REGULAMENTO DE EXECUÇÃO (UE) 2025/1550 DA COMISSÃO

de 28 de julho de 2025

que estabelece as especificações técnicas e outros requisitos para o sistema informático descentralizado referido no Regulamento (UE) 2023/1543 do Parlamento Europeu e do Conselho

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta o Regulamento (UE) 2023/1543 do Parlamento Europeu e do Conselho, de 12 de julho de 2023, relativo às ordens europeias de produção e às ordens europeias de conservação para efeitos de prova eletrónica em processos penais e para efeitos de execução de penas privativas de liberdade na sequência de processos penais ([1]), nomeadamente o artigo 25.º, n.º 1, alíneas a), b), c) e d),

Considerando o seguinte:

(1) De modo a criar o sistema informático descentralizado referido no Regulamento (UE) 2023/1543, é necessário definir e adotar especificações técnicas, medidas e objetivos para a implementação desse sistema.

(2) Nos termos do Regulamento (UE) 2023/1543, o sistema informático descentralizado deve incluir os sistemas informáticos dos Estados-Membros e das agências e organismos pertinentes da União e os pontos de acesso e-CODEX interoperáveis através dos quais esses sistemas informáticos estão interligados. Por conseguinte, as especificações técnicas e outros requisitos do sistema informático descentralizado devem refletir este enquadramento.

(3) De acordo com o Regulamento (UE) 2023/1543, os pontos de acesso do sistema informático descentralizado devem basear-se em pontos de acesso e-CODEX autorizados, conforme definido no artigo 3.º, n.º 3, do Regulamento (UE) 2022/850 do Parlamento Europeu e do Conselho ([2]).

(4) Os Estados-Membros podem optar por utilizar a aplicação informática de referência desenvolvida pela Comissão como sistema de retaguarda em vez de um sistema informático nacional. De modo a assegurar a interoperabilidade, tanto os sistemas informáticos nacionais como a aplicação informática de referência devem estar sujeitos às mesmas especificações técnicas e requisitos estabelecidos no presente regulamento.

(5) A fim de atenuar eventuais problemas técnicos relacionados com a capacidade e a fiabilidade do sistema informático descentralizado, é necessário estabelecer um limiar para o volume de provas eletrónicas transmitidas através deste sistema. Após o lançamento do sistema, a frequência e o volume das transmissões devem ser monitorizados, procedendo-se ao ajustamento do limiar, se necessário, com vista a maximizar a eficiência do sistema.

(6) A fim de reforçar a interoperabilidade e a eficácia do sistema informático descentralizado, deve ser obrigatória a utilização de normas ETSI adequadas. A evolução futura deve ser acompanhada e, se necessário, deve ser considerada a adoção de normas ETSI adicionais.

(7) A Irlanda está vinculada pelo Regulamento (UE) 2023/1543, pelo que participa na adoção do presente regulamento.

(8) Nos termos dos artigos 1.º e 2.º do Protocolo n.º 22 relativo à posição da Dinamarca, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União Europeia, a Dinamarca não fica vinculada nem sujeita à aplicação do presente regulamento.

([1]) JO L 191 de 28.7.2023, p. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj.

([2]) Regulamento (UE) 2022/850 do Parlamento Europeu e do Conselho, de 30 de maio de 2022, relativo a um sistema informatizado de intercâmbio eletrónico transfronteiriço de dados no domínio da cooperação judiciária em matéria civil e penal (sistema e-CODEX) e que altera o Regulamento (UE) 2018/1726 (JO L 150 de 1.6.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/850/oj).

(9) A Autoridade Europeia para a Proteção de Dados foi consultada em conformidade com o disposto no artigo 42.º, n.º 1, do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho [3] e emitiu um parecer em 25 de junho de 2025.

(10) As medidas previstas no presente regulamento estão em conformidade com o parecer do comité instituído pelo artigo 26.º do Regulamento (UE) 2023/1543,

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

Especificações técnicas do sistema informático descentralizado

As especificações técnicas, os requisitos, as medidas e os objetivos do sistema informático descentralizado referidos no artigo 25.º, n.º 1, do Regulamento (UE) 2023/1543 para a comunicação, na aceção do artigo 19.º do mesmo, são os estabelecidos no anexo do presente regulamento.

Artigo 2.º

Entrada em vigor

O presente regulamento entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável nos Estados-Membros, em conformidade com os Tratados.

Feito em Bruxelas, em 28 de julho de 2025.

