PEDRO AUGUSTO ZANIOLO

CRIMES MODERNOS

O IMPACTO DA TECNOLOGIA NO DIREITO

6ª EDIÇÃO
Revista, ampliada
e atualizada

2024

EDITORA JusPODIVM
www.editorajuspodivm.com.br

a ser reconhecida entre outras que com ela guardem qualquer semelhança, não sendo, de fato, um requisito estrito para a validade da prova[83].

> **Art. 226.** Quando houver necessidade de fazer-se o reconhecimento de pessoa, proceder-se-á pela seguinte forma:
>
> I – a pessoa que tiver de fazer o reconhecimento será convidada a descrever a pessoa que deva ser reconhecida;
>
> Il – a pessoa, cujo reconhecimento se pretender, será colocada, se possível, ao lado de outras que com ela tiverem qualquer semelhança, convidando-se quem tiver de fazer o reconhecimento a apontá-la;
>
> III – se houver razão para recear que a pessoa chamada para o reconhecimento, por efeito de intimidação ou outra influência, não diga a verdade em face da pessoa que deve ser reconhecida, a autoridade providenciará para que esta não veja aquela;
>
> IV – do ato de reconhecimento lavrar-se-á auto pormenorizado, subscrito pela autoridade, pela pessoa chamada para proceder ao reconhecimento e por duas testemunhas presenciais.
>
> Parágrafo único. O disposto no nº III deste artigo não terá aplicação na fase da instrução criminal ou em plenário de julgamento.

A jurisprudência do Superior Tribunal de Justiça anteriormente admitia a possibilidade do reconhecimento do acusado por meio fotográfico, mesmo na ausência da observância integral das formalidades previstas no art. 226, CPP. Nesse contexto, o reconhecimento fotográfico do réu, quando posteriormente ratificado em Juízo e respaldado pelo contraditório e ampla defesa, era considerado um meio idôneo de prova apto a fundamentar a condenação[84].

Entretanto, em conformidade com a recente orientação estabelecida pela 6ª Turma do STJ: não é admissível condenar alguém *exclusivamente* com base em reconhecimento por fotografia. Esse posicionamento se justifica pelo rigor probatório necessário para evitar erros judiciários. As conclusões são as seguintes[85]:

a) O reconhecimento de pessoas, seja presencial ou por fotografia, deve observar o procedimento previsto no art. 226, CPP, cujas formalidades representam garantia mínima para aqueles que estão na condição de suspeitos da prática de um crime;

---

83 TRF3, 11ª Turma, ACrim 0016402-28.2017.4.03.6181, Rel. Des. Federal José Marcos Lunardelli, publ. 18.05.2020.

84 STJ, 5ª Turma, AgRg-AgRg-AREsp 1.631.690, Rel. Min. Ribeiro Dantas, publ. 29.06.2020.

85 STJ, 6ª Turma, HC 1.631.690, Rel. Min. Rogerio Schietti Cruz, publ. 18.12.2020.

b) Diante dos efeitos e dos riscos de um reconhecimento falho, a inobservância do procedimento descrito na referida norma processual torna inválido o reconhecimento da pessoa suspeita, não podendo servir como base para eventual condenação, mesmo se confirmado em Juízo;
c) O Magistrado pode realizar, em Juízo, o ato de reconhecimento formal, desde que observado o devido procedimento probatório. Além disso, ele pode convencer-se da autoria delitiva através do exame de outras provas que não guardem relação de causa e efeito com o ato viciado de reconhecimento; e
d) O reconhecimento do suspeito por meio da simples exibição de fotografia(s) ao reconhecedor, embora deva seguir o mesmo procedimento do reconhecimento pessoal, deve ser considerado uma etapa anterior a eventual reconhecimento pessoal e, portanto, não pode servir como prova em ação penal, mesmo que confirmado em Juízo.

Em um julgamento concluído em 23.02.2022, a 2ª Turma do STF deu provimento ao RHC 206.846, da relatoria do Min. Gilmar Mendes, para absolver um indivíduo preso em São Paulo após ser reconhecido por fotografia, devido à nulidade do reconhecimento fotográfico e à ausência de provas para a condenação. Referindo-se à decisão no julgamento do mencionado HC 598.886 no STJ, foram estabelecidas três teses[86]:

a) O reconhecimento de pessoas, seja presencial ou por fotografia, deve obedecer ao procedimento do art. 226, CPP, cujas formalidades representam garantia mínima para suspeitos;
b) A falta de observância desse procedimento invalida o reconhecimento da pessoa suspeita, não podendo fundamentar eventual condenação ou decretação de prisão cautelar, mesmo se refeito e confirmado em Juízo. Se declarada a irregularidade do ato, uma condenação já proferida pode ser mantida, desde que fundamentada em provas independentes e não contaminadas; e
c) A realização do ato de reconhecimento pessoal precisa ser justificada por elementos que indiquem, mesmo que de maneira verossímil, a autoria do fato investigado, evitando medidas investigativas genéricas e arbitrárias que aumentem os erros na verificação dos fatos.

O Projeto de Lei 676/2021, de autoria do Senador Marcos do Val, propõe alterações no Código de Processo Penal (Capítulo VII) para regulamentar o

[86] STJ, 6ª Turma, HC 712.781, Rel. Min. Rogerio Schietti Cruz, publ. 22.03.2022.

reconhecimento fotográfico de pessoas, buscando evitar um grande número de inocentes condenados com base unicamente em fotografias.

Com o exato propósito de prevenir a condenação de inocentes e facilitar a responsabilização dos culpados, o Plenário do CNJ aprovou a Resolução 484, de 19.12.2022[87], que estabelece diretrizes para a realização do reconhecimento de pessoas em procedimentos e processos criminais, bem como para a sua avaliação no âmbito do Poder Judiciário.

