Conselho da
União Europeia

Bruxelas, 18 de abril de 2018
(OR. en)

8110/18

Dossiê interinstitucional:
2018/0108 (COD)

JAI 323
COPEN 104
CYBER 66
DROIPEN 53
JAIEX 27
ENFOPOL 171
TELECOM 94
DAPIX 106
EJUSTICE 27
MI 269
IA 101
CODEC 577

PROPOSTA

de:	Secretário-Geral da Comissão Europeia, assinado por Jordi AYET PUIGARNAU, Diretor
data de receção:	18 de abril de 2018
para:	Jeppe TRANHOLM-MIKKELSEN, Secretário-Geral do Conselho da União Europeia
n.° doc. Com.:	COM(2018) 225 final
Assunto:	Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo às ordens europeias de entrega ou de conservação de provas eletrónicas em matéria penal

Envia-se em anexo, à atenção das delegações, o documento COM(2018) 225 final.

Anexo: COM(2018) 225 final

COMISSÃO
EUROPEIA

Estrasburgo, 17.4.2018
COM(2018) 225 final

2018/0108 (COD)

Proposta de

REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

relativo às ordens europeias de entrega ou de conservação de provas eletrónicas em matéria penal

{SWD(2018) 118 final} - {SWD(2018) 119 final}

EXPOSIÇÃO DE MOTIVOS

1. CONTEXTO DA PROPOSTA

• Justificação e objetivos da proposta

Hoje em dia, a utilização das redes sociais, do correio eletrónico, dos serviços de mensagens e de aplicações («*apps*») para comunicar, trabalhar, socializar ou obter informações tornou-se um lugar-comum em muitas partes do mundo. Estes serviços ligam centenas de milhões de utilizadores e proporcionam benefícios consideráveis para o seu bem-estar económico e social, tanto na União como no resto do mundo. Contudo, também podem ser utilizados para praticar ou viabilizar a prática de crimes, nomeadamente crimes graves como ataques terroristas. Quando tal sucede, estes serviços e aplicações são, muitas vezes, os únicos locais onde os investigadores podem encontrar indícios que ajudem a identificar os autores dos crimes e obter provas que possam ser usadas em tribunal.

Dada a natureza transnacional da Internet, estes serviços podem ser prestados em qualquer parte do mundo, não exigindo necessariamente infraestruturas físicas, presença empresarial ou efetivos nos Estados-Membros em que são prestados ou no conjunto do mercado interno. Também não precisam de um local específico para armazenar os dados, o qual é frequentemente escolhido pelo prestador de serviços com base em considerações legítimas como a segurança dos dados, as economias de escala e a rapidez de acesso. Neste contexto, as autoridades dos Estados-Membros precisam, num número cada vez maior de processos penais que envolvem todos os tipos de criminalidade[1], de aceder a dados que possam servir de prova e que estão armazenados fora do seu país e/ou armazenados por prestadores de serviços estabelecidos noutros Estados-Membros ou em países terceiros.

Há várias décadas que têm vindo a ser desenvolvidos mecanismos de cooperação entre os países para as situações em que as provas ou o prestador de serviços se encontram noutro local[2]. Embora sejam periodicamente revistos, esses mecanismos estão sujeitos a uma pressão cada vez maior para responder à crescente necessidade de acesso transnacional em tempo útil a provas eletrónicas. Para colmatar essa necessidade, vários Estados-Membros e países terceiros recorreram à expansão dos respetivos instrumentos nacionais. A fragmentação daí resultante gera insegurança jurídica e obrigações contraditórias, suscitando questões quanto à proteção dos direitos fundamentais e das garantias processuais das pessoas afetadas por esses pedidos de dados e informações.

Em 2016, o Conselho apelou à adoção de medidas concretas baseadas numa abordagem comum da UE, a fim de tornar o auxílio judiciário mútuo mais eficaz, melhorar a cooperação entre as autoridades dos Estados-Membros e os prestadores de serviços estabelecidos em países terceiros e propor soluções para os problemas da determinação e do exercício da competência coerciva[3] no ciberespaço[4]. O Parlamento Europeu destacou igualmente os

---

1 Ver pontos 2.1.1 e 2.3 da avaliação do impacto.

2 Na União, existem mecanismos de reconhecimento mútuo, que são atualmente baseados na Diretiva relativa à decisão europeia de investigação. No caso de países terceiros, estão previstos mecanismos de auxílio judiciário mútuo (AJM).

3 No presente documento, entende-se por «competência coerciva» a competência das autoridades pertinentes para levarem a cabo uma medida de investigação.

4 Conclusões do Conselho da União Europeia sobre a melhoria da justiça penal no ciberespaço, ST9579/16.

problemas que a fragmentação do atual quadro jurídico pode criar aos prestadores de serviços que procuram cumprir as exigências das autoridades policiais, tendo preconizado a definição de um quadro jurídico europeu que preveja a salvaguarda dos direitos e liberdades de todos os interessados[5].

A presente proposta visa resolver o problema específico criado pela natureza volátil da prova eletrónica e a sua dimensão internacional. Procura adaptar os mecanismos de cooperação à era digital, dotando o sistema judiciário e as autoridades policiais de instrumentos que permitam contemplar os novos meios de comunicação que os criminosos utilizam e combater as formas modernas de criminalidade. Estes instrumentos estão sujeitos a mecanismos de proteção rigorosos no que respeita aos direitos fundamentais. A presente proposta tem por objetivo melhorar a segurança jurídica para as autoridades, os prestadores de serviços e as pessoas afetadas, assegurando normas exigentes quanto aos pedidos formulados pelas autoridades policiais e garantindo, assim, a proteção dos direitos fundamentais, a transparência e a responsabilização. Visa igualmente agilizar o processo de obtenção de provas eletrónicas armazenadas e/ou conservadas por prestadores de serviços estabelecidos noutra jurisdição. Este instrumento irá coexistir com os instrumentos de cooperação judiciária que se encontrem em vigor e que sejam passíveis de ser utilizados pelas autoridades competentes. Paralelamente, a Comissão está a trabalhar no sentido de reforçar os mecanismos de cooperação judiciária existentes, através de medidas como a criação de uma plataforma segura para o rápido intercâmbio de pedidos de dados entre as autoridades judiciais da UE, tendo investido um milhão de euros na formação de profissionais de todos os Estados-Membros da UE nos domínios da cooperação judiciária e do auxílio judiciário mútuo, com ênfase nos Estados Unidos enquanto país terceiro que recebe o maior número de pedidos da UE[6].

