REGULAMENTO DE EXECUÇÃO (UE) 2025/2447 DA COMISSÃO

de 4 de dezembro de 2025

que estabelece as regras de execução do Regulamento (UE) 2018/1727 do Parlamento Europeu e do Conselho no que respeita às especificações técnicas, às medidas e a outros requisitos para a criação e utilização do sistema informático descentralizado para o tratamento e a comunicação seguros de informações

A COMISSÃO EUROPEIA,

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

Tendo em conta o 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 ([1]), nomeadamente o artigo 22.º-A, n.º 3, e o artigo 22.º-B, n.º 1, alíneas a), b), c) e d),

Considerando o seguinte:

(1) O Regulamento (UE) 2018/1727 estabelece o quadro para a nova infraestrutura interna digital da Eurojust e a criação de um sistema de comunicação digital segura descentralizado entre as autoridades nacionais competentes dos Estados-Membros e a Eurojust.

(2) A comunicação digital segura deve ser efetuada através do sistema informático descentralizado. Para criar o sistema informático descentralizado, é necessário estabelecer especificações técnicas que definam os métodos de comunicação e os protocolos de comunicação, medidas técnicas que assegurem os padrões mínimos de segurança da informação e a segurança em geral, bem como objetivos mínimos em matéria de disponibilidade para a aplicação desse sistema.

(3) Nos termos do artigo 22.º-A, n.º 1, do Regulamento (UE) 2018/1727, o sistema informático descentralizado deve incluir os sistemas informáticos dos Estados-Membros e da Eurojust, bem como pontos de acesso e-CODEX interoperáveis através dos quais esses sistemas informáticos estão interligados. As especificações técnicas e outros requisitos do sistema informático descentralizado estabelecidos no presente regulamento deverão ter em conta esse quadro.

(4) 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]).

(5) O sistema informático descentralizado é implementado no contexto de um sistema informático descentralizado de âmbito mais alargado, que assenta no sistema e-CODEX, denominado «sistema de intercâmbio digital de dados judiciários (JUDEX)». Por conseguinte, é necessário assegurar um intercâmbio eficaz de informações sobre a evolução horizontal.

(6) Nos termos do artigo 22.º-A, n.º 4, do Regulamento (UE) 2018/1727, os Estados-Membros e a Eurojust 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.

(7) Os dados relativos às infrações terroristas e à criminalidade organizada grave deverão ser transmitidos de forma estruturada, a fim de melhorar a qualidade e a pertinência das informações, bem como para assegurar que as informações possam ser integradas de forma mais eficiente no sistema de gestão de processos da Eurojust e mais bem controladas com as informações já armazenadas nesse sistema. No que diz respeito aos dados dactiloscópicos e às fotografias que podem ser transmitidos à Eurojust para efeitos de identificação de pessoas sujeitas a processos penais relacionados com infrações terroristas, deverão ser definidos o formato e as normas técnicas para a transmissão.

([1]) JO L 295 de 21.11.2018, p. 138, ELI: http://data.europa.eu/eli/reg/2018/1727/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).

(8) A Eurojust facilita e apoia a emissão e a execução dos pedidos de cooperação judiciária, incluindo os pedidos e as decisões baseados em instrumentos que dão execução ao princípio do reconhecimento mútuo. As autoridades nacionais competentes deverão poder solicitar assistência e coordenação à Eurojust através do sistema informático descentralizado.

(9) A fim de assegurar a eficiência e a coerência, é importante que as especificações técnicas a estabelecer ao abrigo do Regulamento (UE) 2018/1727 sejam compatíveis com as especificações técnicas estabelecidas ao abrigo dos Regulamentos (UE) 2023/2844 ([3]), (UE) 2023/1543 ([4]) e (UE) 2024/3011 ([5]) do Parlamento Europeu e do Conselho, bem como com futuras medidas de digitalização pertinentes para o mandato da Eurojust com vista a apoiar as autoridades nacionais competentes.

(10) Qualquer outra comunicação entre a Eurojust e as autoridades nacionais competentes, como a comunicação de informações sobre os resultados do tratamento de informações, incluindo a existência de ligações com casos já armazenados no sistema de gestão de processos em conformidade com o artigo 22.º do Regulamento (UE) 2018/1727, quando a Eurojust atua por iniciativa própria, ou de informações transmitidas à Eurojust para efeitos de preservação, análise e armazenamento de provas relacionadas com genocídio, crimes contra a humanidade, crimes de guerra e infrações penais conexas, em conformidade com o artigo 4.º, n.º 1, alínea j), desse regulamento, deverá também ser possibilitada através do sistema informático descentralizado.

(11) A fim de assegurar que o presente regulamento tem em conta as necessidades operacionais da Eurojust, esta foi consultada em conformidade com o artigo 22.º-A, n.º 3, do Regulamento (UE) 2018/1727.

(12) Nos termos do artigo 4.º do Protocolo n.º 21 relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, segurança e justiça, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União Europeia, a Irlanda notificou, por ofício de 9 de setembro de 2019, a sua intenção de aceitar e ficar vinculada pelo Regulamento (UE) 2018/1727. A Decisão (UE) 2019/2006 da Comissão ([6]) confirmou tal participação. O Regulamento (UE) 2023/2131 do Parlamento Europeu e do Conselho ([7]) alterou o Regulamento (UE) 2018/1727 a fim de permitir a criação de canais de comunicação digital seguros entre a Eurojust e as autoridades nacionais competentes e constitui a base jurídica para o presente regulamento. Nos casos em que a Irlanda não notificou a sua intenção de participar na adoção e na aplicação do Regulamento (UE) 2023/2131 e não notificou a sua intenção de aceitar e ficar vinculada por esse regulamento, a Irlanda, em conformidade com os artigos 1.º e 2.º e com o artigo 4.º-A, n.º 1, do Protocolo n.º 21, não fica vinculada pelo Regulamento (UE) 2023/2131 nem sujeita à sua aplicação. Por conseguinte, a Irlanda não participa na adoção do presente regulamento.