No que diz respeito ao reconhecimento fotográfico, destacam-se os seguintes julgados:

- *STF, 1ª Turma*: RHC 176.025, publ. 25.11.2021;
- *STF, 2ª Turma*: RHC 206.846, publ. 25.05.2022;
- *STJ, 5ª Turma*: AgRg-HC 788.350, publ. 19.12.2022; HC 617.717, publ. 24.08.2021; HC 598.886, publ. 18.12.2020; HC 427.051, publ. 10.04.2018; AgRg-AREsp 683.840, publ. 23.03.2018 e HC 408.857, publ. 16.02.2018;
- *STJ, 6ª Turma*: AgRg-HC 761.921, publ. 25.05.2023; HC 700.313, publ. 10.06.2022; HC 682.108, publ. 16.05.2022; HC 681.704, publ. 13.05.2022; REsp 1.964.391, publ. 13.05.2022; HC 652.074, publ. 06.05.2022; HC 725.007, publ. 03.05.2022; HC 640.868, publ. 07.06.2021; HC 598.886, publ. 18.12.2020; RHC 133.408, publ. 18.12.2020; AgRg-AREsp 1.204.990, publ. 01.03.2018; AgInt-AREsp 1.000.882, publ. 24.11.2016 e HC 224.831, publ. 01.08.2016; e
- *TJDF, 2ª TCrim*: ACrim 0001221-50.2017.8.07.0002, publ. 10.09.2021.

Nas perícias conduzidas em material fotográfico com o objetivo de identificação para fins de autoria delitiva, deve-se prestar especial atenção à possibilidade de existirem *gêmeos idênticos*.

Em 2017, testes realizados com o sistema de reconhecimento facial do *iPhone X*, capaz de identificar 30 mil pontos, relataram casos de confusão com gêmeos, resultando na liberação indevida do acesso ao *smartphone* para o irmão gêmeo[88].

---

87 Disponível em: https://atos.cnj.jus.br/atos/detalhar/4883.

88 SOARES, Bruno. iPhone X: testes comprovam que Face ID se confunde com rostos de gêmeos. **Tech Tudo**, 7 nov. 2017. Disponível em: <https://www.techtudo.com.br/noticias/2017/11/iphone-x-testes-comprovam-que-face-id-se-confunde-com-rostos-de-gemeos.ghtml>. Acesso em: 25 ago. 2020.

12

DOCUMENTOS ELETRÔNICOS

12.1 DOCUMENTO ELETRÔNICO E DOCUMENTO CONVENCIONAL

Documento, no âmbito da técnica jurídica, pode ser conceituado como "o papel escrito, em que se mostra ou se indica a existência de um ato, um fato, ou de um negócio"[1].

No entanto, essa definição parece inadequada quando aplicada aos documentos veiculados na rede Internet: os *documentos eletrônicos*, que, ao contrário, caracterizam-se pelo *desapego ao papel*.

Moacyr Amaral Santos conceitua documento como *uma coisa representativa de um fato*. Nesse sentido, argumenta-se que o documento eletrônico não pode ser considerado um documento, pois não é uma coisa e, portanto, não pode representar um fato. No entanto, ao examinar a perspectiva do *registro do fato*, é possível inferir que o conceito se ajusta perfeitamente, pois uma sequência de bits pode ser interpretada por meio de *softwares*, revelando o pensamento ou a vontade de quem o elaborou. Isso exige do intérprete uma abstração para compreendê-lo[2].

---

1 SILVA, De Plácido e. **Vocabulário jurídico**. 24. ed. Rio de Janeiro: Forense, 2004. p. 493.

2 BRASIL, Angela Bittencourt. O documento físico e o documento eletrônico. **Jus Navigandi**, Teresina, a. 5, n. 42, jun. 2000. Disponível em: <https://jus.com.br/artigos/1781/o-documento-fisico-e-o-documento-eletronico>. Acesso em: 25 ago. 2020.

Dessa forma, define-se *documento eletrônico* como "uma sequência de *bits* que, traduzida por meio de um determinado programa de computador, seja representativa de um fato"[3] ou "a representação de um fato concretizada por meio de um computador e armazenado em formato específico (organização singular de *bits* e *bytes*), capaz de ser traduzido ou apreendido pelos sentidos mediante o emprego de programa (*software*) apropriado"[4].

É importante destacar a diversidade de tipos de documentos eletrônicos, devido à ampla variedade de *softwares* que possibilitam sua criação e interpretação.

Sob o aspecto *arquivístico*, é fundamental diferenciar entre documento *eletrônico* e *digital*. Uma petição inicial em formato PDF seria considerada um *documento digital*, pois se originou de *softwares* como *Libre Office* ou *Microsoft Word*. Músicas em MP3 e vídeos em AVI também se enquadram nessa categoria. Contudo, para este estudo, o foco está na *assinatura digital* como requisito formal dos sistemas de tecnologia de informação nas Cortes de Justiça nacionais, como *Projudi* e *PJe*. A assinatura digital não é aplicável a músicas e audiovisuais. Destarte, desnecessária a exploração dessa discussão técnica: adotaremos a abordagem preconizada pela *doutrina majoritária*, tratando esses elementos como documentos *eletrônicos*.

Pode-se assinar ou não documentos eletrônicos[5].

A assinatura *digital* de documentos eletrônicos difere da assinatura convencional feita à mão em documentos físicos.

Nos documentos eletrônicos, não se trata simplesmente da digitalização por meio de um *scanner* ou da inserção de uma imagem digitalizada contendo a assinatura.

Esses documentos são gerados por *softwares*, e respaldados por ferramentas específicas, como a *assinatura digital* e a *certificação digital*, o que lhes confere *confiabilidade* e *integridade* de conteúdo.

Ao trabalhar com documentos eletrônicos, é importante observar que não é possível distinguir o *original* da *cópia*. Considera-se *original* o

---

3 MARCACINI, Augusto Tavares Rosa. **O documento eletrônico como meio de prova**. Disponível em: <http://augustomarcacini.net/index.php/DireitoInformatica/DocumentoEletronico>. Acesso em: 25 ago. 2020.

4 CASTRO, Aldemario Araújo. **O documento eletrônico e a assinatura digital**: uma visão geral. **Jus Navigandi**, Teresina, a. 7, n. 54, fev. 2002. Disponível em: <https://jus.com.br/artigos/2632/o-documento-eletronico-e-a-assinatura-digital>. Acesso em: 25 ago. 2020.

