamento é o extrato digital de banco de dados, que tem previsão lacônica e pouco utilizada desde a edição do art. 11, § 1º, da Lei n.º 11.419, de 2006[14], e teve sua força probante reiterada pelo art. 425, inc. V, do Código de Processo Civil atualmente em vigor[15].

O banco de dados, no âmbito jurídico, tem sido tratado como uma "compilação de dados, obras e outros materiais organizados de uma maneira sistemática e ordenada, em função de determinados critérios e para finalidades específicas, em condições de serem acessados individualmente por meio eletrônico ou não" (SANTOS, 2005, pp. 321-322), com especial enfoque na proteção de direitos de autor, em conformidade com a Diretiva n.º 96/9/CE, do Parlamento Europeu e do Conselho da União Europeia, e, mais recentemente, sob o ponto de vista da proteção de dados pessoais.

O conceito, porém, é abrangente e alcança também os registros informatizados da Administração Pública, bem como de empresas privadas, com ênfase, pela utilidade, nos dados mantidos por concessionárias de serviços públicos – ou de caráter público, como os "cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres" (art. 43, § 4º, do Código de Proteção e Defesa do Consumidor) –, instituições financeiras e provedores de conexão à *internet* e de aplicação na *internet*, que frequentemente são necessários para o esclarecimento de diversas situações. A corroborar essa percepção, a doutrina destaca a inclusão, no dispositivo legal, do banco de dados privado, sem exigência da presença de autoridade pública na extração da cópia (NEVES, 2016, p. 628).

A manutenção de um banco de dados é complexa e encerra múltiplas funções, de que depende a adequada compreensão do seu valor de prova: primeiro, a produção da informação que dele constará; depois, a efetiva inserção da informação no banco; em seguida, a guarda da informação (o que envolve pessoas físicas ou jurídicas, *software* e *hardware* utilizados no armazenamento dos registros digitais); e, por fim, a extração do conteúdo do banco de dados para qualquer finalidade.

De início, então, sobressai a importância da origem da informação. Caso se trate de reprodução, para fins internos, de conteúdo extraído de outra fonte de prova – como a transcrição do registro em áudio de uma ligação telefônica, ou o resumo de um relatório

[13] Nos Estados Unidos da América, a terminologia empregada é *electronically-stored information (ESI)*, que nos parece adequada para retratar a multiplicidade de formas e meios que a tecnologia propicia, sem prejuízo da sua subsunção à categoria de documentos, em sentido amplo.

[14] "Art. 11. […]
§ 1º Os extratos digitais e os documentos digitalizados e juntados aos autos pelos órgãos da Justiça e seus auxiliares, pelo Ministério Público e seus auxiliares, pelas procuradorias, pelas autoridades policiais, pelas repartições públicas em geral e por advogados públicos e privados têm a mesma força probante dos originais, ressalvada a alegação motivada e fundamentada de adulteração antes ou durante o processo de digitalização."

[15] "Art. 425. Fazem a mesma prova que os originais:
[…]
V – os extratos digitais de bancos de dados públicos e privados, desde que atestado pelo seu emitente, sob as penas da lei, que as informações conferem com o que consta na origem".

elaborado em meio físico –, o extrato digital do banco de dados não poderá suprir a fonte de prova direta, porque de tal modo violada a própria garantia de autenticidade da informação, uma vez rompida a sua vinculação ao seu autor. Ressalva-se, neste particular, a presunção de legitimidade dos atos administrativos, que pode, porém, ser desconstituída diante de prova em contrário, e não desobriga a Administração, em caso de impugnação fundada, de apresentar o suporte documental do que inscreveu nos seus assentos.

Caso, todavia, se trate de informações produzidas em meio exclusivamente eletrônico, assim as inseridas pelo preenchimento de um formulário digital, que têm possibilidade de vinculação ao seu autor, como aquelas resultantes de escrituração eletrônica de transações financeiras, ou mesmo geradas automaticamente por sistemas informatizados, para registro da sua utilização ou em função dela – desde ligações telefônicas, troca de mensagens, acesso a aplicações na *internet*, até dados de localização obtidos de dispositivos móveis utilizados no acesso etc. –, não haverá outro meio de prova possível e a informação deverá ser necessariamente extraída do banco de dados digital.

Em tal situação, pode haver dúvida fundada a respeito da fidelidade da informação contida no banco de dados, sendo então necessário o esclarecimento pelo responsável pela base de dados quanto ao seu funcionamento e, assim, quanto ao crédito que possam merecer os dados por meio dele obtidos.