(13) 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 participou na adoção do Regulamento (UE) 2018/1727. Por conseguinte, a Dinamarca não fica vinculada pelo presente regulamento nem sujeita à sua aplicação.

([3]) Regulamento (UE) 2023/2844 do Parlamento Europeu e do Conselho, de 13 de dezembro de 2023, relativo à digitalização da cooperação judiciária e do acesso à justiça em matéria civil, comercial e penal com incidência transfronteiriça, e que altera determinados atos no domínio da cooperação judiciária (JO L, 2023/2844, 27.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2844/oj).

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

([5]) Regulamento (UE) 2024/3011 do Parlamento Europeu e do Conselho, de 27 de novembro de 2024, relativo à transmissão de processos penais (JO L, 2024/3011, 18.12.2024, ELI: http://data.europa.eu/eli/reg/2024/3011/oj).

([6]) Decisão (UE) 2019/2006 da Comissão, de 29 de novembro de 2019, relativa à participação da Irlanda no Regulamento (UE) 2018/1727 do Parlamento Europeu e do Conselho que cria a Agência da União Europeia para a Cooperação Judiciária Penal (Eurojust) (JO L 310 de 2.12.2019, p. 59, ELI: http://data.europa.eu/eli/dec/2019/2006/oj).

([7]) Regulamento (UE) 2023/2131 do Parlamento Europeu e do Conselho, de 4 de outubro de 2023, que altera o Regulamento (UE) 2018/1727 do Parlamento Europeu e do Conselho e a Decisão 2005/671/JAI do Conselho, no que respeita ao intercâmbio de informações digitais em casos de terrorismo (JO L, 2023/2131, 11.10.2023, ELI: http://data.europa.eu/eli/reg/2023/2131/oj).

(14) 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 ([8]) e emitiu um parecer em 21 de outubro de 2025.

(15) As medidas previstas no presente regulamento estão em conformidade com o parecer do comité criado pelo artigo 22.º-C do Regulamento (UE) 2018/1727,

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

Especificações técnicas do sistema informático descentralizado

As especificações técnicas, as medidas e os objetivos do sistema informático descentralizado a que se refere o artigo 22.º-B, n.º 1, alíneas a), b), c) e d), do Regulamento (UE) 2018/1727 são os estabelecidos no anexo I do presente regulamento.

Artigo 2.º

Normas processuais digitais

As normas processuais digitais aplicáveis à comunicação eletrónica através do sistema informático descentralizado a que se refere o artigo 22.º-A, n.º 3, do Regulamento (UE) 2018/1727 são as estabelecidas no anexo II do presente regulamento.

Artigo 3.º

Especificações técnicas para a transmissão de impressões digitais e fotografias

As especificações técnicas e o formato para a transmissão de impressões digitais e fotografias ~~a~~ que se refere o artigo 22.º-A, n.º 3, do Regulamento (UE) 2018/1727 constam do anexo III do presente regulamento.

Artigo 4.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 4 de dezembro de 2025.

Pela Comissão
A Presidente
Ursula VON DER LEYEN

([8]) 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 I

ESPECIFICAÇÕES TÉCNICAS, MEDIDAS E OBJETIVOS DO SISTEMA INFORMÁTICO DESCENTRALIZADO

1. **Introdução e âmbito de aplicação**

O presente anexo estabelece as especificações técnicas, as medidas e os objetivos do sistema informático descentralizado relativamente ao intercâmbio de informações previsto no Regulamento (UE) 2018/1727.

A natureza descentralizada do sistema informático permite o intercâmbio direto e seguro de dados entre as autoridades nacionais competentes e a Eurojust.

2. **Definições**

Para efeitos do presente anexo, entende-se por:

2.1. «Protocolo seguro de transferência de hipertexto» ou «HTTPS»: canais de comunicação encriptada 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» (Protocolo Simples de Acesso a Objetos): 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. «REST» (Transferência de estado representacional): 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 e documentos através do sistema informático descentralizado;

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

2.9. «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;

2.10. «ebMS»: serviço de transmissão de mensagens ebXML, um 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. Apoia a integração entre empresas em diversos sistemas;

2.11. «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;

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

2.13. «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. O sistema informático descentralizado utilizará métodos de comunicação assentes em serviços, nomeadamente serviços Web ou outros componentes e soluções de *software* reutilizáveis para efeitos de intercâmbio de mensagens e documentos.

3.2. Especificamente, o sistema informático descentralizado 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.

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 e a Eurojust;

b) Comunicação com a autoridade competente/base de dados dos tribunais a que se refere o ponto 7.1.

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.

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 encriptação 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 encriptação.

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. Se for caso disso, os esquemas XML devem utilizar as normas ou vocabulários pertinentes necessários para a correta validação dos elementos e tipos definidos no esquema. Essas normas ou vocabulários podem 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.

4.6. 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 encriptada 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 ICP (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.

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 o seguinte:

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 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 para garantir o registo das ocorrências em termos de segurança em conformidade com as recomendações internacionais reconhecidas em matéria de normas de segurança informática ([1]);

e) 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 encriptação, 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. Se for utilizada uma TLS no contexto do sistema informático descentralizado, deve ser utilizada a última versão estável do protocolo ou, na sua falta, uma versão sem vulnerabilidades de segurança conhecidas. Só são permitidos comprimentos de chave que garantam um nível adequado de segurança criptográfica, não podendo ser utilizadas sequências de cifras que se saiba serem inseguras ou obsoletas.