Pela Comissão
A Presidente
Ursula VON DER LEYEN

[3] Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (JO L 295 de 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

ANEXO

ESPECIFICAÇÕES TÉCNICAS DO SISTEMA INFORMÁTICO DESCENTRALIZADO

(a que se refere o artigo 1.º)

1. Introdução e âmbito de aplicação

O presente anexo estabelece as especificações técnicas, as medidas e os objetivos do sistema informático descentralizado relativamente aos procedimentos previstos no Regulamento (UE) 2023/1543.

Nos termos do Regulamento (UE) 2023/1543, nomeadamente do artigo 19.º, o sistema informático descentralizado deve permitir a comunicação escrita entre as autoridades competentes e os estabelecimentos designados ou os representantes legais, entre as autoridades competentes, e entre as autoridades competentes e as agências ou organismos competentes da União.

2. Definições

2.1. «Protocolo seguro de transferência de hipertexto» ou «HTTPS»: canais de comunicação cifrada e de conexão segura;

2.2. «Não repúdio da origem»: medidas que fornecem a prova da integridade e a prova da origem dos dados através de métodos como a certificação digital, a infraestrutura de chave pública, as assinaturas eletrónicas e os selos eletrónicos;

2.3. «Não repúdio da receção»: medidas que fornecem a prova ao emitente de que os dados foram recebidos pelo destinatário previsto através de métodos como a certificação digital, a infraestrutura de chave pública, as assinaturas eletrónicas e os selos eletrónicos;

2.4. «SOAP»: de acordo com as normas do Consórcio World Wide Web, especificação de protocolo de transmissão de mensagens para o intercâmbio de informações estruturadas na execução dos serviços Web nas redes informáticas;

2.5. «Transferência de estado representacional ("REST")»: arquitetura para a conceção de aplicações em rede, com base num modelo de comunicação apátrida e cliente-servidor e utilizando métodos normalizados para realizar operações sobre recursos, que, por norma, são representados em formatos estruturados;

2.6. «Serviço Web»: sistema de programas informáticos concebido para suportar a interoperabilidade de equipamentos em rede e que possui uma interface descrita em formato processável por máquina;

2.7. «Intercâmbio de dados»: troca de mensagens, formulários, documentos e provas eletrónicas através do sistema informático descentralizado;

2.8. «API»: interface de programação de aplicações baseada numa norma comum de intercâmbio de dados, que permite aos prestadores de serviços que utilizam soluções informáticas concebidas especificamente para efeitos do intercâmbio de informações e dados relacionados com pedidos de provas eletrónicas aceder aos sistemas informáticos descentralizados por meios automatizados;

2.9. «Interface em linha»: interface de utilizador, disponível através do HTTPS na Internet, que permite aos prestadores de serviços aceder ao sistema informático descentralizado manualmente para comunicar de forma segura com as autoridades e proceder ao intercâmbio de informações e dados relacionados com pedidos de provas eletrónicas, sem terem de criar a sua própria infraestrutura específica;

2.10. «Normas ETSI»: especificações e normas técnicas desenvolvidas pelo Instituto Europeu de Normalização das Telecomunicações (ETSI) para garantir a interoperabilidade, a segurança e a eficiência das tecnologias da informação e da comunicação. Proporcionam quadros, protocolos e boas práticas para um amplo conjunto de tecnologias, incluindo redes móveis, radiocomunicações, cibersegurança e infraestrutura de Internet;

2.11. «Valor de dispersão»: saída de tamanho fixo gerada por uma função criptográfica de dispersão quando aplicada a uma entrada de tamanho arbitrário. É concebida uma função criptográfica de dispersão para satisfazer propriedades de segurança fundamentais, nomeadamente a resistência à pré-imagem, a resistência à segunda pré-imagem e a resistência à colisão, assegurando a sua robustez contra ataques de inversão e de colisão;

2.12. «Sistema e-CODEX»: o sistema e-CODEX definido no artigo 3.º, n.º 1, do Regulamento (UE) 2022/850;

2.13. «Vocabulário de Base da Justiça Eletrónica da UE»: o vocabulário de base da justiça eletrónica da UE, conforme definido no ponto 4 do anexo do Regulamento (UE) 2022/850;

2.14. «ebMS»: serviço de mensagens ebXML, que consiste num protocolo de transmissão de mensagens desenvolvido no âmbito do quadro normativo OASIS que permite o intercâmbio seguro, fiável e interoperável de documentos operacionais eletrónicos através do SOAP, apoiando a integração entre empresas em diversos sistemas;

2.15. «AS4»: Declaração de Aplicabilidade 4, uma norma OASIS que define o perfil ebMS 3.0; simplifica a transmissão de mensagens entre empresas de forma segura e a interoperabilidade através da utilização de normas abertas, como o SOAP e a WS-Security;

2.16. «Objetivo de tempo de recuperação»: tempo máximo admissível para o restabelecimento do serviço após um incidente;

2.17. «Objetivo de ponto de recuperação»: quantidade máxima aceitável de perda de dados em caso de falha.