Essa premissa é aplicável aos históricos de utilização de sistemas informáticos, denominados *logs*, que já foram considerados "registros digitais potencialmente adulteráveis, passíveis de erros gerados pelo sistema que os produz, como ocorre com qualquer sistema informático" (MARCACINI, 2015, p. 471). De fato, o Marco Civil da Internet no Brasil, embora tenha disciplinado a requisição de dados aos provedores de conexão e aplicação, não cuidou da confiabilidade desses dados e, *potencialmente*, as assertivas que embasam a crítica doutrinária são verdadeiras, como também em relação a qualquer documento eletrônico, sem que implementadas formas de garantia do seu conteúdo. Nada impede, porém, que na produção da prova se previnam tais riscos, seja com a declaração do emitente, expressamente prevista no art. 425, inc. V, do Código de Processo Civil, seja por meio de prova pericial, a persistir a dúvida.

No direito estrangeiro, a título exemplificativo e sem pretensão comparatística, encontra-se a prestigiada solução adotada no caso *Lorraine v. Markel American Insurance Co.* em respeitada decisão singular de juiz de instrução (*magistrate judge*), de se exigir prova testemunhal, a respeito da criação, aquisição, manutenção, preservação e extração da informação armazenada em meio digital, inclusive, se o caso, quanto ao funcionamento específico de *software* e *hardware*, a fim de garantir que o sistema tenha adequados mecanismos de segurança; sem prejuízo do exame de metadados, do procedimento adequado para extração dos dados e do reconhecimento do extrato pela testemunha (FRIEDEN; MURRAY; LEIGH, 2011).

O precedente estrangeiro também reforça, em linha com o que se afirmou a respeito das funções relacionadas ao banco de dados, que a fidedignidade da informação original não garante que o seu transporte para o processo conserve os mesmos atributos. É disso que se trata quando a lei exige o atestado, pelo emitente, que as informações conferem com o que consta na origem (art. 425, inc. V, do Código de Processo Civil), sujeitando-o assim a responsabilidade penal e civil, sem prejuízo da impugnação do documento em arguição de falsidade (NERY JÚNIOR; NERY, 2018, p. 1209).

Tão relevante é a responsabilidade pela extração dos dados digitais que o tema recebeu, em outras ordens jurídicas, tratamento mais minucioso, a exemplo da alteração, em 2008, da legislação italiana, na esteira da Convenção sobre o Cibercrime, firmada em Budapeste (CONSELHO DA EUROPA, 2001), a fim de que o *codice di procedura penale* (ITÁLIA, 1988) passasse a exigir a conformidade dos dados extraídos aos respectivos originais e também a sua inalterabilidade[16].

A extração do banco de dados, em suma, é um processo: implica o acesso a um sistema de informática, com controles de permissões, e o adequado manejo de ferramentas previamente instaladas para que se possa chegar a determinado conteúdo, que deve então ser transportado para suporte adequado, com a garantia do responsável pela extração quanto à conformidade com o original, que é a própria base de dados digital.

A prática forense, no entanto, tem se mostrado aquém até mesmo dos rasos parâmetros traçados pela legislação brasileira. São frequentemente juntadas aos autos, como documento ou mesmo em reprodução de baixa qualidade no corpo dos arrazoados, imagens de telas de computador, em que aparentemente se contém um registro informatizado, mas sem nenhum esclarecimento sobre a criação e guarda dos dados, sobre o método de acesso ao banco de dados nem a responsabilidade por essa atividade.

Fica inteiramente prejudicada, dessa forma, a eficácia probatória do banco de dados digital, porque não se pode garantir que a informação é confiável na origem, tampouco que o que foi reproduzido nos autos corresponde ao que consta na origem (autenticidade), sem possibilidade de alteração desde a extração (integridade).

A produção adequada dessa prova pode se dar, por expressa previsão legal, mediante atestado do responsável pela extração dos dados, que pressupõe também a devida justificação sobre os meios utilizados para tanto; ou, por cautela, pela extração dos dados acompanhada por notário e descrita em ata notarial. Pode ainda, na pendência de controvérsia fundada, ensejar exame pericial, a que não se poderão opor restrições de acesso, irrelevante a qualidade dos dados armazenados e o vulto dos sistemas envolvidos, se necessário ao esclarecimento a respeito dos meios de criação e guarda das informações.

c. O caso especial da obtenção forçosa das informações

Um último registro é pertinente, a respeito das informações armazenadas em meio eletrônico que podem, além das hipóteses de oferecimento de extratos digitais com certificação de autenticidade, ser obtidas forçosamente, sobretudo em procedimentos criminais, a partir de dispositivos apreendidos no curso de uma investigação penal, ou do recolhimento de conjuntos de informações obtidas por meio de provedores de aplicação.