No que respeita à notificação e à execução das ordens emitidas no âmbito deste instrumento, as autoridades devem recorrer ao representante legal nomeado pelos prestadores de serviços. A Comissão apresenta hoje uma proposta para garantir que esses representantes legais sejam efetivamente designados, a qual prevê uma solução comum ao nível da UE para a notificação de ordens jurídicas a prestadores de serviços através de um representante legal.

- **Coerência com o quadro jurídico da UE no domínio em causa e com a Convenção de Budapeste do Conselho da Europa**

O atual quadro jurídico da UE é constituído por instrumentos de cooperação em matéria penal, como a Diretiva 2014/41/UE, relativa à decisão europeia de investigação em matéria penal[7] (Diretiva relativa à DEI), a Convenção relativa ao auxílio judiciário mútuo em matéria penal entre os Estados-Membros da União Europeia[8], a Decisão 2002/187/JAI do Conselho, relativa à criação da Eurojust[9], o Regulamento (UE) 2016/794, relativo à Europol[10],

5 P8_TA(2017)0366.

6 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf

7 Diretiva 2014/41/UE do Parlamento Europeu e do Conselho, de 3 de abril de 2014, relativa à decisão europeia de investigação em matéria penal (JO L 130 de 1.5.2014, p. 1).

8 Ato do Conselho, de 29 de maio de 2000, que estabelece, em conformidade com o artigo 34.º do Tratado da União Europeia, a Convenção relativa ao auxílio judiciário mútuo em matéria penal entre os Estados-Membros da União Europeia.

9 Decisão 2002/187/JAI do Conselho, de 28 de fevereiro de 2002, relativa à criação da Eurojust a fim de reforçar a luta contra as formas graves de criminalidade. Em 2013, a Comissão adotou uma proposta de

a Decisão-Quadro 2002/465/JAI do Conselho, relativa às equipas de investigação conjuntas[11], bem como acordos bilaterais entre a União e países terceiros, como o Acordo sobre auxílio judiciário mútuo entre a UE e os EUA[12] e o Acordo sobre auxílio judiciário mútuo entre a UE e o Japão[13].

A presente proposta visa, mediante a introdução das ordens europeias de entrega ou de conservação de provas, facilitar a obtenção e a recolha de provas eletrónicas em processo penal que se encontrem armazenadas ou sejam detidas por prestadores de serviços estabelecidos noutra jurisdição. A Diretiva relativa à DEI, que substituiu em larga medida a Convenção relativa ao auxílio judiciário mútuo em matéria penal, abrange todas as medidas de investigação[14], incluindo o acesso a provas eletrónicas, mas não contém disposições específicas para este tipo de provas[15]. O novo instrumento não substituirá a decisão europeia de investigação (DEI) quanto à obtenção de provas eletrónicas, mas prevê um mecanismo suplementar para as autoridades. Poderão existir situações (por exemplo, quando seja necessário aplicar várias medidas de investigação no Estado-Membro de execução) em que a decisão europeia de investigação poderá ser o instrumento preferido das autoridades públicas. A criação de um novo instrumento para as provas eletrónicas é uma alternativa melhor do que a alteração da Diretiva relativa à DEI, uma vez que os desafios específicos inerentes à obtenção deste tipo de provas não afetam as outras medidas de investigação abrangidas por essa diretiva.

Por forma a facilitar a recolha transnacional de provas eletrónicas, o novo instrumento basear-se-á nos princípios de reconhecimento mútuo. Para a notificação e execução da ordem não será necessário envolver diretamente a autoridade do país no qual o destinatário se encontre, salvo em caso de incumprimento, situação que implicaria a execução coerciva e a intervenção da autoridade competente do país onde o representante está localizado. Por conseguinte, este instrumento requer a adoção de um conjunto de disposições e salvaguardas sólidas como, por exemplo, a validação das ordens por uma autoridade judicial em cada caso concreto. A título de exemplo, as ordens europeias de entrega de dados transacionais ou de conteúdos (em oposição a dados de assinantes e de acesso) só podem ser emitidas no caso de infrações penais puníveis no Estado de emissão com uma pena privativa de liberdade de duração máxima não inferior a três anos ou no caso de crimes específicos nos

---

Regulamento para a reforma da Eurojust (Proposta de Regulamento do Parlamento Europeu e do Conselho que cria a Agência Europeia para a Cooperação Judiciária Penal (Eurojust), COM/2013/0535 final).

10 Regulamento (UE) 2016/794 do Parlamento Europeu e do Conselho, de 11 de maio de 2016, que cria a Agência da União Europeia para a Cooperação Policial (Europol) e que substitui e revoga as Decisões 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI e 2009/968/JAI do Conselho.

11 Decisão-Quadro 2002/465/JAI do Conselho, de 13 de junho de 2002, relativa às equipas de investigação conjuntas.

12 Decisão 2009/820/PESC do Conselho, de 23 de outubro de 2009, relativa à celebração, em nome da União Europeia, do Acordo entre a União Europeia e os Estados Unidos da América sobre extradição e do Acordo entre a União Europeia e os Estados Unidos da América sobre auxílio judiciário mútuo.

13 Decisão 2010/616/UE do Conselho, de 7 de outubro de 2010, sobre a celebração do Acordo entre a União Europeia e o Japão relativo ao auxílio judiciário mútuo em matéria penal.

14 Com exceção das equipas de investigação conjuntas (ver artigo 3.º da Diretiva relativa à DEI); nem todos os Estados-Membros participam na Diretiva relativa à DEI (Irlanda, Dinamarca).

15 Com exceção de uma referência, no artigo 10.º, n.º 2, alínea e), à identificação de pessoas que tenham uma assinatura de um número de telefone ou um endereço IP específicos, para as quais a dupla criminalização não pode ser invocada como fundamento para a recusa de reconhecimento e de execução do pedido.

domínios da cibercriminalidade e da criminalidade possibilitada pelo ciberespaço ou relacionados com o terrorismo, conforme referido na proposta.