5.4. Na medida do possível, os certificados digitais ICP utilizados para efeitos do funcionamento do sistema informático descentralizado são emitidos pelas autoridades de certificação reconhecidas como prestadores qualificados de serviços de confiança, em conformidade com o Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho ([2]). Devem ser aplicadas medidas para garantir que esses certificados sejam utilizados exclusivamente para os fins a que se destinam, com o nível de confiança exigido e em conformidade com os requisitos aplicáveis do Regulamento (UE) n.º 910/2014.

5.5. 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.

5.6. 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 nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ([3]) e da Diretiva (UE) 2016/680, consoante o caso.

([1]) Sem prejuízo do registo para efeitos de segurança, os mecanismos de registo utilizados pelos componentes do sistema informático descentralizado devem, se for caso disso, permitir assegurar o cumprimento dos requisitos estabelecidos no artigo 88.º do Regulamento (UE) 2018/1725 e, se for caso disso, no artigo 25.º da 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, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

([2]) Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE (JO L 257 de 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([3]) 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

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

5.8. A Eurojust aplica as medidas necessárias para assegurar que o seu sistema de retaguarda, ou o exemplar da aplicação informática de referência que utiliza, cumpre os requisitos dos Regulamentos (UE) 2018/1725 e (UE) 2018/1727.

5.9. Os Estados-Membros e a Eurojust 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. **Objetivos mínimos em matéria de disponibilidade**

6.1. A Eurojust e os Estados-Membros 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.

6.2. 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.

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

6.4. Os Estados-Membros devem notificar a Comissão, a Eurojust e os outros Estados-Membros das atividades de manutenção do seguinte modo:

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

b) Dez 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.

6.5. Sempre que os Estados-Membros estabelecerem períodos fixos de manutenção regular, devem informar a Comissão, a Eurojust e os outros Estados-Membros da hora e do(s) dia(s) em que estão previstos esses períodos fixos de manutenção regular. Em derrogação das obrigações estabelecidas na primeira frase, caso os componentes do sistema informático descentralizado sob a responsabilidade dos Estados-Membros fiquem indisponíveis durante esses períodos fixos de manutenção regular, os Estados-Membros podem optar, nesses casos, por não notificar a Comissão.

6.6. Em caso de falha técnica imprevista de um componente do sistema informático descentralizado sob a responsabilidade dos Estados-Membros, os Estados-Membros devem informar a Comissão e os outros Estados-Membros desta falha, sem demora, bem como do período de recuperação estimado, caso seja conhecido.

6.7. A Eurojust notifica a Comissão e os Estados-Membros das atividades de manutenção do seguinte modo:

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

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

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

6.8. Sempre que a Eurojust estabelecer períodos fixos de manutenção regular, deve informar a Comissão e os Estados-Membros da hora e do(s) dia(s) em que estão previstos esses períodos fixos de manutenção regular. Em derrogação das obrigações estabelecidas na primeira frase, caso os componentes do sistema informático descentralizado sob a responsabilidade da Eurojust fiquem indisponíveis durante esses períodos fixos de manutenção regular, a Eurojust pode optar, nesses casos, por não notificar a Comissão.

6.9. Em caso de falha técnica imprevista de um componente do sistema informático descentralizado sob a responsabilidade da Eurojust, a Eurojust deve informar a Comissão e os Estados-Membros desta falha, sem demora, bem como do período de recuperação estimado, caso seja conhecido.

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

6.11. Em caso de perturbação do serviço, os Estados-Membros e a Eurojust devem assegurar que o serviço é restabelecido de forma célere e que a perda de dados é mínima, em conformidade com o objetivo de tempo de recuperação e com o objetivo de ponto de recuperação.

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

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

7.1. Nos termos do artigo 22.º-A do Regulamento (UE) 2018/1727, o sistema informático descentralizado deve permitir a comunicação eletrónica entre as autoridades nacionais competentes e a Eurojust. Tendo em conta as obrigações de intercâmbio de informações entre as autoridades nacionais competentes e a Eurojust nos termos dos artigos 21.º, 21.º-A e 22.º, mas também o papel da Eurojust na facilitação e no apoio à emissão e execução de qualquer pedido de auxílio judiciário mútuo ou de reconhecimento mútuo em conformidade com o artigo 8.º, n.º 1, do Regulamento (UE) 2018/1727, as autoridades competentes envolvidas devem ser claramente identificáveis aquando da utilização do sistema informático descentralizado. Por conseguinte, é essencial criar uma base de dados fidedigna das informações dessas autoridades para efeitos do sistema informático descentralizado.

7.2. A base de dados deve incluir as seguintes informações num formato estruturado:

a) para efeitos do artigo 8.º, n.ºs 1, 3 e 4, do artigo 21.º, do artigo 21.º-A e do artigo 22.º do Regulamento (UE) 2018/1727, informações sobre as autoridades nacionais competentes, incluindo os correspondentes nacionais, tal como estabelecido no artigo 20.º desse regulamento, bem como sobre os membros nacionais, em conformidade com o artigo 7.º ([4]) do mesmo regulamento;

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

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

7.3. A Comissão é responsável pelo desenvolvimento, manutenção, funcionamento e apoio da base de dados das autoridades competentes/dos tribunais.

7.4. A base de dados deve permitir que os Estados-Membros e a Eurojust atualizem as informações nela contidas, e que as autoridades nacionais competentes e os membros nacionais que participam no sistema informático descentralizado acedam e recuperem de forma programática informações nesse sistema.

7.5. O acesso à base de dados deve ser possível através de um protocolo de comunicação comum, independentemente de as autoridades competentes ligadas ao sistema informático descentralizado operarem um sistema nacional de retaguarda ou uma implantação da aplicação informática de referência.