Também neste particular a prática forense frequentemente se situa aquém do necessário a atender à natureza e da finalidade da prova digital, podendo-se observar, não raro, a juntada aos autos de meras fotografias de dispositivos eletrônicos, a fim de

[16] "Art. 254-bis. Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni. 1. L'autorita' giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, puo' stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformita' dei dati acquisiti a quelli originali e la loro immodificabilita'. In questo caso e', comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali."

retratar conteúdo ilícito em si mesmo (a exemplo de pornografia infantil) ou reproduzir outras imagens armazenadas, que documentem fatos pertinentes à prática criminosa; além de históricos de comunicação (com tratativas entre criminosos a respeito dos delitos investigados).

Ocorre que a reprodução fotográfica, como já anotado, constitui prova do objeto reproduzido, mesmo no âmbito civil, apenas até que haja impugnação (art. 225 do Código Civil), considerando que a mediação pode implicar prejuízo à sua conformidade com o original (autenticidade); e, por considerações semelhantes, não pode ser tida, em princípio, como prova suficiente no âmbito criminal, sem que se proceda ao exame pericial do corpo de delito, tal como preceituado pelo art. 158 do Código de Processo Penal.

Essa abordagem, ademais, subestima gravemente a riquíssima gama de informações que o exame pericial bem realizado pode fornecer, relativas à utilização do dispositivo, à sua geolocalização etc., além das vicissitudes originadas na complexidade da microinformática atual, que permite a eliminação remota do conteúdo de dispositivos eletrônicos sem nenhum preparo especial, desde que conectados à *internet*, ou ativar criptografia capaz de torná-los indevassáveis às autoridades públicas, mesmo tendo à sua disposição técnicas avançadas e vasto poder computacional.

Essas situações são mencionadas apenas exemplificativamente, porque as possibilidades e dificuldades relacionadas à atividade pericial são muitas e cabem a estudo de maior profundidade técnica, no âmbito da informática, excedentes da proposta deste artigo; mas dos exemplos já é possível inferir que a produção da prova digital "não se compraz com os velhos métodos de busca que se realizavam (e continuam a realizar) na descoberta de provas de outros tipos de criminalidade" (RAMOS, 2014, cap. 2.3), podendo o descuido com a técnica inviabilizar a confirmação da autenticidade e da integridade das informações com repercussão probatória.

Esta a questão central: não há técnica única ou estanque para o exame pericial de uma infinidade de dispositivos com características próprias, mas, a despeito do concurso de técnico para a realização do exame, é sempre possível ao julgador e às partes do processo zelar pela garantia de autenticidade e integridade das informações submetidas ao exame do perito, controlando os métodos empregados para tal fim.

A modificabilidade inerente aos meios de armazenamento digitais, se não devidamente acautelada por meios justificadamente suficientes, expõe o conteúdo de interesse probatório, em tese, ao acréscimo, à supressão e à alteração, com aptidão para conduzir à conclusão de que o material apreendido não se relaciona ao detentor do equipamento ou do titular da conta em determinado serviço *online* (falta de autenticidade), ou mesmo de que o material, conquanto original, possa ter sofrido alteração proposital, seja de grande extensão, em prejuízo do contexto, ou pontual, com a inclusão em um acervo aparentemente autêntico de informações inverídicas, anulando assim a sua força probante, por falta de integridade.

Independentemente da solução técnica a ser adotada em cada caso, tal precaução somente tem valor se a posse do material for restrita a pessoas idôneas e desinteressadas no resultado da investigação, demonstrando-se tal circunstância por fiel registro documental, complementado por testemunhas, se necessário, anotando-se o uso de lacres, transporte e acondicionamento. É o que se chama, no direito estrangeiro, de cadeia de custódia (*chain of custody*), também identificada na célebre decisão do já citado caso

Lorraine v. Markel American Insurance Co. como pressuposto elementar da admissibilidade da prova digital (RASHBAUM; KNOUFF; MURRAY, 2012, p. 4).