Os dados pessoais abrangidos pela presente proposta estão protegidos e só podem ser tratados de acordo com o Regulamento geral sobre a proteção de dados[16] e com a Diretiva relativa à proteção dos dados destinados às autoridades policiais e judiciais (Diretiva sobre a proteção de dados na aplicação da lei)[17]. O Regulamento geral sobre a proteção de dados entra em vigor em 25 de maio de 2018 enquanto a Diretiva sobre a proteção de dados na aplicação da lei deveria ser transposta pelos Estados-Membros até 6 de maio de 2018.

A Convenção de Budapeste do Conselho da Europa sobre a Cibercriminalidade (CETS n.º 185), ratificada pela maioria dos Estados-Membros da UE, estabelece mecanismos internacionais de cooperação contra a cibercriminalidade[18]. A Convenção aborda os crimes cometidos através da Internet e de outras redes informáticas e insta as Partes a instituir poderes e procedimentos para obter provas eletrónicas e prestar auxílio judiciário mútuo, no que respeita à cibercriminalidade e não só. Em particular, exige que as Partes criem a figura da ordem de entrega de provas a fim de obter dados informáticos dos prestadores de serviços estabelecidos no seu território e dados de assinantes de prestadores de serviços que operam no seu território. Além disso, prevê a emissão de ordens de conservação de provas quando existam motivos para crer que os dados informáticos são particularmente vulneráveis a perdas ou alterações. A notificação e a execução coerciva das ordens nacionais de entrega de provas dirigidas a prestadores estabelecidos fora do território de uma Parte na Convenção suscitam questões adicionais. A este respeito, estão atualmente em estudo novas medidas para melhorar o acesso transnacional a provas eletrónicas[19].

- **Resumo da proposta de regulamento**

A proposta de regulamento introduz a ordem europeia de entrega de provas e a ordem europeia de conservação de provas, que são ambas vinculativas e devem ser emitidas ou validadas por uma autoridade judicial de um Estado-Membro. As referidas ordens podem ser emitidas com a finalidade de obter ou conservar dados armazenados por um prestador de serviços estabelecido noutra jurisdição, para serem utilizados como prova em investigações ou processos penais. Contudo, só podem ser emitidas se existir uma medida semelhante para a mesma infração penal numa situação nacional comparável no Estado de emissão. Ambas as ordens podem ser notificadas aos prestadores de serviços de comunicações eletrónicas, de

16 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.

17 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.

18 Na Estratégia para a Cibersegurança da União Europeia, de 2013, a Convenção de Budapeste foi reconhecida como o principal quadro multilateral de combate à cibercriminalidade - Comunicação Conjunta da Comissão e da Alta Representante da União Europeia para os Negócios Estrangeiros e a Política de Segurança intitulada «Estratégia da União Europeia para a cibersegurança: um ciberespaço aberto, seguro e protegido (JOIN(2013) 1 final).

19 Na sua 17.ª reunião (junho de 2017), o Comité da Convenção sobre a Cibercriminalidade (T-CY) adotou o mandato para a preparação de um segundo protocolo adicional da Convenção («Segundo Protocolo Adicional»), que deverá ser elaborado e concluído pelo T-CY até dezembro de 2019. O objetivo é que o local de armazenamento de dados deixe de ser considerado como fator decisivo.

redes sociais e de mercados em linha, a outros prestadores de serviços de alojamento e aos prestadores de serviços de Internet, como registos de endereço IP e nomes de domínio, ou aos seus representantes legais, quando existam. A ordem europeia de entrega de provas, tal como a ordem europeia de conservação de provas, é dirigida ao representante legal estabelecido fora da jurisdição do Estado-Membro de emissão e tem por objetivo conservar os dados tendo em vista um pedido subsequente de entrega de provas, por exemplo através de canais de auxílio judiciário mútuo, no caso de países terceiros, ou através de uma decisão europeia de investigação entre os Estados-Membros participantes. Ao contrário das medidas de vigilância ou das obrigações de retenção de dados estabelecidas por lei, que não estão previstas no regulamento, uma ordem europeia de conservação de provas é uma ordem emitida ou validada por uma autoridade judicial no âmbito de um processo penal, após uma avaliação individual da proporcionalidade e da necessidade em cada caso concreto. Tal como a ordem europeia de entrega de provas, diz respeito ao autor concreto, conhecido ou desconhecido, de uma infração penal já cometida. A ordem europeia de conservação de dados só permite conservar dados que já se encontrem armazenados à data da sua receção, não permitindo o acesso aos dados numa data posterior à receção da mesma.

Ambas as ordens europeias só podem ser utilizadas em processo penal, desde a fase de investigações preliminares e a fase de instrução até ao encerramento do processo por sentença ou outra decisão. As ordens de entrega de dados de assinantes e de acesso podem ser emitidas para qualquer infração penal, enquanto as ordens de entrega de dados transacionais ou de conteúdo só podem ser emitidas no caso de infrações penais puníveis no Estado de emissão com uma pena privativa de liberdade de duração máxima não inferior a três anos ou no caso de crimes específicos (referidos na proposta) e de crimes com ligação específica a ferramentas eletrónicas ou infrações abrangidas pela Diretiva 2017/541/UE relativa à luta contra o terrorismo.

Tendo em conta os diferentes níveis de ingerência das medidas impostas quanto aos dados solicitados, a proposta de regulamento estabelece uma série de condições e salvaguardas, que incluem a obrigação de validação prévia das ordens por uma autoridade judicial. A proposta aplica-se exclusivamente aos dados já armazenados. A interceção de telecomunicações em tempo real não é abrangida pelo seu âmbito de aplicação. A medida é limitada ao que é necessário e proporcional no âmbito do processo penal. Permite igualmente que os prestadores de serviços solicitem esclarecimentos às autoridades que emitiram a ordem, sempre que necessário. Se não for possível obter os esclarecimentos solicitados e a autoridade emissora decidir executar coercivamente a ordem, os prestadores de serviços poderão utilizar os mesmos fundamentos para se oporem à execução da ordem pelas respetivas autoridades. Além disso, o regulamento estabelece um procedimento específico para as situações em que a obrigação de fornecer dados entre em conflito com uma obrigação concorrente por força do direito de um país terceiro.