7.6. Os Estados-Membros asseguram que as informações relativas às suas autoridades competentes na base de dados referida no ponto 7.2, são completas, exatas e atualizadas.

([4]) Tal não prejudica a delegação de poderes do membro nacional no seu adjunto, noutro pessoal do gabinete nacional ou no pessoal autorizado da Eurojust.

ANEXO II

NORMAS PROCESSUAIS DIGITAIS

O artigo 3.º, ponto 9, do Regulamento (UE) 2022/850 define normas processuais digitais como as especificações técnicas para os modelos dos processos operacionais e esquemas de dados que determinam a estrutura eletrónica dos dados trocados através do sistema e-CODEX.

O presente anexo estabelece as especificações técnicas dos modelos de processo operacional e as especificações técnicas dos esquemas de dados.

1. **Especificações técnicas dos modelos de processo operacional ao abrigo do Regulamento (UE) 2018/1727**

As especificações técnicas para os modelos de processo operacional são estabelecidas nos pontos 1.1 a 1.5 e definem os aspetos essenciais necessários para permitir a comunicação eletrónica para efeitos do Regulamento (UE) 2018/1727 através do sistema informático descentralizado.

O sistema informático descentralizado só permite o intercâmbio de informações entre as autoridades nacionais competentes de um Estado-Membro e o membro nacional desse Estado-Membro.

1.1. *Intercâmbio de informações relacionadas com o Registo Judiciário Europeu em Matéria de Contraterrorismo (RCT) — artigo 21.º-A do Regulamento (UE) 2018/1727*

1.1.1. Modelo para a transmissão de dados RCT:

A autoridade nacional competente transmite ao membro nacional dados sobre processos terroristas relativos ao RCT.

1.1.2. Modelo para a receção de dados RCT:

O membro nacional recebe os dados RCT.

1.1.3. Modelo de pedido de consentimento:

O membro nacional solicita o consentimento da sua autoridade nacional competente.

1.1.4. Modelo para a receção de um pedido de consentimento:

A autoridade nacional competente recebe o pedido de consentimento.

1.1.5. Modelo para o envio de uma resposta ao pedido de consentimento:

A autoridade nacional competente envia uma resposta ao pedido de consentimento.

1.1.6. Modelo para a receção de uma resposta ao pedido de consentimento:

O membro nacional recebe a resposta ao pedido de consentimento.

1.1.7. Modelo para a transmissão de informações sobre uma ligação:

O membro nacional informa a autoridade nacional competente acerca da ligação com outro processo.

1.1.8. Modelo para a atualização de dados RCT:

A autoridade nacional competente transmite ao respetivo membro nacional dados que necessitam de ser atualizados ou suprimidos.

1.1.9. Modelo para a atualização de dados RCT:

O membro nacional recebe os dados RCT que necessitam de atualização ou supressão.

1.2. *Intercâmbio de informações relacionadas com formas graves de criminalidade — artigo 21.º do Regulamento (UE) 2018/1727*

1.2.1. Modelo para a transmissão de dados sobre formas graves de criminalidade transfronteiriça:

A autoridade nacional competente transmite à Eurojust dados sobre as formas graves de criminalidade transfronteiriça.

1.2.2. Modelo para a receção de dados sobre as formas graves de criminalidade transfronteiriça:

O membro nacional recebe os dados relativos às formas graves de criminalidade transfronteiriça.

1.2.3. Modelo de pedido de consentimento:

O membro nacional solicita o consentimento da sua autoridade nacional competente.

1.2.4. Modelo para a receção de um pedido de consentimento:

A autoridade nacional competente recebe o pedido de consentimento.

1.2.5. Modelo para o envio de uma resposta ao pedido de consentimento:

A autoridade nacional competente envia uma resposta ao pedido de consentimento.

1.2.6. Modelo para a receção de uma resposta ao pedido de consentimento:

O membro nacional recebe a resposta ao pedido de consentimento.

1.2.7. Modelo para a transmissão de informações sobre uma ligação:

O membro nacional informa a autoridade nacional competente acerca da ligação com outro processo.

1.2.8. Modelo para a atualização de dados sobre formas graves de criminalidade transfronteiriça:

A autoridade nacional competente transmite ao respetivo membro nacional dados que necessitam de ser atualizados ou suprimidos.

1.2.9. Modelo para a receção de dados atualizados sobre formas graves de criminalidade transfronteiriça:

O membro nacional recebe os dados sobre formas graves de criminalidade transfronteiriça que necessitam de ser atualizados ou suprimidos.

1.3. *Intercâmbio de informações gerais*

1.3.1. Modelo para o envio de informações:

O membro nacional envia informações à autoridade nacional competente ou vice-versa.

1.3.2. Modelo para a receção de informações:

A autoridade nacional competente ou o membro nacional recebe as informações.

1.3.3. Modelo para a resposta às informações:

A autoridade nacional competente responde às informações recebidas do membro nacional ou vice-versa.

1.3.4. Modelo para a receção de uma resposta:

O membro nacional recebe a resposta da autoridade nacional competente.

1.3.5. Modelo para o envio de informações:

A autoridade nacional competente envia informações ao membro nacional.

1.3.6. Modelo para a receção de informações:

O membro nacional recebe as informações.

1.3.7. Modelo para a resposta às informações:

O membro nacional responde às informações recebidas da autoridade nacional competente.

1.3.8. Modelo para a receção de uma resposta:

A autoridade nacional competente recebe a resposta do membro nacional.