3. **Métodos de comunicação por via eletrónica**

3.1. Para efeitos de comunicação escrita entre as autoridades competentes dos Estados-Membros, entre as autoridades competentes e os estabelecimentos designados ou os representantes legais de prestadores de serviços e entre as autoridades competentes e as agências ou organismos competentes da União, o sistema informático descentralizado utiliza métodos de comunicação assentes em serviços, como os serviços Web ou outros componentes e soluções de *software* reutilizáveis para efeitos de intercâmbio de dados. Especificamente, envolve a comunicação através de pontos de acesso e-CODEX, conforme estabelecido no artigo 5.º, n.º 2, do Regulamento (UE) 2022/850. Por conseguinte, de modo a assegurar um intercâmbio de dados transfronteiriço eficaz e interoperável, o sistema informático descentralizado deve apoiar a comunicação através do sistema e-CODEX.

3.2. Tendo em conta o elevado volume previsto de provas eletrónicas a transmitir através do sistema informático descentralizado na sequência de uma ordem europeia de produção, conforme previsto no artigo 19.º, n.ºs 1 e 4, do Regulamento (UE) 2023/1543, o que pode resultar em limitações de capacidade técnica com impacto negativo no sistema informático descentralizado, as provas eletrónicas devem ser transmitidas através deste sistema, na medida em que não excedam o limiar de 25 megabytes (25 600 kilobytes). A transmissão de provas eletrónicas que excedam esse limiar deve ser efetuada nos termos do artigo 19.º, n.º 5, do referido regulamento.

3.3. Tendo em conta o artigo 19.º, n.º 6, do Regulamento (UE) 2023/1543, se a transmissão for efetuada por meios alternativos, conforme previsto nesse número, devido à incapacidade de utilizar o sistema informático descentralizado, por um dos motivos previstos no artigo 19.º, n.º 5, do mesmo regulamento:

3.3.1. Se a transmissão disser respeito à comunicação escrita, incluindo o intercâmbio de formulários, entre as autoridades competentes e os prestadores de serviços na aceção do artigo 19.º, n.º 1, do Regulamento (UE) 2023/1543, a entidade que iniciou a transmissão deve registar a transmissão no seu sistema informático nacional que faz parte do sistema informático descentralizado. As informações registadas devem incluir, no mínimo, um número de referência do processo ou do ficheiro, a data e hora da transmissão, o remetente e o destinatário, o nome do ficheiro e a sua dimensão.

3.3.2. Se a transmissão disser respeito à comunicação escrita, incluindo o intercâmbio de formulários, entre as autoridades competentes, bem como à comunicação escrita com agências ou organismos competentes da União, na aceção do artigo 19.º, n.º 4, do Regulamento (UE) 2023/1543, a entidade que iniciou a transmissão deve registar a transmissão no sistema informático descentralizado, nomeadamente no seu sistema informático nacional ou, se for caso disso, nos sistemas informáticos geridos pela agência ou organismo competente da União. As informações registadas devem incluir, no mínimo, um número de referência do processo ou do ficheiro, a data e hora da transmissão, o remetente e o destinatário, o nome do ficheiro e a sua dimensão.

3.3.3. Quando as provas eletrónicas ao abrigo de uma ordem europeia de produção tiverem sido transmitidas através de meios alternativos de comunicação entre os prestadores de serviços e as autoridades competentes no Estado de emissão ([1]) ou quando as provas eletrónicas sejam transmitidas através de meios alternativos pela autoridade de execução às autoridades competentes no Estado de emissão ao abrigo do procedimento de execução previsto no artigo 16.º, n.º 9, do Regulamento (UE) 2023/1543, o emitente:

a) Deve registar e transmitir à autoridade à qual as provas eletrónicas foram transmitidas ou disponibilizadas as seguintes informações como parte de um manifesto:

1) informações sobre o remetente e o destinatário,

2) metadados que associem as provas eletrónicas fornecidas a uma ou mais ordens europeias específicas de produção ou de conservação,