5 LORENZETTI, Ricardo Luis. Informática, cyberlaw, e-commerce. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coords.). **Direito & internet**. São Paulo: Edipro, 2001. p. 428.

documento eletrônico que possui a garantia de ter sido entregue na sua totalidade ao destinatário[6].

Se considerarmos a possibilidade de reprodução de um documento eletrônico em formato físico (e vice-versa), torna-se factível discutir sobre *original* e *cópia*. Se um documento foi inicialmente elaborado e assinado em meio eletrônico, a sequência de *bits* correspondente é considerada original, independentemente do meio de armazenamento utilizado. No entanto, podemos referir-nos a uma cópia do documento eletrônico quando essa mesma sequência de *bits*, traduzida por um programa de computador, é impressa em papel. Nesse cenário, o papel é considerado cópia, enquanto o arquivo eletrônico com assinatura criptográfica é reconhecido como original[7].

Qualquer alegação de desconformidade entre o original e a cópia exigirá uma análise do documento eletrônico, utilizando um computador e *softwares* específicos capazes de ler o arquivo eletrônico e reconhecer a assinatura. Por outro lado, um documento originalmente registrado em papel pode ser introduzido em formato eletrônico no computador, por meio de um *scanner* (processo de digitalização), seja para fins de armazenamento, recuperação rápida ou transmissão. Nesse caso, o original em papel existe, e o documento eletrônico representa apenas a cópia. Qualquer incerteza quanto à autenticidade da cópia eletrônica exigirá a verificação do original em papel[8].

No CPC/2015, as disposições referentes aos documentos eletrônicos são abordadas nos arts. 439 a 441:

> **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.
>
> **Art. 440.** O juiz apreciará o valor probante do documento eletrônico não convertido, assegurado às partes o acesso ao seu teor.
>
> **Art. 441.** Serão admitidos documentos eletrônicos produzidos e conservados com a observância da legislação específica.

---

6 BRASIL, Angela Bittencourt. O documento físico e o documento eletrônico. **Jus Navigandi**, Teresina, a. 5, n. 42, jun. 2000. Disponível em: <https://jus.com.br/artigos/1781/o-documento-fisico-e-o-documento-eletronico>. Acesso em: 25 ago. 2020.

7 MARCACINI, Augusto Tavares Rosa. O documento eletrônico como meio de prova. Disponível em: <http://augustomarcacini.net/index.php/DireitoInformatica/DocumentoEletronico>. Acesso em: 25 ago. 2020.

8 MARCACINI, Augusto Tavares Rosa. O documento eletrônico como meio de prova. Disponível em: <http://augustomarcacini.net/index.php/DireitoInformatica/DocumentoEletronico>. Acesso em: 25 ago. 2020.

12.2 CRIPTOGRAFIA, ASSINATURA DIGITAL E CERTIFICADO DIGITAL

12.2.1 Criptografia

O termo *criptografia* tem origem em palavras gregas que significam *escrita secreta*. No estudo dessa disciplina, é comum distinguir *cifra* e *código*. *Cifra* "é uma transformação de caractere por caractere ou de *bit* por *bit*, sem levar em conta a estrutura linguística da mensagem". O *código*, por sua vez, "substitui uma palavra por outra palavra ou símbolo". Embora o código tenha tido um passado glorioso, como no caso de sua utilização pelas Forças Armadas dos Estados Unidos durante a Segunda Guerra Mundial, por meio dos índios navajo, que se comunicavam utilizando palavras específicas de seu idioma nativo para representar termos militares, atualmente ele não é amplamente utilizado[9].

Os primeiros sistemas de criptografia para comunicação surgiram com a Primeira Guerra Mundial, mas o grande avanço ocorreu durante a Segunda Guerra e se desenvolveu nos anos 1970, com a invenção do sistema de codificação *assimétrica*, mais sofisticado que o sistema *simétrico*. Os dois se distinguem da seguinte maneira: o sistema *simétrico*, ou de *chave única*, utiliza a mesma chave para encriptar e decriptar, enquanto o sistema *assimétrico*, ou de *chaves pública e privada*, utiliza *chaves distintas* para codificar e decodificar mensagens[10].

A *criptografia* é a ciência e arte de escrever mensagens de forma cifrada ou codificada, sendo parte de um campo de estudos que abrange as comunicações secretas. Ela é utilizada, entre outras finalidades, para: autenticar a identidade de usuários; autenticar e proteger o sigilo de comunicações pessoais e transações comerciais e bancárias; bem como proteger a integridade de transferências eletrônicas de fundos[11].

Na *criptografia assimétrica*, cada pessoa ou entidade deve manter *duas chaves*: uma *pública*, divulgada livremente, e outra *privada*, mantida em segredo pelo proprietário.

As mensagens codificadas com a chave pública só poderão ser decodificadas com a correspondente chave privada.

---

9 TANENBAUM, Andrew S. **Redes de computadores**. 4. ed. Rio de Janeiro: Campus, 2003. p. 770.

10 VOLPI NETO, Angelo. **Comércio eletrônico**: direito e segurança. Curitiba: Juruá, 2001. p. 58-59.

11 CARTILHA de segurança para internet. **Comitê Gestor da Internet no Brasil**, jun. 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 29 jul. 2020. p. 67.

Por exemplo, José e Maria podem se comunicar de maneira sigilosa seguindo procedimentos específicos:

a) José codifica uma mensagem utilizando a chave pública de Maria, a qual está acessível para qualquer pessoa utilizar;
b) Após criptografada, José envia a mensagem para Maria;
c) Maria recebe e decodifica a mensagem utilizando sua chave privada, mantida exclusivamente em seu conhecimento; e
d) Se Maria desejar responder à mensagem, ela deve seguir o mesmo procedimento, porém utilizando a chave pública de José.

A arte de solucionar mensagens cifradas é chamada de *criptoanálise*, enquanto a *criação* (criptografia) e a *solução* (criptoanálise) de mensagens cifradas formam a *criptologia*[12].

A *função de resumo* é um método criptográfico que, ao ser aplicado a uma informação, independentemente do seu tamanho, gera um resultado único e de tamanho fixo chamado de *hash*. Essa técnica pode ser utilizada para verificar a integridade de arquivos armazenados no computador, como *backups*, ou obtidos por meio da Internet, garantindo que foram transmitidos e armazenados corretamente, além de gerar assinaturas digitais[13].