1.4. *Papel de facilitação e apoio — artigo 8.º, n.º 1, do Regulamento (UE) 2018/1727*

Nota: Sempre que os modelos de facilitação e apoio descritos no ponto 1.5 envolvam o intercâmbio de formulários legais estabelecidos por atos jurídicos da União no domínio da cooperação judiciária em matéria penal, os modelos devem, sempre que disponíveis, utilizar as representações de dados estruturadas e os esquemas XML pertinentes desenvolvidos para esses atos, por exemplo os estabelecidos para efeitos do Regulamento de Execução (UE) 2023/2844 ou de outros instrumentos pertinentes.

1.5. *Modelo de pedido de facilitação ou de apoio:*

1.5.1. Modelo para a transmissão de um pedido de facilitação ou de apoio:

A autoridade nacional competente transmite um pedido de facilitação ou de apoio ao respetivo membro nacional.

1.5.2. Modelo para a receção de um pedido de facilitação ou de apoio:

O membro nacional recebe o pedido de facilitação ou de apoio e transmite-o ao membro nacional do Estado-Membro requerido fora do JUDEX.

1.5.3. Modelo para a transferência de um pedido de facilitação ou de apoio à autoridade nacional competente:

O membro nacional do Estado-Membro requerido envia o pedido à respetiva autoridade nacional competente.

1.5.4. Modelo para a receção de um pedido de facilitação ou de apoio:

A autoridade nacional competente recebe o pedido de facilitação ou de apoio.

1.5.5. Modelo para o envio de uma resposta a um pedido de facilitação ou de apoio:

A autoridade nacional competente envia uma resposta ou informações sobre o pedido ao membro nacional do Estado-Membro requerido.

1.5.6. Modelo para a receção de uma resposta a um pedido de facilitação ou de apoio:

O membro nacional recebe a resposta ou informações relativas ao pedido de facilitação ou de apoio da autoridade nacional competente e partilha-a(s) com o membro nacional do Estado-Membro requerente fora do JUDEX.

1.5.7. Modelo para a resposta a um pedido de facilitação ou de apoio:

O membro nacional do Estado-Membro requerente responde ou partilha as informações relativas ao pedido de facilitação ou de apoio recebidas da autoridade nacional competente.

1.5.8. Modelo para a receção de uma resposta:

A autoridade nacional competente recebe a resposta ou as informações relativas ao pedido de facilitação ou de apoio.

2. **Especificações técnicas dos esquemas de dados**

As especificações técnicas que devem servir de base para o desenvolvimento de definições de esquemas XML (XSD) para a digitalização do Regulamento (UE) 2018/1727 são estabelecidas nos pontos 2.1 e 2.2 do presente anexo. Estas especificações definem os principais componentes, bem como quaisquer outras informações, a fim de fornecer uma descrição exaustiva para a criação destes esquemas.

A descrição pretende ser genérica, permitindo que os XSD produzidos sejam modificados e alargados sem necessidade de alterações significativas às presentes especificações.

As especificações aplicam-se à forma legal dos esquemas anexados ao Regulamento (UE) 2018/1727, a quaisquer mensagens predefinidas ou a quaisquer mensagens de texto livre utilizadas nos intercâmbios ao abrigo desse regulamento.

2.1. *Considerações gerais*

Para todos os esquemas a fornecer, aplicam-se as seguintes disposições:

2.1.1. Versões

Deve ser incluído um atributo de versão que facilite a gestão de versões do esquema e permita que o esquema seja atualizado em versões posteriores de acordo com os requisitos operacionais. O atributo de versão deve indicar se a nova versão é retrocompatível, aquando da introdução de novas características ou aperfeiçoamentos.

2.1.2. Declaração do esquema e metadados

— Se for caso disso, o esquema deve utilizar as normas ou vocabulários pertinentes exigidos pelo e-CODEX para permitir a interoperabilidade, necessários para a correta validação dos elementos e tipos definidos neste esquema, podendo incluir:

  — O Vocabulário de Base da Justiça Eletrónica da UE

  — Tipos de dados não qualificados

  — Uma lista de códigos para os códigos de língua da União Europeia

— Além disso, quando aplicável, o esquema pode incorporar normas ETSI pertinentes para utilizar as suas definições.

2.1.3. Anotações e documentação

— **Anotações**: Cada elemento do esquema deve normalmente ser acompanhado de anotações. As anotações fornecem informações legíveis pelo ser humano sobre o elemento, definindo frequentemente a sua finalidade ou utilização de forma clara e concisa.

2.1.4. Utilização e adaptabilidade

O esquema deve seguir as regras estabelecidas nas alíneas a) a d):

a) **Estrutura modular**: cada secção deve ser concebida com uma funcionalidade específica e pode ser reutilizada ou adaptada de forma independente, o que deve tornar o esquema mais fácil de adaptar para diferentes casos de utilização.

b) **Extensibilidade**: o esquema deve ser concebido de modo a apoiar a inclusão de novos elementos ou atributos, caso sejam necessárias informações adicionais no futuro. Para o efeito, utilizam-se elementos e sequências facultativos, que podem ser completados sem quebrar as aplicações existentes.

c) **Estrutura adaptável**: o esquema deve ser concebido de modo a permitir a adição ou modificação de elementos ou tipos de dados, conforme necessário. A estrutura do esquema deve ter em conta as alterações dos requisitos sem necessidade de remodelações importantes.

d) **Elementos facultativos**: os elementos de um esquema podem ser assinalados como facultativos, ou seja, podem ser incluídos ou omitidos com base em circunstâncias específicas.

O esquema deve ser concebido de forma a apoiar a recolha de dados estruturados para pedidos específicos.

2.1.5. Modificações

A conceção do esquema deve caracterizar-se por flexibilidade, modularidade e facilidade de adaptação. Os tipos complexos e os elementos facultativos devem ser incorporados na conceção de modo a permitir lidar com diferentes cenários, permanecendo a conceção, ao mesmo tempo, fácil de modificar e de ampliar.