3) a data e a hora da transmissão ou a indicação do momento em que as provas eletrónicas foram disponibilizadas ao destinatário,

4) informações relativas aos meios de transmissão (por exemplo, um registo da ligação segura através da qual as provas eletrónicas foram disponibilizadas, um comprovativo de receção ou de entrega dos serviços postais, etc. ([2])),

5) o(s) nome(s) completo(s) do(s) ficheiro(s) das provas eletrónicas transmitidas ou de outro modo disponibilizadas ao destinatário previsto no Estado de emissão,

6) a dimensão dos dados das provas eletrónicas transmitidas ou de outro modo disponibilizadas ao destinatário previsto no Estado de emissão,

7) pelo menos, um valor de dispersão dos dados transmitidos ou disponibilizados e uma indicação do(s) algoritmo(s) de dispersão utilizado(s). O(s) algoritmo(s) de dispersão utilizado(s) para calcular esse(s) valor(es) de dispersão deve(m) ser criptograficamente robusto(s), de utilização corrente, e não sujeito(s) a vulnerabilidades divulgadas publicamente, como colisões (por exemplo, SHA-512, SHA3-512, BLAKE2 ou RIPEMD-160, mas possivelmente mais forte, dependendo da evolução tecnológica);

b) Consoante aplicável, deve indicar, como parte do manifesto referido na alínea a) *supra*, a data e a hora até às quais as provas eletrónicas permanecerão acessíveis. Este período fornece à autoridade competente no Estado de emissão um prazo razoável para a obtenção das provas eletrónicas, que não pode ser inferior a 10 dias de calendário nem superior a 45 dias de calendário, a contar do momento em que as provas eletrónicas são disponibilizadas. A pedido da autoridade competente do Estado de emissão, o período indicado pelo emitente pode ser prorrogado num caso concreto;

c) Pode registar e transmitir quaisquer informações ou observações adicionais relevantes para o processo à autoridade à qual as provas eletrónicas foram transmitidas ou disponibilizadas, como parte do manifesto referido na alínea a) *supra*.

3.4. Tendo em conta o artigo 28.º do Regulamento (UE) 2023/1543, a aplicação informática de referência deve recolher, transmitir ou, de outro modo, facultar o acesso, através de programas, às estatísticas referidas no n.º 2 desse artigo, tanto em formatos de dados estruturados (por exemplo, XML) como não estruturados (por exemplo, PDF). Em conformidade com o artigo 28.º, n.º 3, do Regulamento (UE) 2023/1543, quando tecnicamente equipados, os portais nacionais ([3]) operados pelos Estados-Membros podem igualmente transmitir ou fornecer essas estatísticas à Comissão através de um processo automatizado. A Comissão deve emitir orientações sobre a estrutura dos dados e o método de recolha e de comunicação dessas estatísticas.

([1]) Para que não subsistam dúvidas, quaisquer referências às autoridades nacionais competentes devem igualmente ser entendidas como sendo aplicáveis, com as devidas adaptações, aos membros nacionais da Eurojust, aos procuradores europeus e aos procuradores europeus delegados, na medida em que se encontrem habilitados a desempenhar as mesmas funções ao abrigo do direito da UE e do direito nacional.

([2]) Importa recordar que, nos termos do artigo 19.º, n.º 5, a transmissão através desses meios de comunicação alternativos deve cumprir requisitos como ser rápida, segura e fiável, permitindo ao destinatário determinar a sua autenticidade.

([3]) Por «portais nacionais», entende-se os «sistemas informáticos» nacionais que fazem parte do sistema informático descentralizado definido no artigo 3.º, n.º 21, do Regulamento (UE) 2023/1543.

4. **Protocolos de comunicação**

4.1. O sistema informático descentralizado deve utilizar protocolos Internet seguros para a:

a) Comunicação, no âmbito do sistema informático descentralizado, entre as autoridades competentes;

b) Comunicação, no âmbito do sistema informático descentralizado, entre as autoridades competentes e as agências e organismos da União;

c) Comunicação entre as autoridades competentes e os prestadores de serviços através de uma API e de uma interface em linha; e

d) Comunicação com a base de dados dos Tribunais.

4.2. No que respeita à definição e à transmissão de dados estruturados e metadados, os componentes do sistema informático descentralizado devem basear-se em normas e protocolos setoriais abrangentes e amplamente aceites, como o SOAP e a REST, nomeadamente os referidos por organizações europeias de normalização, como o ETSI.