O *hash* é uma espécie de *impressão digital* do arquivo.

Para verificar a integridade de documentos eletrônicos, pode-se calcular o *hash* do arquivo utilizando métodos como SHA-1, SHA-256 ou MD5. Após a transmissão do arquivo, o receptor recalcula o *hash*: se os valores permanecerem iguais, conclui-se que não houve alteração no documento. Caso contrário, o arquivo pode ter sido corrompido ou modificado[14].

Por exemplo, ao codificar a palavra *criptografia*, o *hash* MD5 resultante é *97c6105c1d97d600ec16ab4abace6d4c* (32 caracteres). Se a palavra for alterada para *criptografar*, o *hash* torna-se *d1b30d6c8440eaa7bd08b3e146dcc674*, indicando claramente a modificação no texto original.

---

12 TANENBAUM, Andrew S. **Redes de computadores**. 4. ed. Rio de Janeiro: Campus, 2003. p. 772.

13 CARTILHA de segurança para internet. **Comitê Gestor da Internet no Brasil**, jun. 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 29 jul. 2020. p. 69.

14 CARTILHA de segurança para internet. **Comitê Gestor da Internet no Brasil**, jun. 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 29 jul. 2020. p. 69.

12.2.2 Assinatura Digital

Assinatura digital é a ferramenta tecnológica que viabiliza a comprovação da *autenticidade* e *integridade* de informações específicas: se foram realmente criadas pelo signatário (a pessoa a quem é atribuída a autoria) e se sofreram alguma alteração[15].

Também conhecida como *assinatura numérica*, baseia-se em chaves criptográficas, com a condição de que apenas o signatário conheça a chave *privada*. Dessa forma, se a mensagem, codificada com essa chave privada, sofrer alguma modificação, ela só pode ter sido realizada pelo signatário. A verificação da assinatura ocorre através da chave *pública*: se o texto foi codificado com a chave privada, apenas a chave pública pode decodificá-lo[16].

Assinatura *eletrônica* não é sinônimo de assinatura *digital*. A assinatura eletrônica é *gênero* da qual a digital é *espécie*. Dessa forma, toda assinatura digital é eletrônica, mas a recíproca não é verdadeira.

É importante ressaltar que assinatura *eletrônica* não é sinônimo de assinatura *digital*; a primeira é um *gênero* do qual a segunda é uma *espécie*. Assim, toda assinatura digital é eletrônica, mas a recíproca não é verdadeira.

Existem várias formas de assinatura eletrônica: senhas, impressões digitais (biometria), *tokens* e escaneamento da assinatura realizada de próprio punho.

Quando um documento (despacho, informação, parecer etc.) é assinado no *Sistema Eletrônico de Informações* (SEI), utilizado por diversos órgãos da Administração Pública, utiliza-se a assinatura eletrônica. Ao final do documento, aparecerá a informação: "Documento assinado eletronicamente por FULANO DE TAL, Diretor de Departamento". O SEI também oferece um mecanismo para verificar a autenticidade do documento assinado, bastando acessar a URL indicada e inserir os códigos verificador e CRC fornecidos.

A assinatura digital, por sua vez, possui características específicas:

a) Necessita obrigatoriamente de um *certificado digital*, emitido por uma Autoridade Certificadora, como detalhado no próximo tópico;
b) Utiliza criptografia para cifrar ou codificar mensagens. É importante destacar que *apenas a assinatura digital é criptografada*, não o conteúdo do documento assinado;

---

15 CARTILHA de segurança para internet. **Comitê Gestor da Internet no Brasil**, jun. 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 29 jul. 2020. p. 69.

16 CARTILHA de segurança para internet. **Comitê Gestor da Internet no Brasil**, jun. 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 29 jul. 2020. p. 69.

c) Garante a comprovação da *autenticidade* (origem do signatário) e *integridade* (caso tenha ocorrido alguma alteração) de informações específicas;

d) Pode incluir informações de data e hora de sua execução (*timestamping* ou carimbo do tempo)[17];

e) Dificilmente haverá assinaturas digitais idênticas, pois estão vinculadas ao conteúdo dos documentos assinados, dependendo de seus *hashes* (resumos criptográficos). Assim, documentos diferentes (com *hashes* distintos) terão, em tese, assinaturas digitais diferentes, mesmo que assinados pelo mesmo signatário. Sobre esse complexo tema, existem estudos especializados sobre *colisão de hashes*, quando são encontradas igualdades nos valores de *hash* de conteúdos diferentes. Se o documento sofrer qualquer modificação, a assinatura digital tornar-se-á inválida;

f) Reveste-se de validade jurídica, equivalendo a uma assinatura de próprio punho.

Exemplificando, caso José queira enviar uma mensagem assinada para Maria, ele a codificará usando sua chave privada. Esse processo resultará na criação de uma assinatura digital, a qual será anexada à mensagem enviada para Maria. Ao recebê-la, Maria utilizará a chave pública de José para decodificar a mensagem, ocasionando a criação de uma segunda assinatura digital, que será então comparada à primeira. Se ambas forem idênticas, Maria terá a certeza de que o remetente da mensagem é de fato José e que a mensagem não foi alterada. Ressalte-se que a segurança desse método se baseia na exclusividade do conhecimento da chave privada pelo seu proprietário.

Conforme mencionado anteriormente, a assinatura digital de uma mensagem não a torna confidencial. No exemplo citado, se José desejar assinar a mensagem e garantir que apenas Maria tenha acesso ao seu conteúdo confidencial, ele deverá codificá-la com a chave pública de Maria após assiná-la.

Em relação à *assinatura eletrônica*, destaca-se a Lei 14.063/2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde.

O art. 2º estabelece regras e procedimentos para o uso de assinaturas eletrônicas, nas interações:

[17] VOLPI NETO, Angelo. **Comércio eletrônico**: direito e segurança. Curitiba: Juruá, 2001. p. 53-54.

a) Internas dos órgãos e entidades da administração direta, autárquica e fundacional dos Poderes e órgãos constitucionalmente autônomos dos entes federativos (inc. I);
b) Entre pessoas naturais ou pessoas jurídicas de direito privado e os entes públicos mencionados no inc. I do *caput* deste artigo (inc. II); e
c) Entre os entes públicos de que trata o inc. I do *caput* deste artigo (inc. III).