2.2. *Intercâmbio de dados estruturados*

Os dados estruturados referidos nos pontos 2.2.1 e 2.2.2 devem ser fornecidos nos termos do artigo 22.º-A, n.º 3, do Regulamento (UE) 2018/1727. O esquema deve também permitir a indicação de conjuntos de dados que devem ser apagados em futuras atualizações.

2.2.1. Dados do Registo Judiciário Europeu em matéria de Contraterrorismo

As seguintes especificações técnicas para o esquema de dados estabelecem um quadro estruturado para a criação do esquema em formato XML.

a) Secção de nível superior

Esta secção de nível superior corresponde às informações constantes do anexo III do Regulamento (UE) 2018/1727 para o Registo Judiciário Europeu em Matéria de Contraterrorismo (RCT).

b) Estrutura da mensagem

A estrutura dos dados RCT deve consistir numa sequência de elementos e incluir, no mínimo, os seguintes elementos:

i) informações para a identificação das pessoas singulares:

— apelidos,

— nomes próprios,

— quaisquer outros nomes por que é conhecida,

— data de nascimento,

— local de nascimento (localidade e país),

— nacionalidade ou nacionalidades,

— documento de identificação (tipo e número do documento),

— género,

— local de residência,

ii) informações para a identificação das pessoas coletivas:

— firma,

— forma jurídica,

— sede social,

iii) informações para a identificação de pessoas singulares e coletivas:

— números de telefone,

— endereços de correio eletrónico,

— informações relativas a contas em bancos ou outras instituições financeiras,

— situação do processo,

iv) informações sobre a infração:

— informações relativas a pessoas coletivas implicadas na preparação ou prática de uma infração terrorista,

— qualificação jurídica da infração nos termos do direito nacional,

— formas graves de criminalidade aplicáveis da lista referida no anexo I,

— qualquer filiação num grupo terrorista,

— tipo de terrorismo, como seja, jiadista, separatista, de esquerda ou de direita,

— breve resumo do processo,

v) informações sobre o processo nacional:

— situação do processo,

— Ministério Público responsável,

— número do processo,

— data de instauração do processo judicial formal,

— ligações com outros processos conexos,

vi) campo de informações adicionais (texto livre),

vii) código da autorização prévia.

2.2.2. Dados transmitidos nos termos do artigo 21.º do Regulamento (UE) 2018/1727

a) Artigo 21.º, n.º 4, do Regulamento (UE) 2018/1727, criação de equipas de investigação conjunta (EIC)

(i) Secção de nível superior

Esta secção de nível superior corresponde às informações previstas no artigo 21.º, n.º 4, do Regulamento (UE) 2018/1727 sobre a criação de EIC.

ii) Estrutura da mensagem

A estrutura dos dados deve consistir numa sequência de elementos e incluir, no mínimo, os seguintes elementos:

— Autoridade judiciária nacional responsável pelo processo penal

— Número de referência nacional do processo penal

— Situação do processo penal

— Infrações penais investigadas

— Outros países envolvidos no processo

— Processo já apoiado pela Eurojust?

— Em caso afirmativo, identificação do processo da Eurojust

— Em caso negativo, trata-se de um pedido de apoio?

— Processo apoiado pela Europol?

— Em caso afirmativo, unidade operacional e/ou Aplicação de Intercâmbio Seguro de Informações (SIENA)

— Acordo da EIC:

— Países envolvidos

— Partes na EIC (autoridades nacionais responsáveis pelas investigações)

— Número de referência nacional do processo penal visado pela EIC

— Data de assinatura

— Duração

— Infrações penais investigadas

— Breve resumo do processo

— Principais suspeitos nos processos penais visados pela EIC (nome, apelido, data e local de nascimento e, eventualmente, outras categorias de dados pertinentes e necessárias nos termos do anexo II)

— Resultados do trabalho das EIC:

— Dificuldades/atrasos:

— na criação da EIC

— no pedido/na partilha de elementos de prova no âmbito da EIC

— acordo sobre/aplicação de uma estratégia comum em matéria de ação penal

— Admissibilidade/inadmissibilidade/avaliação dos elementos de prova da EIC nos processos nacionais

— Resultado dos processos judiciais (ações penais e condenações/absolvições bem-sucedidas/infrutíferas)

iii) Código da autorização prévia

b) Artigo 21.º, n.º 5, do Regulamento (UE) 2018/1727, processos graves e complexos

i) Secção de nível superior

Esta secção de nível superior corresponde às informações previstas no artigo 21.º, n.º 5, do Regulamento Eurojust, processos graves e complexos

ii) Estrutura da mensagem

A estrutura dos dados deve consistir numa sequência de elementos e incluir, no mínimo, os seguintes elementos:

— Autoridade judiciária nacional responsável pelo processo penal

— Número de referência nacional do processo penal

— Situação do processo penal

— Infrações penais investigadas

— Outros países envolvidos no processo

— Processo já apoiado pela Eurojust?

— Em caso afirmativo, identificação do processo da Eurojust

— Em caso negativo, trata-se de um pedido de apoio?

— Processo apoiado pela Europol?