A legislação da UE protege os direitos dos suspeitos e dos arguidos em processo penal, prevendo normas de proteção dos dados pessoais. No entanto, para as pessoas cujos dados são solicitados, as salvaguardas suplementares que constam da proposta de regulamento conferem-lhes direitos processuais no âmbito do processo penal ou fora dele. Esses direitos incluem a possibilidade de contestar a legalidade, a necessidade ou a proporcionalidade da ordem, sem restringir os fundamentos da contestação de acordo com o direito nacional. Os direitos decorrentes do direito do Estado de execução são plenamente respeitados, garantindo que as imunidades e os privilégios que protegem os dados solicitados no Estado-Membro do prestador de serviços sejam tidos em conta no Estado de emissão, sobretudo quando esses

direitos preveem uma proteção mais elevada do que a conferida pelo direito do Estado de emissão.

As ordens emitidas ao abrigo do regulamento proposto serão executáveis da mesma forma que as ordens nacionais equivalentes na jurisdição onde o prestador de serviços for notificado da ordem. O regulamento prevê que os Estados-Membros apliquem sanções eficazes e proporcionadas.

2. BASE JURÍDICA, SUBSIDIARIEDADE E PROPORCIONALIDADE

• Base jurídica

A base jurídica da intervenção neste domínio é o artigo 82.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia, que estabelece que podem ser adotadas medidas de acordo com o processo legislativo ordinário, destinadas a definir regras e procedimentos para assegurar o reconhecimento em toda a União de todas as formas de sentenças e decisões judiciais. Prevê ainda a adoção de medidas destinadas a facilitar a cooperação entre as autoridades judiciais ou outras equivalentes dos Estados-Membros, no âmbito da investigação e do exercício da ação penal, assim como da execução de decisões.

Esta base jurídica aplica-se aos mecanismos abrangidos pelo regulamento. O artigo 82.º, n.º 1, assegura o reconhecimento mútuo de decisões judiciais, através das quais uma autoridade judicial do Estado de emissão notifica uma pessoa coletiva noutro Estado-Membro e inclusive lhe impõe obrigações, sem a intervenção prévia de uma autoridade judicial nesse outro Estado-Membro. Uma ordem europeia de entrega ou de conservação de provas pode implicar a intervenção de uma autoridade judicial do Estado de execução, se tal for necessário para a sua execução coerciva.

• Escolha do instrumento

O artigo 82.º, n.º 1, do TFUE confere ao legislador da União a possibilidade de adotar regulamentos e diretivas.

Uma vez que a proposta diz respeito a procedimentos transnacionais, que requerem normas uniformes, não é necessário deixar margem de manobra aos Estados-Membros para a transposição das mesmas. Um regulamento é diretamente aplicável, proporciona clareza e maior segurança jurídica, evitando interpretações divergentes nos Estados-Membros, bem como outros problemas de transposição que afetaram anteriormente as decisões-quadro sobre o reconhecimento mútuo de sentenças e decisões judiciais. Além disso, um regulamento permite que uma mesma obrigação seja imposta uniformemente em toda a União. Por estas razões, considera-se que o regulamento é a forma mais adequada para este instrumento de reconhecimento mútuo.

• Subsidiariedade

Tendo em conta a dimensão transnacional dos problemas encontrados, as medidas incluídas na proposta devem ser adotadas a nível da União, com vista à consecução dos objetivos. Os crimes para os quais existem provas eletrónicas envolvem frequentemente situações em que a infraestrutura na qual essas provas são armazenadas e o prestador de serviços que a gere são abrangidos por um quadro jurídico nacional diferente, dentro ou fora da União, do quadro

jurídico nacional aplicável à vítima e ao autor da infração. Por conseguinte, sem normas mínimas comuns, poderá ser demasiado moroso e difícil para o país competente dispor de acesso transnacional eficaz a essas provas eletrónicas. Mas concretamente, os Estados-Membros agindo isoladamente teriam dificuldade em abordar as seguintes questões:

- Fragmentação dos quadros jurídicos nos Estados-Membros, já identificada como um sério problema pelos prestadores de serviços que procuram satisfazer os pedidos apresentados com base em diferentes legislações nacionais;

- Melhor oportunidade de cooperação judiciária com base na legislação da União em vigor, nomeadamente através da DEI.

Tendo em conta a diversidade das abordagens jurídicas, o número de domínios de intervenção em causa (segurança, direitos fundamentais e direitos processuais, proteção de dados pessoais, questões económicas) e o vasto leque de partes interessadas, a legislação à escala da União é o meio mais adequado para resolver os problemas identificados.

- **Proporcionalidade**

A proposta estabelece as normas segundo as quais uma autoridade competente de um Estado-Membro da União pode ordenar a um prestador de serviços que opere na União e não esteja estabelecido nesse mesmo Estado-Membro que entregue ou conserve em seu poder provas eletrónicas. As suas principais características, designadamente o âmbito material da ordem europeia de entrega de provas, as condições que garantem o princípio da cortesia internacional, o mecanismo sancionatório e o sistema de salvaguardas e vias de recurso, limitam a proposta ao necessário para atingir os seus principais objetivos. Concretamente, a proposta cinge-se aos pedidos relativos a dados armazenados (os dados relativos à interceção das telecomunicações em tempo real não são abrangidos) e às decisões proferidas em processo penal para infrações penais específicas sob investigação. Não abrange, por conseguinte, a prevenção da criminalidade ou outros tipos de processos ou infrações (como processos administrativos por infração à lei) e não exige que os fornecedores dos dados recolham ou armazenem sistematicamente mais dados do que aqueles que recolhem ou armazenam por razões profissionais ou para cumprimento de outros requisitos legais. Além disso, enquanto as ordens de entrega de dados de assinantes e de acesso podem ser emitidas para qualquer infração penal, as ordens de entrega de dados transacionais ou de conteúdo só podem ser emitidas no caso de infrações penais puníveis no Estado de emissão com uma pena privativa de liberdade de duração máxima não inferior a três anos, ou no caso de infrações específicas nos domínios da cibercriminalidade e da criminalidade possibilitada pelo ciberespaço (definidas na proposta) e de crimes relacionados com o terrorismo. Por último, a proposta clarifica as normas processuais e as salvaguardas aplicáveis ao acesso transnacional a provas eletrónicas, mas não visa harmonizar as medidas nacionais. Limita-se ao que é necessário e proporcional para atender às necessidades das autoridades policiais e judiciais na era digital.