No entanto, esse dispositivo não se aplica (parágrafo único):

a) Aos processos judiciais (inc. I);
b) À interação (inc. II) entre pessoas naturais ou entre pessoas jurídicas de direito privado (alínea "a"); na qual seja permitido o anonimato (alínea "b") e na qual seja dispensada a identificação do particular (alínea "c");
c) Aos sistemas de ouvidoria de entes públicos (inc. III);
d) Aos programas de assistência às vítimas e testemunhas ameaçadas (inc. IV); e
e) Às outras hipóteses nas quais deva ser necessário garantir a preservação do sigilo da identidade do particular ao interagir com o ente público (inc. V).

Além disso, o art. 3º conceitua:

a) *Autenticação*: o processo eletrônico que permite a identificação eletrônica de uma pessoa natural ou jurídica (inc. I);
b) *Assinatura eletrônica*: os dados em formato eletrônico que se ligam ou estão logicamente associados a outros dados em formato eletrônico e que são utilizados pelo signatário para assinar, observados os níveis de assinaturas apropriados para os atos previstos nesta Lei (inc. II);
c) *Certificado digital*: atestado eletrônico que associa os dados de validação da assinatura eletrônica a uma pessoa natural ou jurídica (inc. III); e
d) *Certificado digital ICP-Brasil*: certificado digital emitido por uma Autoridade Certificadora (AC) credenciada na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), conforme a legislação vigente (inc. IV).

Trata-se de interpretação *autêntica* destes quatro conceitos: conforme a intenção do legislador de como a lei deveria ser interpretada.

No art. 4º, a mencionada lei *classifica* as assinaturas eletrônicas da seguinte forma:

a) *Assinatura eletrônica simples* (inc. I): aquela que permite identificar o signatário (alínea "a") e que anexa ou associa dados a outros dados em formato eletrônico do signatário (alínea "b");
b) *Assinatura eletrônica avançada* (inc. II): a que utiliza certificados não emitidos pela ICP-Brasil ou outro meio de comprovação da autoria e integridade de documentos em formato eletrônico, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento. Possui as seguintes características: está associada ao signatário de maneira unívoca (alínea "a"); utiliza dados para a criação de assinatura eletrônica cujo signatário pode operar sob seu controle exclusivo com elevado nível de confiança (alínea "b") e está relacionada aos dados a ela associados de tal modo que qualquer modificação posterior é detectável (alínea "c"); e
c) *Assinatura eletrônica qualificada* (inc. III): a que utiliza certificado digital, nos termos do § 1º do art. 10 da Medida Provisória 2.200-2/2001.

As assinaturas eletrônicas simples, avançada e qualificada caracterizam o nível de confiança sobre a identidade e a manifestação de vontade de seu titular, sendo a assinatura eletrônica *qualificada* aquela com o *nível mais elevado de confiabilidade*, conforme suas normas, padrões e procedimentos específicos.

O Decreto 10.543, de 13.11.2020, dispõe sobre o uso de assinaturas eletrônicas na Administração Pública Federal e regulamenta o art. 5º, Lei 14.063/2020, quanto ao nível mínimo exigido para a assinatura eletrônica em interações com o Ente Público.

A Lei 14.063/2020 contempla situações especiais, disciplinando atos praticados por particulares perante Entes Públicos (art. 8º), atos realizados em situações decorrentes da pandemia da Covid-19 (art. 10) e da assinatura eletrônica em questões envolvendo saúde pública (arts. 13 a 15).

A Lei 14.620/2023 alterou o art. 784 do CPC/2015, incluindo o § 4º:

§ 4º Nos títulos executivos constituídos ou atestados por meio eletrônico, é admitida qualquer modalidade de assinatura eletrônica prevista em lei, dispensada a assinatura de testemunhas quando sua integridade for conferida por provedor de assinatura.

Essa modificação trata do reconhecimento, já estabelecido em decisões de tribunais brasileiros, dos contratos constituídos ou assinados por meios eletrônicos como títulos executivos extrajudiciais.

12.2.3 Certificado Digital e a ICP-Brasil

Outros termos da linguagem técnica que ganham cada vez mais relevância no cotidiano jurídico: *certificado digital* e *Autoridade Certificadora*.

A *Autoridade Certificadora* ou *Agente Certificador* é responsável por atestar a validade de determinado ato, associando a chave pública à pessoa identificada como proprietária das chaves. A emissão de certificados é uma atribuição da Autoridade Certificadora, que utiliza uma base de dados mantida de forma segura, protegida contra alterações, intencionais ou não. Em razão dessa responsabilidade, o Agente Certificador é frequentemente comparado a um *tabelião virtual*[18].

Exemplos de Autoridade Certificadora: *Serasa Experian* e *CertiSign*.

A *Infraestrutura de Chaves Públicas Brasileira* (ICP-Brasil) é uma cadeia hierárquica de confiança que possibilita a emissão de certificados digitais para a identificação virtual do cidadão[19].

A criação da ICP-Brasil foi estabelecida pela Medida Provisória 2.200-2/2001, publicada em 27.08.2001, a qual transformou o *Instituto Nacional de Tecnologia da Informação* em uma autarquia, conforme previsto no art. 12.

> **Art. 1º.** Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.
>
> **Art. 12.** Fica transformado em autarquia federal, vinculada ao Ministério da Ciência e Tecnologia, o Instituto Nacional de Tecnologia da Informação – ITI, com sede e foro no Distrito Federal.

Nos termos do art. 2º da mencionada Medida Provisória, a ICP-Brasil organiza-se da seguinte forma[20]:

---

18 MATTE, Mauricio. **Internet – comércio eletrônico**: aplicabilidade do código de defesa do consumidor nos contratos de e-commerce. São Paulo: LTr, 2001. p. 39.

19 ICP-Brasil. **Instituto Nacional de Tecnologia da Informação**. Disponível em: <https://www.gov.br/iti/pt-br/assuntos/icp-brasil>. Acesso em: 26 ago. 2020.