— Em caso afirmativo, unidade operacional e/ou SIENA

— Forma de criminalidade grave aplicável

— Participação de uma rede de criminalidade organizada

— Tipo mafioso

— Rede transnacional de criminalidade organizada

— Repercussões a nível da UE

— Principais suspeitos nos processos penais (nome, apelido, data e local de nascimento e, eventualmente, outras categorias de dados pertinentes e necessárias nos termos do anexo II)

— Breve resumo do processo

— Outros países envolvidos

— Países com os quais a cooperação já foi iniciada

— Autoridades competentes envolvidas noutro país

— Ferramentas de cooperação judiciária utilizadas

— Número de pedidos enviados/recebidos

— Existência de investigações conexas

— Países com os quais a cooperação deve ser ativada/países eventualmente afetados

— Tipo de cooperação necessária (por exemplo, extradição, recolha de provas, outro tipo de cooperação)

— Existência de investigações conexas

iii) Código da autorização prévia

c) Artigo 21.º, n.º 6, alínea a), do Regulamento (UE) 2018/1727, conflitos de jurisdição

i) Secção de nível superior

Esta secção de nível superior corresponde às informações previstas no artigo 21.º, n.º 6, alínea a), do Regulamento (UE) 2018/1727, conflitos de jurisdição

ii) Estrutura da mensagem

A estrutura dos dados deve consistir numa sequência de elementos e incluir, no mínimo, os seguintes elementos:

— Autoridade judiciária nacional responsável pelo processo penal

— Número de referência nacional do processo penal

— Situação do processo penal (por exemplo, investigação, ação penal, julgamento)

— Infrações penais investigadas

— Outros países envolvidos no processo

— Processo já apoiado pela Eurojust?

— Em caso afirmativo, identificação do processo da Eurojust

— Em caso negativo, trata-se de um pedido de apoio?

— Processo apoiado pela Europol?

— Em caso afirmativo, unidade operacional e/ou SIENA

— Outros países envolvidos

— Autoridades nacionais competentes do outro país, se forem conhecidas

— Número de referência nacional do processo penal noutro país

— Fase do processo noutro país, se for conhecido

— Conflito positivo ou negativo

— Conflito real ou potencial

— Atividades de coordenação já realizadas (por exemplo, consultas ao abrigo da Decisão-Quadro 2009/948/JAI do Conselho ([1]))

— Breve resumo do processo

— Principais suspeitos comuns (nome, apelido, data e local de nascimento e, eventualmente, outras categorias de dados pertinentes e necessárias nos termos do anexo II)

iii) Código da autorização prévia

d) Artigo 21.º, n.º 6, alínea b), entregas controladas

i) Secção de nível superior

Esta secção de nível superior corresponde às informações previstas no artigo 21.º, n.º 6, alínea b), do Regulamento (UE) 2018/1727: entregas controladas.

ii) Estrutura da mensagem

A estrutura dos dados deve consistir numa sequência de elementos e incluir, no mínimo, os seguintes elementos:

— Autoridade judiciária nacional responsável pelo processo penal

— Número de referência nacional do processo penal

— Situação do processo penal (por exemplo, investigação, ação penal, julgamento)

— Infrações penais investigadas

— Outros países envolvidos no processo

— Processo já apoiado pela Eurojust?

— Em caso afirmativo, identificação do processo da Eurojust

— Em caso negativo, trata-se de um pedido de apoio?

— Processo apoiado pela Europol?

— Em caso afirmativo, unidade operacional e/ou SIENA

— Outros países envolvidos

— País de origem/trânsito/destino

— Autoridades nacionais competentes dos outros países

— Existência de investigações conexas noutros países

([1]) Decisão-Quadro 2009/948/JAI do Conselho, de 30 de Novembro de 2009 , relativa à prevenção e resolução de conflitos de exercício de competência em processo penal (JO L 328 de 15.12.2009, p. 42, ELI: http://data.europa.eu/eli/dec_framw/2009/948/oj).

— Tipo de mercadorias entregues (por exemplo, drogas e indicação do seu tipo/dinheiro/armas/ /cigarros/outros)

— Situação da entrega controlada (por exemplo, prevista, em curso, concluída)

— Resultado da entrega controlada, se já tiver sido executada

— Ferramenta de cooperação judiciária utilizada

— Principais suspeitos comuns (nome, apelido, data e local de nascimento e, eventualmente, outras categorias de dados pertinentes e necessárias nos termos do anexo II)

iii) Código da autorização prévia

e) Artigo 21.º, n.º 6, alínea c), do Regulamento (UE) 2018/1727, dificuldades reiteradas com instrumentos de cooperação judiciária

i) Secção de nível superior

Esta secção de nível superior corresponde às informações previstas no artigo 21.º, n.º 6, alínea c), do Regulamento (UE) 2018/1727: dificuldades reiteradas com instrumentos de cooperação judiciária.

ii) Estrutura da mensagem

A estrutura dos dados deve consistir numa sequência de elementos e incluir, no mínimo, os seguintes elementos:

— Autoridade judiciária nacional responsável pelo processo penal

— Número de referência nacional do processo penal

— Situação do processo penal (por exemplo, investigação, ação penal, julgamento)

— Infrações penais investigadas

— Outros países envolvidos no processo

— Processo já apoiado pela Eurojust?

— Em caso afirmativo, identificação do processo da Eurojust

— Em caso negativo, trata-se de um pedido de apoio?

— Processo apoiado pela Europol?

— Em caso afirmativo, unidade operacional e/ou SIENA

— Outros países envolvidos

— Autoridades nacionais competentes, se forem conhecidas

— Agindo na qualidade de autoridade emissora ou de execução

— Instrumento de cooperação judiciária em causa (por exemplo, MDE, DEI, congelamento de bens e perda)

— Pedido específico em causa (ou seja, que medida de investigação, que tipo de congelamento de bens, MDE para execução da pena ou para ação penal)

— Recusa ou dificuldade reiterada

— Em caso de recusa, qual o motivo específico invocado?

— Breve descrição do assunto

— Outras autoridades nacionais afetadas pela mesma dificuldade, se for caso disso

iii) Código da autorização prévia

2.3. *Códigos de autorização prévia*

Ao partilharem dados com a Eurojust através do JUDEX, as autoridades nacionais competentes devem indicar, através de códigos de autorização prévia, o tratamento, o acesso e a transferência de dados posteriores à identificação de uma ligação. Os códigos de autorização prévia devem indicar se, e em que medida, as informações relacionadas com a ligação podem ser partilhadas com outras autoridades nacionais competentes, outras agências e organismos da União, países terceiros ou organizações internacionais.