3. RESULTADOS DAS AVALIAÇÕES *EX POST*, DA CONSULTA DAS PARTES INTERESSADAS E DAS AVALIAÇÕES DE IMPACTO

• Consulta das partes interessadas

Durante um ano e meio, a Comissão consultou todas as partes interessadas relevantes para identificar os problemas e as possíveis vias a seguir nesta matéria. Essa consulta foi levada a cabo através de inquéritos, nomeadamente uma consulta pública e inquéritos específicos às autoridades públicas pertinentes. Foram ainda organizadas reuniões do grupo de peritos e reuniões bilaterais para analisar os possíveis efeitos da legislação da UE, assim como conferências para debater o acesso transnacional a provas eletrónicas, que serviram para sondar as opiniões sobre esta iniciativa.

De um modo geral, os inquiridos consideraram que o aumento da utilização dos serviços de informação representa um desafio para as autoridades policiais, já que muitas vezes estas estão insuficientemente equipadas para tratar provas eletrónicas. A morosidade do processo de obtenção de provas é considerada um dos principais obstáculos. Outras questões importantes identificadas pelas autoridades públicas incluem a falta de cooperação fiável com os prestadores de serviços, a falta de transparência e, no que respeita às medidas de investigação, a incerteza jurídica quanto à competência jurisdicional. Foi igualmente reconhecido que a cooperação transnacional direta entre as autoridades policiais e os prestadores de serviços digitais acrescenta valor às investigações penais. Os prestadores de serviços e algumas organizações da sociedade civil referiram a necessidade de garantir a segurança jurídica no âmbito da cooperação com as autoridades públicas e de prevenir conflitos de leis. No que se refere às preocupações sobre a forma como a nova legislação da UE poderá afetar os direitos das pessoas em causa, as partes interessadas consideraram que deveriam ser garantidas salvaguardas específicas como condição necessária para se adotar qualquer instrumento de caráter transnacional.

As observações recolhidas na avaliação de impacto inicial mostraram que as partes interessadas consideram que a resolução das deficiências do atual sistema de auxílio judiciário mútuo o tornaria mais eficaz e aumentaria a segurança jurídica. Algumas organizações da sociedade civil não concordam que seja adotada legislação a nível da UE sobre cooperação direta, preferindo limitar a intervenção da UE à melhoria dos procedimentos em matéria de auxílio jurídico mútuo. Esta ideia será desenvolvida no âmbito das medidas práticas aprovadas pelo Conselho em junho de 2016.

Um inquérito específico efetuado junto das autoridades dos Estados-Membros revelou igualmente que não existe uma abordagem comum para obter acesso transnacional a provas eletrónicas, pois cada Estado-Membro tem a sua própria prática nacional. Os prestadores de serviços também reagem de forma diferente aos pedidos apresentados por autoridades policiais estrangeiras, variando os prazos de resposta consoante o Estado-Membro requerente. Esta situação cria insegurança jurídica para todas as partes interessadas.

Em termos gerais, a consulta das partes interessadas revelou que o enquadramento jurídico em vigor é fragmentado e complexo, podendo originar atrasos durante a fase de execução e tornar as investigações e ações penais pouco eficazes no caso de crimes que requeiram o acesso transnacional a provas eletrónicas.

- **Avaliação de impacto**

O Comité de Controlo da Regulamentação emitiu um parecer positivo sobre a avaliação de impacto subjacente a esta proposta[20], tendo apresentado várias sugestões de melhoria[21]. Na sequência desse parecer, a avaliação de impacto foi alterada de modo a analisar mais aprofundadamente as questões dos direitos fundamentais associadas à partilha transnacional de dados, em especial as ligações entre as várias medidas que fazem parte da opção preferida. A avaliação foi ainda alterada a fim de refletir de forma mais precisa as opiniões das partes interessadas e dos Estados-Membros, assim como a forma como foram tidas em conta. Além disso, o contexto estratégico foi revisto de modo a incluir referências adicionais a vários aspetos como, por exemplo, as análises dos grupos de peritos que ajudaram a configurar a iniciativa. A complementaridade entre as diferentes medidas (nomeadamente, a Diretiva relativa à DEI, as negociações de um protocolo adicional da Convenção de Budapeste e a revisão conjunta do acordo de auxílio jurídico mútuo UE-EUA) foi clarificada em termos de âmbito de aplicação, calendário e profundidade, tendo o cenário de base sido revisto a fim de refletir melhor os desenvolvimentos suscetíveis de ocorrerem, independentemente da adoção das medidas propostas. Por último, foram adicionados fluxogramas que permitem descrever de forma mais exata os fluxos de trabalho quanto à partilha de dados.

Além do cenário de base (opção O), foram analisadas outras quatro opções estratégicas: um conjunto de medidas práticas destinadas a melhorar os procedimentos de cooperação judiciária e a cooperação direta entre as autoridades e os prestadores de serviços (opção A: não-legislativa); uma opção combinando as medidas práticas da opção A com soluções internacionais a nível bilateral ou multilateral (opção B: legislativa); uma opção combinando as medidas da opção B com uma ordem europeia de entrega de provas e uma medida para melhorar o acesso a bases de dados que fornecem informações sobre assinantes, como a informação Whois do Nome de Domínio (opção C: legislativa); e uma opção que combina todas as medidas da opção C com a legislação relativa ao acesso direto a dados armazenados remotamente (opção D: legislativa)[22].

Se não forem adotadas quaisquer medidas (opção O), a situação agravar-se-á em virtude do aumento do número de pedidos apresentados. Todas as outras opções contribuem para a consecução dos objetivos da iniciativa, mas em diferentes graus. A opção A melhoraria a eficiência dos processos atuais, por exemplo, melhorando a qualidade dos pedidos, mas a margem de melhoria seria limitada pelas deficiências estruturais do sistema atual.