20 ENTES da ICP-Brasil. **Instituto Nacional de Tecnologia da Informação**. Disponível em: <https://www.gov.br/iti/pt-br/assuntos/icp-brasil/entes-da-icp-brasil>. Acesso em: 26 ago. 2020.

a) *Autoridade Certificadora Raiz (AC-Raiz)*: é a primeira autoridade da cadeia de certificação. O *Instituto Nacional de Tecnologia da Informação* (ITI), de acordo com o art. 13, MP 2200-2/2001, é a Autoridade Certificadora Raiz da ICP-Brasil. Essa entidade credencia, audita e fiscaliza as demais entidades da ICP-Brasil. A AC-Raiz assina seu próprio certificado, bem como os certificados das Autoridades Certificadoras imediatamente abaixo dela. Ela também possui a competência de emitir, expedir, distribuir, revogar e gerenciar os certificados das Autoridades Certificadoras de nível imediatamente subsequente ao seu. Além disso, é responsável por emitir a *Lista de Certificados Revogados* (LCR) e por fiscalizar e auditar as *Autoridades Certificadoras* (AC), *Autoridades de Registro* (AR) e demais prestadores de serviço habilitados na ICP-Brasil. A AC-Raiz verifica se as Autoridades Certificadoras atuam em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil;

b) *Autoridades Certificadoras (AC)*: são entidades públicas ou privadas subordinadas à hierarquia da ICP-Brasil, responsáveis por emitir, distribuir, renovar, revogar e gerenciar certificados digitais. Essas entidades têm a responsabilidade de verificar se o titular do certificado possui a chave privada correspondente à chave pública contida no certificado. Elas criam e assinam digitalmente o certificado do assinante, representando a declaração da identidade do titular, que detém um par único de chaves (pública/privada). As ACs também emitem e publicam a *Lista de Certificados Revogados* (LCR). Na estrutura de Carimbo do Tempo (*timestamping*) da ICP-Brasil, emitem os certificados digitais utilizados nos equipamentos e sistemas das *Autoridades de Carimbo do Tempo* (ACT) e da *Entidade de Auditoria do Tempo* (EAT). Existem Autoridades Certificadoras de 1º (AC 1) e 2º níveis (AC 2), dependendo da hierarquia;

c) *Autoridade de Registro (AR)*: é uma entidade responsável pela interface entre o usuário e a Autoridade Certificadora. Vinculada a uma AC, tem por objetivo receber, validar e encaminhar solicitações de emissão ou revogação de certificados digitais às ACs, além de identificar, de forma presencial, os solicitantes. A AR também é responsável por manter registros de suas operações e pode estar fisicamente localizada em uma AC ou ser uma entidade de registro remota.

GLOSSÁRIO. **Instituto Nacional de Tecnologia da Informação**. Disponível em: <https://www.gov.br/iti/pt-br/centrais-de-conteudo/glossario>. Acesso em: 26 ago. 2020.

Essa organização hierárquica é conhecida como *cadeia de certificados*.

O *Comitê Gestor da ICP-Brasil* tem a função primordial de coordenar o funcionamento da infraestrutura, conforme originalmente elencado no art. 4º, MP 2.200-2/2001 e regulamentado pelo art. 3º, Decreto 6.605/2008:

> **Art. 3º.** Compete ao CG da ICP-Brasil:
>
> I – coordenar o funcionamento da ICP-Brasil;
>
> II – estabelecer a política, os critérios e as normas técnicas para o credenciamento das Autoridades Certificadoras – AC, Autoridades de Registro – AR, Autoridades de Carimbo de Tempo – ACT e demais prestadores de serviço de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;
>
> III – estabelecer a política de certificação e as regras operacionais da AC Raiz;
>
> IV – auditar e fiscalizar a AC Raiz e os seus prestadores de serviço de suporte;
>
> V – estabelecer diretrizes e normas técnicas para a formulação de políticas de certificado e regras operacionais das AC, AR e ACT e definir níveis da cadeia de certificação;
>
> VI – aprovar políticas de certificados e regras operacionais, credenciar e autorizar o funcionamento das AC, das AR, das ACT e demais prestadores de serviço de suporte, bem como autorizar a AC Raiz a emitir o correspondente certificado;
>
> VII – identificar e avaliar as políticas de infra-estruturas de certificação externas, negociar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional, certificar, quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais.
>
> VIII – aprovar as normas para homologação de sistemas e equipamentos de certificação digital no âmbito da ICP-Brasil;
>
> IX – atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, de modo a garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança; e
>
> X – aprovar seu regimento interno.

O *certificado digital* é considerado um *produto*, não um serviço, sendo intangível por sua natureza eletrônica: um *software* personalíssimo. Não é um produto genérico, pois, durante sua emissão, são verificadas características pessoais dos adquirentes, como nome completo e data de nascimento.

Funciona como uma *identidade virtual*, possibilitando a identificação segura e inequívoca do autor de uma mensagem ou transação realizada em ambientes eletrônicos, como na Internet[21].

Dessa forma, o *certificado* ou *certidão digital* é um arquivo de computador que serve para identificar o usuário. Alguns *softwares* aplicativos utilizam esse arquivo para comprovar a identidade do usuário para outras pessoas ou computadores. Normalmente, um certificado digital contém informações como a chave pública do autor, nome e endereço de correio eletrônico do autor, data de validade da chave pública, nome da empresa (a Autoridade Certificadora) que emitiu o certificado digital, número de série do certificado digital e a assinatura digital da Autoridade Certificadora[22].

Pode-se afirmar que um certificado digital possui três finalidades básicas:

a) *Autenticação*: identifica o usuário do documento eletrônico certificado;
b) *Cifragem*: responsável pelo sigilo da informação; e
c) *Assinatura digital*: possibilita ao usuário assinar eletronicamente os documentos[23].

Na ICP-Brasil, estão previstos 12 tipos de certificados digitais, sendo 8 relacionados à *assinatura digital* (A1, A2, A3, A4, T3, T4, A CF-e-SAT e OM-BR) e 4 associados ao *sigilo* (S1, S2, S3 e S4). Os certificados do *Tipo A*, mais comuns, têm como principal benefício a realização de assinaturas digitais, identificando o titular, atestando a autenticidade da operação e confirmando a integridade do documento assinado. Já os certificados de *sigilo* do *Tipo S* garantem confidencialidade às transações eletrônicas[24].