2.4. *Mensagens predefinidas*

As mensagens predefinidas são representações de intercâmbios estabelecidas pelo Regulamento (UE) 2018/1727, mas para as quais não foi prevista uma forma específica no ato jurídico. Os seus tipos e número são determinados durante a análise comercial e técnica.

As definições do esquema XLM (XSD) para mensagens predefinidas devem ser concebidas de modo a assegurar a coerência, a estrutura e a conformidade com as necessidades operacionais.

A estes esquemas aplica-se o seguinte:

a) A secção de nível superior deste esquema deve ser designada de acordo com o tipo de mensagem específico que é definido;

b) Os campos necessários para o tipo de mensagem específico devem ser acrescentados e definidos no âmbito desta estrutura, assegurando uma representação adequada dos elementos de dados.

2.5. *Mensagens de texto livre*

As mensagens de texto livre são representações de intercâmbios que permitem conteúdos não estruturados ou parcialmente estruturados, facultando flexibilidade ao mesmo tempo que cumprem os requisitos regulamentares e operacionais. O XSD para mensagens de texto livre deve ser concebido de modo a assegurar a coerência e a formatação adequada.

A estes esquemas aplica-se o seguinte:

a) A secção de nível superior do esquema deve ser designada de acordo com o tipo de mensagem de texto livre específico que é definido;

b) O esquema deve definir a estrutura necessária para a mensagem de texto livre, permitindo simultaneamente o ordenamento adequado dos elementos necessários;

c) Os campos necessários para o tipo de mensagem de texto livre específico devem ser acrescentados e definidos no âmbito desta estrutura, assegurando uma representação adequada do elemento de dados.

ANEXO III

ESPECIFICAÇÕES TÉCNICAS DAS IMPRESSÕES DIGITAIS E DAS FOTOGRAFIAS

As mensagens trocadas através do sistema informático descentralizado podem ser acompanhadas de anexos, incluindo ficheiros do Instituto Nacional de Normas e Tecnologia («NIST») que contenham impressões digitais e fotografias, em conformidade com as especificações técnicas estabelecidas nos pontos 1 e 2.

1. **Impressões digitais**

As impressões digitais que podem ser partilhadas com a Eurojust para efeitos de identificação fiável de pessoas sujeitas a processos penais relacionados com infrações terroristas devem satisfazer as seguintes condições:

a) As impressões digitais são fornecidas num único ficheiro que contém imagens digitais de impressões digitais (ficheiro NIST das impressões digitais) e são enviadas em conformidade com a norma ANSI/NIST-ITL 1-2011 Atualização de 2015 (ou versão mais recente);

b) O ficheiro NIST das impressões digitais é composto por até dez impressões digitais individuais: roladas, planas ou ambas;

c) Todas as impressões digitais têm uma referência informativa;

d) As impressões digitais são obtidas através de digitalizações instantâneas ou de impressões com tinta em papel, desde que as impressões digitais registadas em papel tenham sido digitalizadas com a resolução exigida e com a mesma qualidade;

e) o ficheiro NIST das impressões digitais permite a inclusão de informações complementares, tais como as condições de registo das impressões digitais e o método utilizado para a obtenção de imagens de impressões digitais individuais;

f) As impressões digitais têm uma resolução nominal de 500 ou 1 000 ppi ([1]) (com um desvio aceitável de +/– 10 ppi), com 256 níveis de cinzento;

g) O algoritmo de compressão das impressões digitais a utilizar segue as recomendações do Instituto Nacional de Normas e Tecnologia («NIST»). Os dados dactiloscópicos com uma resolução de 500 ppi são comprimidos utilizando o algoritmo WSQ (ISO/IEC 19794-5:2005). Os dados dactiloscópicos com uma resolução de 1 000 ppi são comprimidos utilizando a norma de compressão de imagens JPEG 2000 (ISO/IEC 15444-1) e o sistema de codificação. A taxa de compressão visada é 15:1.

2. **Fotografias**

As fotografia que podem ser partilhadas com a Eurojust para efeitos de identificação fiável de pessoas sujeitas a processos penais relacionados com infrações terroristas devem satisfazer as seguintes condições:

a) É fornecida apenas uma imagem facial num ficheiro fotográfico (o ficheiro fotográfico NIST) que é apresentada em conformidade com a norma ANSI/NIST-ITL 1-2011 Atualização de 2015, ou com qualquer versão mais recente disponível;

b) As fotografias são numa escala de cinzentos, a cores ou no infravermelho próximo;

c) A qualidade das fotografias baseia-se nos requisitos de imagem estabelecidos na norma ISO/IEC 19794-5: 2011 «Frontal image type» ou em qualquer versão mais recente disponível;

d) O ficheiro fotográfico NIST permite a inclusão de informações complementares, incluindo a data em que a imagem foi captada;

([1]) Píxeis por polegada.

e) As fotografias em modo retrato têm uma resolução mínima de 600 píxeis por 800 píxeis e uma resolução máxima de 1 200 píxeis por 1 600 píxeis;

f) A face ocupa um espaço dentro da fotografia que assegura um mínimo de 120 píxeis entre o centro de cada olho;

g) O algoritmo de compressão das fotografias utilizado segue as recomendações do Instituto Nacional de Normas e Tecnologia («NIST»). As fotografias são comprimidas uma única vez utilizando a norma de compressão de imagens JPG (ISO/IEC 10918) ou JPEG 2000 (ISO/IEC 15444) e um sistema de compressão e de codificação de imagens, a uma taxa máxima de compressão de imagem permitida de 20:1.