4.3. Relativamente aos protocolos de transporte e de transmissão de mensagens, o sistema informático descentralizado deve basear-se em protocolos normalizados seguros, por exemplo:

a) Um perfil AS4 para o intercâmbio transfronteiriço de dados, garantindo a transmissão segura e fiável de mensagens com cifragem e não repúdio;

b) Interfaces API HTTPS/RESTful para comunicação que suportem os formatos JSON e XML;

c) Um SOAP para interações de elevada fiabilidade, incorporando a WS-Security para autenticação e cifragem.

4.4. Para efeitos de um intercâmbio de dados contínuo e interoperável, os protocolos de comunicação utilizados pelo sistema informático descentralizado devem cumprir as normas de interoperabilidade pertinentes.

4.5. Quando aplicável, os esquemas XML das provas eletrónicas devem utilizar as normas ou vocabulários pertinentes necessários para uma validação adequada dos elementos e tipos definidos nesse esquema, podendo incluir:

a) O Vocabulário de Base da Justiça Eletrónica da UE;

b) Tipos de dados não qualificados;

c) Uma lista de códigos para os códigos de língua da União Europeia.

Além disso, quando aplicável, os esquemas XML podem incorporar normas ETSI pertinentes para utilizar as suas definições.

4.6. A Comissão define as especificações da API comum, a qual deve ser disponibilizada pelos Estados de execução aos prestadores de serviços como meio de acesso ao sistema informático descentralizado. Na medida do possível e razoável, esta API deve basear-se na ETSI TS 104 144 («Definição de interface para efeitos do Regulamento Provas Eletrónicas (UE) 2023/1543 para as autoridades nacionais e os prestadores de serviços»).

4.7. Quanto aos protocolos de segurança e de autenticação, o sistema informático descentralizado deve basear-se em protocolos normalizados, por exemplo:

a) Uma TLS (Segurança da Camada de Transporte) para comunicação cifrada e autenticada em redes que suporte autenticação mútua através de certificados digitais X.509;

b) Um OAuth/OpenID Connect (OIDC) para autenticação e autorização seguras;

c) Uma infraestrutura de chaves públicas e assinaturas digitais para a transmissão segura de chaves e para a verificação da integridade das mensagens, utilizando certificados digitais (X.509) emitidos por autoridades de certificação (AC).

5. **Objetivos relativos à segurança da informação e medidas técnicas pertinentes**

5.1. No que respeita ao intercâmbio de informações através do sistema informático descentralizado, as medidas técnicas para assegurar o respeito pelas normas mínimas de segurança informática devem contemplar:

a) Medidas destinadas a garantir a confidencialidade das informações, incluindo a utilização de canais seguros de comunicação;

b) Medidas destinadas a garantir a integridade dos dados (mensagens, formulários, documentos e provas eletrónicas) inativos e em trânsito;

c) Medidas destinadas a garantir o não repúdio da origem das informações pelo sistema informático descentralizado e o não repúdio da receção de informações;

d) Medidas destinadas a garantir a disponibilidade, assegurando o acesso contínuo aos serviços e aos dados e prevenindo perturbações resultantes de ciberataques ou falhas;

e) Medidas para garantir o registo das ocorrências em termos de segurança em conformidade com as recomendações internacionais reconhecidas em matéria de normas de segurança informática;

f) Medidas para garantir a autenticação e a autorização dos utilizadores, e medidas para verificar a identidade dos sistemas ligados ao sistema informático descentralizado.

5.2. Os componentes do sistema informático descentralizado devem garantir a segurança das comunicações e da transmissão de dados através da cifragem, da infraestrutura de chaves públicas com certificados digitais para autenticação e transmissão segura de chaves, bem como garantir protocolos seguros de transmissão de mensagens, como o AS4 (ebMS), as API RESTful e o SOAP, a fim de manter a confidencialidade e a integridade das mensagens.

5.3. Os componentes do sistema informático descentralizado devem ser desenvolvidos em conformidade com o princípio da proteção de dados desde a conceção e por defeito, devendo ser implementadas as medidas administrativas, organizativas e técnicas adequadas para garantir um elevado nível de cibersegurança.

5.4. A Comissão deve conceber, desenvolver e manter a aplicação informática de referência de acordo com os requisitos e princípios em matéria de proteção de dados estabelecidos no Regulamento (UE) 2018/1725. A aplicação informática de referência fornecida pela Comissão deve permitir que os Estados-Membros cumpram as obrigações que lhes incumbem por força, respetivamente, do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ([4]) e da Diretiva (UE) 2016/680 ([5]) do Parlamento Europeu e do Conselho, consoante o caso.