Os certificados de *tempo*, conhecidos como *Tipo T* (também chamados de *Carimbo do Tempo* ou *timestamping*), atuam como um "selo", certificando a existência de um documento eletrônico ou de uma assinatura digital em um determinado momento (data e hora). Os certificados *Tipo A CF-e-SAT* só podem ser emitidos para equipamentos integrantes do *Sistema de Autenticação e Transmissão do Cupom Fiscal Eletrônico* (SAT-CF-e), conforme regulamentação do *Conselho Nacional de Política Fazendária* (Confaz). Por fim, os

---

21 CERTIFICADO digital. **Instituto Nacional de Tecnologia da Informação**. Disponível em: <https://www.gov.br/iti/pt-br/assuntos/certificado-digital>. Acesso em: 26 ago. 2020.

22 PERGUNTAS frequentes. **CertiSign**. Disponível em: <https://www.certisign.com.br/duvidas-suporte/perguntas-frequentes/certificado-digital>. Acesso em: 26 ago. 2020.

23 RODRIGUES, Rendrik Vieira. Segurança jurídica do documento eletrônico. **Justilex**, Brasília, a. 3, n. 26, p. 34, fev. 2004.

24 QUAIS são os tipos de certificados digitais que existem? CertiSign, 19 dez. 2019. Disponível em: <https://blog.certisign.com.br/tipo-de-certificado-digital/>. Acesso em: 26 ago. 2020.

certificados *Tipo OM-BR* (Objeto Metrológico) são emitidos exclusivamente para equipamentos metrológicos regulados pelo Inmetro[25].

Entre os certificados mais comuns, destacam-se o A1 e o A3[26]:

a) *A1*: são emitidos diretamente no computador, permitindo a realização de cópias de segurança e a subsequente instalação em outros computadores; e

b) *A3*: podem ser armazenados em dispositivos criptográficos: cartão inteligente (*SmartCard*) – que requer uma unidade leitora – *token* e na nuvem, oferecendo mobilidade.

É importante ressaltar que somente os documentos eletrônicos assinados com certificados da ICP-Brasil possuem *validade jurídica* (presunção *juris tantum*), conforme garantido pela mencionada Medida Provisória.

A Lei 11.419/2006, que trata da informatização do processo judicial, confirma essa validade em seu art. 1º, § 2º, inc. III, alínea "a":

> **Art. 1º.** O uso de meio eletrônico na tramitação de processos judiciais, comunicação de atos e transmissão de peças processuais será admitido nos termos desta Lei. [...]
>
> § 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;

Exemplo: A Secretaria da Receita Federal disponibiliza aos contribuintes brasileiros, por meio dos certificados digitais *e-CNPJ* (identidade digital da Pessoa Jurídica no meio eletrônico) e *e-CPF* (identidade digital da Pessoa Física no meio eletrônico), o acesso a diversos de seus serviços.

Entretanto, é relevante mencionar que, conforme decisão proferida pelo TJDFT[27], o TJSP validou uma assinatura digital certificada por uma autoridade não credenciada à ICP-Brasil. Isso se deu devido à inexistência de elementos que, a princípio, suscitassem dúvidas sobre a autenticidade da assinatura. A Medida Provisória 2.200-2/2001, que regulamenta a emissão

---

25 QUAIS são os tipos de certificados digitais que existem? CertiSign, 19 dez. 2019. Disponível em: <https://blog.certisign.com.br/tipo-de-certificado-digital/>. Acesso em: 26 ago. 2020.

26 QUAIS são os tipos de certificados digitais que existem? **CertiSign**, 19 dez. 2019. Disponível em: <https://blog.certisign.com.br/tipo-de-certificado-digital/>. Acesso em: 26 ago. 2020.

27 TJDFT, 5ª TC, AC 0722309-67.2021.8.07.0001, Rel. Des. Josaphá Francisco dos Santos, publ. 20.10.2021.

de documentos eletrônicos, não impede a utilização de outros meios de comprovação da autoria e integridade de documentos em formato eletrônico, inclusive aqueles que fazem uso de certificados não emitidos pela ICP-Brasil, desde que aceitos pelas partes ou pela pessoa a quem o documento for apresentado[28]. Outro exemplo: AI 2095200-63.2024.8.26.0000 (TJSP, 20ª CDPriv, Rel. Des. Luis Carlos de Barros, publ. 29.04.2024).

Além disso, existem certificados digitais específicos destinados à emissão de notas fiscais eletrônicas (NF-e e NFC-e)[29].

12.3 APLICAÇÕES DE DOCUMENTOS ELETRÔNICOS

Diariamente, milhões de documentos eletrônicos são manipulados em todo o mundo, desempenhando diversas funções, como edição e impressão. No entanto, em sua grande maioria, esses documentos carecem das características fundamentais de confiabilidade e integridade de conteúdo.

A crescente popularização das ferramentas de tecnologia da informação tem destacado a importância da utilização de *documentos eletrônicos seguros*.

Esses projetos, muitas vezes de custo elevado, demandam uma constante preocupação com a segurança, um elemento fundamental para o sucesso de tais aplicações. Elementos como salas-cofre, dispositivos de armazenamento seguro, sistemas gerenciadores de bancos de dados e tecnologias para instrumentalização dos usuários, como computadores e dispositivos portáteis para geração e armazenamento de certificados digitais, conhecidos como *tokens*, são essenciais nesse contexto.

No âmbito do Poder Judiciário, além dos sistemas processuais eletrônicos como *eProc*, *Projudi*, *PJe*, entre outros, destacam-se diversos serviços baseados em tecnologia da informação que envolvem documentos eletrônicos: protocolo eletrônico (TJPE), Juizado Virtual (JFRN), certidões negativas via Internet (JFES), pauta eletrônica de audiências (JFPR), projeto de petição pela Internet (TRTSP), sistema de penhora *on-line* (TST), trâmite eletrônico para seis classes processuais de sua competência (STF), projeto de mandados judiciais eletrônicos (TJDFT), sistema de mandado de prisão *on-line* (TJMT), virtualização de todos os Juizados (TJRN), leilão eletrônico (TJMS) e expansão do sistema de alvará eletrônico (TJMG)[30].