A opção B permitiria mais melhorias, proporcionando soluções internacionalmente aceites, mas o resultado destas soluções internacionais dependeria, em larga medida, de países

---

20 Documento de trabalho dos serviços da Comissão – Avaliação de impacto que acompanha a proposta de regulamento relativo às ordens europeias de entrega ou de conservação de provas eletrónicas em matéria penal e a proposta de diretiva que estabelece normas harmonizadas aplicáveis à designação de representantes legais para efeitos de recolha de provas em processo penal, SWD (2018) 118.

21 Comité de Controlo da Regulamentação da União Europeia – Parecer sobre a avaliação de impacto – Proposta de regulamento relativo às ordens europeias de entrega ou de conservação de provas eletrónicas em matéria penal e proposta de diretiva que estabelece normas harmonizadas aplicáveis à designação de representantes legais para efeitos de recolha de provas em processo penal, SEC (2018) 199.

22 Para mais informações, consultar o documento de trabalho dos serviços da Comissão – avaliação de impacto que acompanha a proposta de regulamento relativo às ordens europeias de entrega ou de conservação de provas eletrónicas em matéria penal e a proposta de diretiva que estabelece normas harmonizadas relativas à designação de representantes legais para efeitos de recolha de provas em processo penal, SWD (2018) 118.

terceiros. Estas soluções implicam, portanto, alguma incerteza e poderão não ser tão eficazes nem oferecer tantas salvaguardas como uma solução a nível da União.

A opção C traria claramente valor acrescentado em comparação com as opções anteriores, prevendo ainda um instrumento da UE de cooperação direta com os prestadores de serviços, o qual poderia resolver a maioria das questões identificadas nos casos em que os prestadores de serviços dispõem dos dados requeridos.

A opção D contém o pacote de soluções mais abrangente. Além das medidas anteriores, prevê uma medida legislativa sobre o acesso direto nas situações em que não seja necessário envolver o prestador de serviços.

A presente iniciativa legislativa da Comissão baseia-se nas conclusões da avaliação de impacto e será complementada com as medidas práticas descritas na avaliação de impacto e com o trabalho em curso com vista à elaboração de um protocolo adicional da Convenção de Budapeste. Com base na sua proposta legislativa, a Comissão irá debater igualmente com os EUA e com outros países terceiros a possibilidade de celebrar futuros acordos bilaterais ou multilaterais sobre o acesso transnacional a provas eletrónicas e respetivas salvaguardas. No que se refere às medidas relativas ao acesso direto e ao acesso a bases de dados, que fazem parte da opção D, a Comissão não propõe, de momento, qualquer tipo de legislação, mas pretende refletir sobre o melhor caminho a seguir quanto a estas duas questões.

Espera-se que a iniciativa permita tornar mais eficaz e eficiente a investigação e a ação penal, melhorar a transparência e a responsabilização, assegurando o respeito dos direitos fundamentais. Deve ainda fomentar a confiança no mercado único digital, reforçar a segurança e reduzir a perceção de impunidade para os crimes cometidos através de dispositivos em rede.

No que respeita às autoridades públicas, prevê-se que a iniciativa implique custos iniciais de execução, que, a longo prazo, seriam compensados por economias nos custos recorrentes. As autoridades nacionais teriam de adaptar-se aos novos procedimentos e de receber formação. Contudo, após essa fase, beneficiariam da simplificação e centralização e de um quadro jurídico claro para regulamentar os pedidos de acesso a dados, com os consequentes ganhos de eficiência. De modo idêntico, uma vez que a opção preferida aliviaria a pressão sobre os canais de cooperação judiciária, os países que recebem pedidos deveriam beneficiar de um redução no número de pedidos que devem tratar.

Os prestadores de serviços teriam de adaptar-se ao novo enquadramento legislativo, mediante (novos) procedimentos e formação do seu pessoal. Por outro lado, um quadro harmonizado poderia reduzir os encargos para os prestadores que atualmente devem satisfazer pedidos relativos a dados não relacionados com conteúdos e que devem avaliá-los à luz dos diferentes direitos nacionais dos Estados-Membros. A segurança jurídica e a normalização dos procedimentos teriam igualmente impacto positivo nas pequenas e médias empresas, uma vez que reduziriam os encargos administrativos, favorecendo a competitividade. De um modo geral, a iniciativa também deverá gerar economias de custos para essas empresas.

- **Direitos fundamentais**

A proposta pode afetar vários direitos fundamentais:

- os direitos da pessoa singular cujos dados são acedidos: o direito à proteção dos dados pessoais; o direito ao respeito pela vida privada e familiar; o direito à

liberdade de expressão; os direitos de defesa; o direito à ação e a um tribunal imparcial;

- os direitos do prestador de serviços: o direito à liberdade de empresa; o direito à ação perante um tribunal;

- os direitos dos cidadãos da UE: o direito à liberdade e à segurança.

Tendo em conta o acervo pertinente em matéria de proteção de dados, a proposta de regulamento prevê salvaguardas suficientes e importantes a fim de assegurar a proteção dos direitos dessas pessoas.

Uma vez que este tipo de ordens só pode ser emitido em processos penais e se existirem situações nacionais comparáveis, tanto durante a fase de instrução como durante a fase de julgamento, são aplicáveis todas as salvaguardas processuais previstas no direito penal. Isto inclui, nomeadamente, o direito a um tribunal imparcial consagrado no artigo 6.º da CEDH e nos artigos 47.º e 48.º da Carta dos Direitos Fundamentais, bem como a legislação aplicável ao nível da UE em matéria de direitos processuais em processo penal, nomeadamente: a Diretiva 2010/64/UE relativa ao direito à interpretação e tradução em processo penal, a Diretiva 2012/13/UE relativa ao direito à informação em processo penal, a Diretiva 2013/48/UE relativa ao direito de acesso a um advogado em processo penal e nos processos de execução de mandados de detenção europeus, a Diretiva (UE) 2016/343 relativa ao reforço de certos aspetos da presunção de inocência e do direito de comparecer em julgamento em processo penal, a Diretiva (UE) 2016/800 relativa a garantias processuais para os menores suspeitos ou arguidos em processo penal e a Diretiva (UE) 2016/1919 relativa ao apoio judiciário para suspeitos e arguidos em processo penal e para as pessoas procuradas em processos de execução de mandados de detenção europeus.