5.5. Os Estados-Membros que utilizem um sistema informático nacional que não a aplicação informática de referência devem implementar as medidas necessárias para garantir que esse sistema informático nacional cumpre os requisitos do Regulamento (UE) 2016/679 e da Diretiva (UE) 2016/680, consoante aplicável.

5.6. Tendo em conta a sua participação no sistema informático descentralizado, a Eurojust e a Procuradoria Europeia devem implementar as medidas necessárias para assegurar que os seus sistemas informáticos cumprem os requisitos do Regulamento (UE) 2018/1725 e dos respetivos atos constitutivos.

5.7. Os Estados-Membros, a Eurojust e a Procuradoria Europeia devem criar mecanismos robustos de deteção de ameaças e de resposta a incidentes, a fim de garantir, em tempo útil, a identificação, atenuação e recuperação de incidentes de segurança, de acordo com as suas políticas pertinentes, no que respeita aos sistemas informáticos sob a sua responsabilidade que fazem parte do sistema informático descentralizado.

6. **Cifragem de provas eletrónicas** ([6])

6.1. Sem prejuízo das medidas de segurança previstas pelo sistema informático descentralizado, ao emitirem uma ordem europeia de produção, as autoridades competentes podem ainda fornecer um certificado público X.509 específico para a cifragem assimétrica de provas eletrónicas.

([4]) Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

([5]) Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (JO L 119 de 4.5.2016, p. 89).

([6]) Para que não subsistam dúvidas, a expressão «provas eletrónicas» limita-se à definição que consta do artigo 3.º, n.º 8, do Regulamento (UE) 2023/1543.

6.2. A emissão, gestão, verificação e quaisquer aspetos conexos dos certificados referidos no ponto 6.1, bem como a infraestrutura de chaves públicas correspondente, são da exclusiva responsabilidade do Estado de emissão.

6.3. Sem prejuízo da evolução tecnológica futura, os certificados públicos devem suportar algoritmos de cifragem normalizados do setor, nomeadamente, o RSA (Rivest-Shamir-Adleman) ou o ECDH (curva elíptica Diffie-Hellman) para ECC (criptografia de curva elíptica).

6.4. Os certificados públicos devem incluir a extensão «keyUsage» adequada, designadamente a «keyEncipherment» ou a «dataEncipherment» para certificados com base em RSA e a «keyAgreement» para certificados com base em ECC. Os certificados devem ser disponibilizados nos formatos PEM [sigla inglesa de Privacy-Enhanced Mail (correio eletrónico com reforço da privacidade)] ou DER [sigla inglesa de Distinguished Encoding Rules (regras distintas de codificação)].

6.5. Caso a autoridade emissora tenha fornecido um certificado público X.509 e um prestador de serviços envie as provas eletrónicas produzidas ao abrigo de uma ordem europeia de produção, este último deve proceder à cifragem das provas eletrónicas utilizando o respetivo certificado público X.509 fornecido pelo Estado de emissão antes de proceder à transmissão desses dados através do sistema informático descentralizado.

6.6. Caso a autoridade emissora tenha fornecido um certificado público X.509, mas a transmissão das provas eletrónicas sob forma cifrada não seja possível por motivos técnicos ou por outros motivos justificáveis, e sem prejuízo do disposto no artigo 19.º, n.º 5, do Regulamento (UE) 2023/1543, o prestador de serviços pode transmitir os dados sem cifragem do conteúdo. Nesses casos, o prestador de serviços deve apresentar uma explicação fundamentada à autoridade emissora.

7. **Objetivos mínimos em matéria de disponibilidade**

7.1. Os Estados-Membros, a Eurojust e a Procuradoria Europeia devem assegurar a disponibilidade, 24 horas por dia, sete dias por semana, dos componentes do sistema informático descentralizado sob a sua responsabilidade, com uma taxa de disponibilidade técnica de referência anual de, pelo menos, 98 %, excluindo a manutenção programada.

7.2. Cabe à Comissão assegurar a disponibilidade, 24 horas por dia, sete dias por semana, da base de dados dos Tribunais, com uma taxa de disponibilidade técnica de referência anual superior a 99 %, excluindo a manutenção programada.