A prova pericial não subtrai, portanto, ao julgador o conhecimento dos meios de investigação e da validade da prova, cabendo às partes e ao juiz zelar diretamente, sem embargo do concurso de auxiliar eventual, pela validade da prova digital, que depende de que sejam garantidos, desde a colheita até valoração, os atributos da autenticidade e da integridade.

5. Conclusão

Pela exposição contida nos tópicos precedentes, pretendeu-se demonstrar que a tecnologia abriu caminho, antes mesmo da disciplina legislativa, para a atividade probatória em meio eletrônico, considerando que a prova é um dos grandes pontos de contato entre o processo e a realidade exterior, cuja evolução necessariamente acompanha. Essa antecipação foi possível porque, a despeito das peculiaridades do suporte digital, as informações armazenadas em meio eletrônico guardam com os documentos, em sentido amplo, identidade de conteúdos e finalidades.

O suporte digital, por si só, permite a alteração irrestrita e indetectável das informações nele armazenadas, mas, paradoxalmente, oferece, na presença de determinadas cautelas, garantias de autenticidade e integridade superiores às que o suporte físico jamais foi capaz de propiciar. Essa contradição enseja a oscilação da doutrina e da prática forense entre extremos, desde a absoluta desconfiança e prevenção em relação ao meio, até a confiança excessiva, desatenta aos atributos de cada específica fonte de prova.

A proposição que se extrai dessas premissas é de que a produção de prova digital depende, quando indisponíveis os direitos em litígio, inclusive no processo criminal, ou quando impugnada a reprodução, de escorreita demonstração de autenticidade e integridade, a ser assegurada por meios técnicos adequados, sob pena de o elemento de prova obtido de fonte digital não carregar eficácia probatória.

Tais meios não se restringem à previsão legal de assinatura digital de documentos eletrônicos, com o uso de certificado emitido no âmbito da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, mas alcançam também quaisquer outros mecanismos que, pelo uso adequado da tecnologia, possam garantir, ainda que parcialmente, os mesmos atributos; excluídos, porém, os esforços que nada garantem quanto à autenticidade e integridade e se relacionam ao desconhecimento da prova digital, como a reprodução digitalizada de assinaturas manuscritas em documentos eletrônicos.

No específico caso dos extratos digitais de bancos de dados, além da atenção à formação do seu conteúdo na origem, a garantia de autenticidade e integridade depende de procedimento documentado de extração, que pode ser atestado pelo emitente, sob pena de responsabilidade civil e criminal, ou fiscalizado por delegado do serviço notarial, em ata própria; não se admitindo, contudo, imagens digitais coligidas sem nenhuma explicação, cuidado ou segurança, como tem sido recorrente na prática forense.

Por fim, em relação à fonte de prova que não escape à necessidade da técnica pericial para a sua produção, de que se destacam os materiais apreendidos no curso de investigação, é inafastável o controle jurisdicional da atividade do perito, de modo a garantir a autenticidade e a integridade, pela supervisão da técnica empregada e pela

observação da cadeia de custódia, a fim de que o manejo do material com fins probatórios seja reservado a pessoas idôneas e desinteressadas no resultado da prova.

Referências

BRASIL. *Decreto-Lei n.º 3.689, de 3 de outubro de 1941*. Código de Processo Penal. Brasília, DF: 1941. Disponível em: http://bit.ly/30xq6z6. Acesso em: 27 set. 2019.

BRASIL. *Lei n.º 5.869, de 11 de janeiro de 1973*. Institui o Código de Processo Civil. Brasília, DF: 1973. Disponível em: http://bit.ly/2RpgtP7. Acesso em: 27 set. 2019.

BRASIL. *Lei n.º 8.078, de 11 de setembro de 1990*. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: 1990. Disponível em: http://bit.ly/2R70Vkd. Acesso em: 27 set. 2019.

BRASIL. *Emenda constitucional n.º 32, de 11 de setembro de 2001*. Altera dispositivos dos arts. 48, 57, 61, 62, 64, 66, 84, 88 e 246 da Constituição Federal, e dá outras providências. Brasília, DF: 2001. Disponível em: http://bit.ly/2ud8LPS. Acesso em: 27 set. 2019.

BRASIL. *Medida provisória n.º 2.200-2, de 24 de agosto de 2001*. Institui a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Brasília, DF: 2001. Disponível em: http://bit.ly/2RuS5eG. Acesso em: 27 set. 2019.

BRASIL. *Lei n.º 10.406, de 10 de janeiro de 2002*. Institui o Código Civil. Brasília, DF: 2002. Disponível em: http://bit.ly/389l1jk. Acesso em: 27 set. 2019.