Mais especificamente, a intervenção prévia de uma autoridade judicial no momento da emissão de uma ordem assegura que foram verificadas a legalidade da medida e a sua necessidade e proporcionalidade ao processo em causa. Esta intervenção assegura igualmente que o pedido não prejudica indevidamente os direitos fundamentais, nomeadamente o respeito pelos princípios de direito, como o sigilo profissional advogado-cliente. A autoridade emissora é obrigada a assegurar, no caso concreto, que a medida é necessária e proporcionada, nomeadamente, tendo em conta a gravidade da infração sob investigação. A proposta também inclui limiares para os dados transacionais e de conteúdo, garantindo que a ordem europeia de entrega de provas só poderá ser usada para formas mais graves de criminalidade, no que respeita a esses dados.

O direito a vias de recurso efetivo por parte das pessoas cujos dados são solicitados também está explicitamente previsto. As imunidades e os privilégios de certos profissionais, como os advogados, assim como os interesses fundamentais de segurança ou de defesa nacional no Estado do destinatário, devem igualmente ser tidos em consideração durante o julgamento no Estado de emissão. O reexame por uma autoridade judicial funciona como uma salvaguarda adicional nesta matéria.

Uma vez que a ordem é uma medida vinculativa, afeta igualmente os direitos dos prestadores de serviços, nomeadamente a liberdade de empresa. A proposta reconhece aos prestadores de serviços o direito de formularem certas reivindicações junto do Estado-Membro de emissão, por exemplo, quando a ordem não tenha sido emitida ou validada por uma autoridade judicial. Se a ordem for transmitida para execução coerciva pelo Estado de execução, a autoridade responsável pela execução poderá decidir, após consulta da autoridade emissora, não

reconhecer ou executar a mesma se, após a sua receção, considerar que se aplica um dos fundamentos limitados de oposição. Além disso, caso seja iniciado o procedimento de execução coerciva, o próprio destinatário poderá opor-se à ordem perante a autoridade de execução, com base em qualquer desses fundamentos limitados. Tal inclui, por exemplo, os casos em que seja notório que a ordem não foi emitida ou validada por uma autoridade competente ou nos quais o cumprimento violaria manifestamente a Carta ou seria manifestamente abusivo. Contudo, esta disposição não exclui o direito do destinatário à ação judicial contra uma decisão que lhe imponha uma sanção.

Uma eventual questão relacionada com as medidas da União neste domínio é a possibilidade de estas medidas poderem contribuir para a introdução, por países terceiros, de obrigações recíprocas para os prestadores de serviços europeus que sejam incompatíveis com os direitos fundamentais da União, nomeadamente o elevado nível de proteção de dados assegurado pelo acervo da UE. A proposta aborda esta situação de duas formas: em primeiro lugar, prevê uma medida que contempla garantias sólidas e referências explícitas às condições e salvaguardas já inerentes ao acervo da UE, servindo assim de modelo para a legislação estrangeira; em segundo lugar, prevê uma cláusula específica relativa a «conflitos de obrigações» permitindo aos prestadores de serviços identificar obrigações que sejam contraditórias, originando assim um reexame jurisdicional. Esta cláusula destina-se a assegurar quer a observância das disposições gerais de bloqueio como, por exemplo, a Lei dos EUA relativa à privacidade das comunicações eletrónicas (*Electronic Communications Privacy Act* – ECPA), que proíbe a divulgação de dados de conteúdo dentro do seu âmbito de aplicação geográfico, exceto em circunstâncias limitadas, quer a observância de legislações que normalmente não proíbem a divulgação, mas podem fazê-lo em casos específicos. Atualmente, nos casos relativos à ECPA, o acesso a dados de conteúdo poderá ser impedido em determinadas situações, pelo que o auxílio judiciário mútuo deverá continuar a ser o principal instrumento de acesso a esses dados. No entanto, com as alterações introduzidas com a adoção da Lei CLOUD dos EUA[23], a disposição de bloqueio pode ser revogada se a UE celebrar um acordo com este país. Outros acordos internacionais com outros parceiros essenciais podem reduzir ainda mais as situações de conflito de leis.

Tendo em conta o acima exposto, as medidas constantes da presente proposta respeitam os direitos fundamentais.

4. INCIDÊNCIA ORÇAMENTAL

A proposta legislativa não tem incidência no orçamento da União.

5. OUTROS ELEMENTOS

- **Planos de execução e mecanismos de acompanhamento, de avaliação e de informação**

O regulamento é diretamente aplicável pelos profissionais na União, sem que seja necessário alterar os sistemas jurídicos nacionais.

[23] Em 23 de março de 2018, foi adotada pelos Estados Unidos a *Clarifying Lawful Overseas Use of Data* (CLOUD) Act. A referida lei pode ser consultada aqui.

O regulamento será avaliado e a Comissão apresentará um relatório ao Parlamento Europeu e ao Conselho, o mais tardar, cinco anos após a sua entrada em vigor. Com base nas conclusões desse relatório, nomeadamente se o regulamento não preencher lacunas que sejam importantes na prática, e tendo em conta a evolução tecnológica, a Comissão avaliará a necessidade de alargar o seu âmbito de aplicação e, se for caso disso, apresentará propostas para a sua adaptação. Os Estados-Membros transmitirão à Comissão todas as informações necessárias para a elaboração do relatório e recolherão os dados necessários para o acompanhamento anual da aplicação do regulamento.

Se necessário, a Comissão emitirá orientações para os prestadores de serviços cumprirem as obrigações decorrentes do regulamento.