7.3. Tanto quanto possível, as operações de manutenção devem ser planeadas entre as 20h00 e as 7h00, CET.

7.4. Os Estados-Membros, a Eurojust e a Procuradoria Europeia devem notificar a Comissão e os restantes Estados-Membros das atividades de manutenção com a seguinte antecedência:

a) Cinco dias úteis, no que respeita às operações de manutenção que possam provocar um período de indisponibilidade de até quatro horas;

b) 10 dias úteis, no que respeita às operações de manutenção que possam provocar um período de indisponibilidade entre quatro e 12 horas;

c) 30 dias úteis, no que respeita às operações de manutenção que possam provocar um período de indisponibilidade superior a 12 horas.

7.5. Sempre que os Estados-Membros, a Eurojust ou a Procuradoria Europeia estabelecerem períodos fixos de manutenção regular, devem informar a Comissão e os participantes no sistema informático descentralizado da hora e do(s) dia(s) em que estão previstos esses períodos fixos de manutenção regular. Sem prejuízo das obrigações estabelecidas no ponto 7.4, caso os componentes do sistema informático descentralizado sob a responsabilidade dos Estados-Membros, da Eurojust ou da Procuradoria Europeia fiquem indisponíveis durante esses períodos fixos de manutenção regular, os mesmos podem optar, nesses casos, por não notificar a Comissão.

7.6. Em caso de falha técnica imprevista dos componentes do sistema informático descentralizado sob a responsabilidade dos Estados-Membros, da Eurojust ou da Procuradoria Europeia, os mesmos devem informar a Comissão e os participantes no sistema informático descentralizado desta falha, sem demora, bem como do período de recuperação estimado, caso seja conhecido.

7.7. Caso ocorram atividades de manutenção ou uma falha técnica imprevista dos componentes do sistema informático descentralizado sob a responsabilidade dos Estados-Membros, com impacto negativo na disponibilidade da API e/ou da interface em linha para os prestadores de serviços, o Estado-Membro em causa deve divulgar imediatamente esta informação num sítio Web e/ou comunicá-la aos prestadores de serviços que exercem a sua atividade no seu território, sem demora injustificada.

7.8. Em caso de falha técnica imprevista da base de dados dos Tribunais, a Comissão deve informar, sem demora, os Estados-Membros, a Eurojust e a Procuradoria Europeia desta indisponibilidade, bem como do período de recuperação estimado, caso seja conhecido.

7.9. Em caso de perturbação do serviço, os Estados-Membros, a Eurojust e a Procuradoria Europeia devem assegurar um restabelecimento célere do serviço e o mínimo de perda de dados, em conformidade com o objetivo de tempo de recuperação e com o objetivo de ponto de recuperação.

7.10. Os Estados-Membros, a Eurojust e a Procuradoria Europeia devem implementar as medidas adequadas para alcançar os objetivos de disponibilidade acima descritos, bem como estabelecer procedimentos para responder de forma eficaz aos incidentes.

8. **Base de dados das autoridades competentes/dos Tribunais**

8.1. Tendo em conta o artigo 19.º do Regulamento (UE) 2023/1543, para efeitos do funcionamento do sistema informático descentralizado, é essencial criar uma base de dados oficial sobre os prestadores de serviços e as autoridades competentes.

8.2. A base de dados oficial das autoridades competentes deve incluir as seguintes informações num formato estruturado:

a) Para efeitos do artigo 19.º do Regulamento (UE) 2023/1543, informações sobre as autoridades competentes notificadas nos termos do artigo 31.º, n.º 1, alíneas a) a c), do mesmo, nomeadamente no que diz respeito:

1) aos membros nacionais da Eurojust, bem como uma indicação sobre se estão autorizados, nos termos do direito nacional, a emitir ordens europeias de produção e de conservação, de acordo com o artigo 8.º, n.ºs 3 e 4, do Regulamento (UE) 2018/1727 do Parlamento Europeu e do Conselho ([7]),

2) aos procuradores europeus delegados e aos procuradores europeus, quando notificados pelos Estados-Membros, nos termos do artigo 105.º, n.º 3, do Regulamento (UE) 2017/1939 do Conselho ([8]), como autoridade emissora competente na aceção do Regulamento (UE) 2023/1543;

b) Quando aplicável, as informações necessárias para determinar as zonas geográficas da competência das autoridades ou outros critérios pertinentes necessários para estabelecer a sua competência;

c) Informações necessárias para o correto funcionamento dos intercâmbios de dados e para o correto encaminhamento de mensagens técnicas dos intercâmbios de dados no sistema informático descentralizado.