BRASIL. *Lei n.º 11.419, de 19 de dezembro de 2006*. Dispõe sobre a informatização do processo judicial; altera a Lei nº 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências. Brasília, DF: 2006. Disponível em: http://bit.ly/38lABIN. Acesso em: 27 set. 2019.

BRASIL. *Lei n.º 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: 2014. Disponível em: http://bit.ly/2Nz5KAA. Acesso em: 27 set. 2019.

BRASIL. *Lei n.º 13.105, de 16 de março de 2015*. Código de Processo Civil. Brasília, DF: 2015. Disponível em: http://bit.ly/3738LR7. Acesso em: 27 set. 2019.

CABRAL, Antonio do Passo. A eficácia probatória das mensagens eletrônicas. *Revista de Processo*, São Paulo, v. 31, n. 135, p. 97-131, 2006.

CONSELHO DA EUROPA. *Convention on cybercrime*: ETS no. 185. Estrasburgo: Council of Europe, 2001. Disponível em: http://bit.ly/38iC7eF. Acesso em: 27 set. 2019.

CONSELHO DA UNIÃO EUROPEIA. Parlamento Europeu. *Directiva 96/9/CE do Parlamento Europeu e do Conselho, de 11 de março de 1996, relativa à protecção jurídica das bases de dados*. Disponível em: http://bit.ly/2uUBJ7C. Acesso em: 27 set. 2019.

DIDIER JÚNIOR, Fredie; BRAGA, Paula Sarno; OLIVEIRA, Rafael Alexandria de. *Curso de direito processual civil*. 11. ed. Salvador: Jus Podivm, 2016. v. 2.

DINAMARCO, Cândido Rangel. *Instituições de direito processual civil*. 7. ed. São Paulo: Malheiros, 2017. v. 3.

FRIEDEN, Jonathan D.; MURRAY, LEIGH M. The admissibility of electronic evidence under the Federal Rules of Evidence. *Richmond Journal of Law and Technology*, Richmond, v. 17, n. 2, p. 1-40, 2011.

GOMES FILHO, Antonio Magalhães. Notas sobre a terminologia da prova (reflexos no processo penal brasileiro). *In*: YARSHELL, Flávio Luiz; MORAES, Maurício Zanoide de (coord.). *Estudos em homenagem à professora Ada Pellegrini Grinover*. São Paulo: DPJ, 2005.

GOODE, Steven. The admissibility of electronic evidence. *The Review of Litigation*, Austin, v. 29, n. 1, p. 1-64, 2009.

ITÁLIA. *Decreto del Presidente dela Repubblica 22 settembre 1988, n. 447*. Approvazione del codice di procedura penale. Roma: 1988. Disponível em: http://bit.ly/30xJz32. Acesso em: 27 set. 2019.

MARCACINI, Augusto Tavares Rosa. O documento eletrônico como meio de prova. *Revista de Direito Imobiliário*, São Paulo, v. 22, n. 47, p. 70-101, 1999.

MARCACINI. Provas digitais: limites constitucionais e o Marco Civil da Internet. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & internet III*. São Paulo: Quartier Latin, 2015. t. 2.

MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz. *Prova*. 2. ed. São Paulo: Revista dos Tribunais, 2011.

NEVES, Daniel Amorim Assumpção. Da produção da prova documental (arts. 434 a 438). *In*: CABRAL, Antonio do Passo; CRAMER, Ronaldo (coord.). *Comentários ao novo Código de Processo Civil*. 2. ed. Rio de Janeiro: Forense, 2016.

RAMOS, Armando Dias. *A prova digital em processo penal*: o correio eletrônico. Lisboa: Chiado, 2014.

RASHBAUM, Kenneth N.; KNOUFF, Matthew F.; MURRAY, Dominique. Admissibility of non-U.S. electronic evidence. *Richmond Journal of Law and Technology*, Richmond, v. 18, n. 3, p. 1-76, 2012.

RINALDI, Luciano. Dos documentos eletrônicos (arts. 439 a 441). *In*: CABRAL, Antonio do Passo; CRAMER, Ronaldo (coord.). *Comentários ao novo Código de Processo Civil*. 2. ed. Rio de Janeiro: Forense, 2016.

SANTOS, Manoel J. Pereira dos. Considerações iniciais sobre a proteção jurídica das bases de dados. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (coord.). *Direito & internet*: aspectos jurídicos relevantes. 2. ed. São Paulo: Quartier Latin, 2005. v. 1.