---

28 TJSP, 24ª CDPriv, AI 2251832-25.2021.8.26.0000, Rel. Des. Plinio Novaes de Andrade Júnior, publ. 30.03.2022.

29 DÚVIDAS – certificado digital. **CertiSign**. Disponível em: <https://www.certisign.com.br/duvidas-suporte/perguntas-frequentes/certificado-digital>. Acesso em: 26 ago. 2020.

30 KAMINSKI, Omar. Tecnologia impulsionou acesso à informação jurídica. **Consultor Jurídico**, 16 dez. 2005. Disponível em: <https://www.conjur.com.br/2005-dez-16/tecnologia_impulsionou_acesso_informacao_juridica>. Acesso em: 28 jul. 2020.

Um exemplo de aplicação bem-sucedida de documento eletrônico, ferramentas de certificação digital e assinatura digital é o *Cartório 24 Horas*, lançado no final de 2003. Criada pela *Associação Brasileira dos Notários e Registradores* (Anoreg-BR), a *Rede Brasileira de Cartórios* (RBC) possibilita a obtenção de certidões de todas as naturezas, visando aprimorar, integrar e agilizar os serviços prestados à comunidade brasileira[31].

A celebração de contratos *on-line* é uma aplicação cada vez mais comum para o documento eletrônico, apesar dos desafios relacionados à contratação entre pessoas fisicamente ausentes e à segurança das plataformas de comércio eletrônico[32].

12.4 O DOCUMENTO ELETRÔNICO COMO MEIO DE PROVA

Com a introdução dos documentos eletrônicos, surgiu a questão sobre se poderiam receber o mesmo tratamento concedido aos documentos jurídicos.

A doutrina destaca a autoria identificável (*autenticidade*) e a impossibilidade de alteração de forma imperceptível (*integridade*) como requisitos fundamentais para que o documento eletrônico adquira validade probatória[33].

As disposições atualmente vigentes na legislação permitem, de forma genérica, a comprovação dos atos jurídicos por meio de quaisquer meios legais ou moralmente legítimos, desde que sejam idôneos[34].

O CPC/2015 estabelece:

> **Art. 369.** As partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz.

Conforme estipulado pelo § 2º do art. 11, Lei 11.419/2006, os *documentos digitalizados*, isto é, aqueles que inicialmente possuíam suporte físico e foram

---

31 NOVOS serviços chegam aos cartórios do Tocantins. **Associação dos Notários e Registradores do Brasil**. Disponível em: <https://www.anoreg.org.br/site/2007/10/24/imported_9830/>. Acesso em: 26 ago. 2020.

32 LORENZETTI, Ricardo Luis. Informática, cyberlaw, e-commerce. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coords.). **Direito & internet**. São Paulo: Edipro, 2001. p. 432.

33 MARCACINI, Augusto Tavares Rosa. **O documento eletrônico como meio de prova**. Disponível em: <http://augustomarcacini.net/index.php/DireitoInformatica/DocumentoEletronico>. Acesso em: 25 ago. 2020.

34 DOS SANTOS, Manoel J. Pereira. Contratos eletrônicos. In: ROVER, Aires José (Org.). **Direito, sociedade e informática**: limites e perspectivas da vida digital. Florianópolis: Fundação Boiteux, 2000, p. 196.

posteriormente convertidos em documentos eletrônicos, possuem a *mesma força probante* dos originais físicos e dos documentos com assinatura digital gerados eletronicamente[35].

> **Art. 11.** Os documentos produzidos eletronicamente e juntados aos processos eletrônicos com garantia da origem e de seu signatário, na forma estabelecida nesta Lei, serão considerados originais para todos os efeitos legais. [...]
>
> § 2º A arguição de falsidade do documento original será processada eletronicamente na forma da lei processual em vigor.

Além disso, *somente os documentos eletrônicos assinados com certificados da ICP-Brasil* têm sua validade jurídica assegurada pela Medida Provisória 2.200-2/2001, conforme explicado no item 12.2.3.

A respeito, destacam-se os seguintes julgados de nossos Tribunais:

- *STJ, Corte Especial*: SEC 8.810, publ. 16.10.2013;
- *STJ, 1ª Turma*: AgInt-AREsp 1.311.006, publ. 05.02.2019;
- *STJ, 3ª Turma*: REsp 1.495.920, publ. 07.06.2018 e AgInt-AREsp 1.162.825, publ. 30.04.2018;
- *STJ, 6ª Turma*: RHC 81.451, publ. 31.08.2017; e
- *TRF3, 6ª Turma*: ACRN 0013588-10.2008.4.03.6100, publ. 09.05.2014.

12.5 A QUESTÃO CRIMINAL

Em novembro de 2022, o Tribunal Regional do Trabalho da 1ª Região (TRT-RJ) identificou uma fraude envolvendo 17 certificados digitais e alvarás falsos, totalizando mais de R$ 4 milhões. Esses alvarás beneficiaram uma pessoa jurídica não relacionada ao processo em questão, registrada recentemente na Receita Federal. A fraude utilizou o certificado digital da Juíza titular da 80ª Vara do Trabalho da Capital, resultando na suspensão dos pagamentos de alvarás em todos os Tribunais do Trabalho do país como medida preventiva. Diversos órgãos colaboraram na investigação, e a *Autoridade Nacional de Proteção de Dados* (ANPD) comprometeu-se a realizar uma reunião urgente com os responsáveis pela emissão dos certificados digitais utilizados na fraude[36].

---

35 STJ, Corte Especial, SEC 8.810, Rel. Min. Humberto Martins, publ. 16.10.2013.

36 FUCCIA, Eduardo Velozo. Fraudes em alvarás no TRT-1 superam R$ 4 mi e sistema de pagamento é suspenso. **Consultor Jurídico**, 13 nov. 2022. Disponível em: < https://www.conjur.com.br/2022-nov-13/fraudes-emissao-alvaras-trt-ultrapassam-milhoes>. Acesso em: 6 set. 2023.