8.2.1. As informações referidas no ponto 8.2, alínea c), devem incluir:

a) Informações sobre o Estado-Membro onde está estabelecido o estabelecimento designado do prestador de serviços ou onde reside o seu representante legal:

1) estado-Membro,

2) autoridade central;

([7]) Regulamento (UE) 2018/1727 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, que cria a Agência da União Europeia para a Cooperação Judiciária Penal (Eurojust), e que substitui e revoga a Decisão 2002/187/JAI do Conselho (JO L 295 de 21.11.2018, p. 138).

([8]) Regulamento (UE) 2017/1939 do Conselho, de 12 de outubro de 2017, que dá execução a uma cooperação reforçada para a instituição da Procuradoria Europeia (JO L 283 de 31.10.2017, p. 1).

b) Informações sobre o prestador de serviços:

1) nome,

2) endereço/sede,

3) número de registo,

4) forma jurídica,

5) número de telefone,

6) endereço eletrónico;

c) Informações sobre o estabelecimento designado/representante legal:

1) tipo de entidade (estabelecimento designado/representante legal),

2) nome,

3) endereço/sede,

4) número de telefone,

5) endereço eletrónico,

6) pessoa/Entidade de contacto geral,

7) língua(s) oficial(ais) aceite(s) pelo prestador de serviços/estabelecimento designado/representante legal,

8) os serviços referidos no artigo 2.º, n.º 1, da Diretiva (UE) 2023/1544 do Parlamento Europeu e do Conselho ([9]) oferecidos na União,

9) tipo de instrumentos jurídicos da UE para os quais é designado o estabelecimento designado/ /representante legal (nas situações em que os Estados-Membros não participam em todos os instrumentos jurídicos pertinentes da UE),

10) âmbito territorial da designação/nomeação;

d) Autenticação das informações:

1) nome do representante autorizado,

2) cargo,

3) endereço,

4) número de telefone,

5) endereço eletrónico,

6) data.

8.2.2. Se disponíveis, as informações referidas no ponto 8.2, alínea c), podem incluir:

a) Informações sobre o prestador de serviços:

1) pessoa de contacto para questões relativas às notificações (se diferente do signatário),

2) sítio Web;

b) Tipos de dados disponíveis:

1) para cada serviço em causa:

— tipos de dados disponíveis,

— categoria de dados,

— identificadores,

— período de disponibilidade dos dados,

([9]) Diretiva (UE) 2023/1544 do Parlamento Europeu e do Conselho, de 12 de julho de 2023, que estabelece regras harmonizadas aplicáveis à designação de estabelecimentos designados e à nomeação de representantes legais para efeitos de recolha de prova eletrónica em processos penais (JO L 191 de 28.7.2023, p. 181, ELI: http://data.europa.eu/eli/dir/2023/1544/oj).

2) informações adicionais sobre os dados,

3) informações adicionais sobre o serviço (por exemplo, relações de subcontratação);

c) Informações sobre o estabelecimento designado/representante legal:

1) outros prestadores de serviços para os quais este estabelecimento designado ou representante legal tenha sido designado,

2) informações de contacto para assistência técnica,

3) contacto de emergência;

d) Informações técnicas:

1) nome do ponto de contacto para apoio técnico,

2) número de telefone do ponto de contacto para apoio técnico,

3) endereço eletrónico do ponto de contacto para apoio técnico,

4) endereço URL da API para obter informações sobre os tipos de dados de forma dinâmica,

5) tipo de ligação ao sistema informático nacional:

— interface em linha,

— API,

— Endereço URL da API para envio automático (*push*).

8.3. Tendo em conta as necessidades operacionais do sistema informático descentralizado:

a) A Comissão é responsável pelo desenvolvimento, manutenção, funcionamento e apoio da base de dados oficial;

b) A Comissão deve permitir o acesso à base de dados oficial através de uma API disponibilizada às autoridades competentes, à Eurojust e à Procuradoria Europeia para efeitos da sua participação no sistema informático descentralizado;

c) Os Estados-Membros devem assegurar que as informações relativas às suas autoridades competentes referidas no ponto 8.2, alíneas a) e b), constantes da base de dados oficial, são completas, exatas e atualizadas;

d) A base de dados oficial deve permitir que os Estados-Membros forneçam e atualizem na mesma as informações sobre os respetivos prestadores de serviços, bem como que as autoridades que participem no sistema informático descentralizado possam aceder a essas informações e recolhê-las através de programas;

e) Os Estados-Membros e os prestadores de serviços devem assegurar que as informações referidas no ponto 8.2, alínea c), constantes da base de dados oficial, são completas, exatas e atualizadas.