- **Explicação pormenorizada das disposições específicas da proposta**

	REGULAMENTO	
	Artigo	**Considerando**
I. Objeto, definições e âmbito de aplicação	1. Objeto	1-15
	2. Definições	16-23
	3. Âmbito de aplicação	24-27
II. Ordem europeia de entrega de provas, ordem europeia de conservação de provas e respetivos certificados, representante legal	4. Autoridade emissora	30
	5. Condições de emissão de uma ordem europeia de entrega de provas	28-29, 31-35
	6. Condições de emissão de uma ordem europeia de conservação de provas	36
	7. Destinatário da ordem europeia de entrega de provas ou da ordem europeia de conservação de provas	37
	8. Certificado de ordem europeia de entrega de provas e certificado de ordem europeia de conservação de provas	38-39
	9. Execução do certificado de ordem europeia de entrega de provas	40-41
	10. Execução do certificado de ordem europeia de conservação de provas (COECP)	42
	11. Confidencialidade e informação do utilizador	43
	12. Reembolso dos custos incorridos	Não aplicável

III. Sanções e execução coerciva	13. Sanções	Não aplicável
	14. Procedimento de execução coerciva	44-45, 55
IV. Vias de recurso	15.º e 16.º Procedimento de reexame em caso de obrigações contraditórias decorrentes do direito de um país terceiro	47-53
	17. Vias de recurso efetivo	54
	18. Garantia dos privilégios e imunidades reconhecidos pelo Estado de execução	35
V. Disposições finais	19. Acompanhamento e divulgação de informações sobre a aplicação	58
	20. Alterações aos certificados e aos formulários	59-60
	21. Exercício da delegação	60
	22. Notificações	Não aplicável
	23. Relação com as decisões europeias de investigação	61
	24. Avaliação	62
	25. Entrada em vigor	Não aplicável

Capítulo 1: Objeto, definições e âmbito de aplicação

Artigo 1.º: Objeto

Este artigo define o âmbito de aplicação geral e o objetivo da proposta, que consiste em estabelecer as normas segundo as quais uma autoridade judicial competente na União Europeia pode, através de uma ordem europeia de entrega de provas ou de uma ordem europeia de conservação de provas, ordenar a um prestador de serviços que opere na União que entregue ou conserve provas eletrónicas. Estes instrumentos só podem ser utilizados em situações transnacionais, ou seja, em situações em que o prestador de serviços esteja estabelecido ou representado noutro Estado-Membro.

O regulamento deve prever instrumentos adicionais para que as autoridades responsáveis pelas investigações obtenham provas eletrónicas, sem limitar as competências já previstas pelo direito nacional para obrigar os prestadores de serviços estabelecidos ou representados no seu território a cumprirem as disposições aplicáveis. Se o prestador de serviços estiver estabelecido ou representado no mesmo Estado-Membro, as autoridades desse Estado-Membro devem, por conseguinte, recorrer a medidas nacionais para o obrigar a cumprir as disposições aplicáveis.

Os dados solicitados através de uma ordem europeia de entrega de provas devem ser fornecidos diretamente às autoridades, sem envolver as autoridades do Estado-Membro no qual o prestador de serviços estiver estabelecido ou representado. O regulamento também não considera a localização dos dados como um fator de ligação determinante, já que o armazenamento de dados, normalmente, não implica qualquer controlo pelo Estado em cujo território estes são armazenados. Na maioria dos casos, esse armazenamento é decidido exclusivamente pelo prestador de serviços, com base em considerações de natureza comercial[24].

Além disso, o regulamento também se aplica se os prestadores de serviços não estiverem estabelecidos ou representados na União, mas prestarem serviços na União. Esta disposição encontra-se refletida no artigo 3.º, n.º 1.

Quando a proposta se refere a um prestador de serviços estabelecido ou representado num Estado-Membro através de um representante legal nomeado, a simples designação desse representante não cria um estabelecimento do prestador de serviços para efeitos do regulamento.

O disposto no artigo 1.º, n.º 2, do regulamento não tem por efeito alterar a obrigação de respeitar os direitos fundamentais e os princípios jurídicos consagrados no artigo 6.º do TUE.

Artigo 2.º: Definições

Este artigo contém as definições aplicáveis no âmbito do regulamento.

Os seguintes tipos de prestadores de serviços são abrangidos pelo âmbito de aplicação do regulamento: prestadores de serviços de comunicações eletrónicas, prestadores de serviços da sociedade da informação para os quais o armazenamento de dados seja uma componente determinante do serviço prestado ao utilizador, incluindo as redes sociais (na medida em que não sejam consideradas serviços de comunicações eletrónicas), mercados em linha que facilitam transações entre os seus utilizadores (consumidores ou empresas) e outros prestadores de serviços de alojamento, e os prestadores de serviços de Internet como nomes de domínio e recursos de numeração.

O regulamento abrange os prestadores de serviços de comunicações eletrónicas, tais como definidos [na Diretiva que estabelece o Código Europeu das Comunicações Eletrónicas]. Os consumidores e as empresas dependem cada vez mais de novos serviços baseados na Internet que permitem comunicações interpessoais, tais como voz sobre IP, mensagens instantâneas e serviços de correio eletrónico, em detrimento dos serviços de comunicações tradicionais. Esses serviços, juntamente com redes sociais como o Twitter e o Facebook (que permitem a partilha de conteúdos entre os utilizadores), devem, portanto, ser abrangidos pela presente proposta.

Em muitos casos, os dados já não são armazenados num dispositivo do utilizador, mas sim disponibilizados numa infraestrutura localizada na nuvem, permitindo, em princípio, o acesso aos mesmos a partir de qualquer lugar. Os prestadores de serviços não precisam de estar estabelecidos ou de ter servidores nas diferentes jurisdições, recorrendo a uma administração centralizada e a sistemas descentralizados para armazenar os dados e prestar os serviços. Esta solução permite-lhes otimizar o equilíbrio da carga e reduzir os atrasos na resposta aos

[24] A avaliação de impacto contém explicações suplementares.

pedidos de dados enviados pelos utilizadores. Geralmente, são implantadas redes de distribuição de conteúdos para agilizar a distribuição dos mesmos, copiando-os para vários servidores em todo o mundo. Esta abordagem permite que as empresas exibam conteúdos a partir do servidor que estiver mais próximo do utilizador ou que possam encaminhar a comunicação através de uma rede menos congestionada. Por forma a ter em conta esse desenvolvimento, a definição abrange os serviços de alojamento na nuvem e outros serviços que fornecem uma variedade de recursos informáticos, como redes, servidores ou outras infraestruturas, armazenamento, aplicações e serviços que possibilitam o armazenamento de dados para diferentes finalidades. O instrumento também se aplica aos mercados digitais que permitem que os consumidores e/ou as empresas executem transações através de contratos de serviços ou vendas em linha. Tais transações são realizadas no sítio Web do mercado em linha ou de um comerciante que utilize serviços informáticos fornecidos pelo mercado em linha. Por conseguinte, é o mercado em linha que está na posse de provas eletrónicas que poderão ser necessárias no decurso de um processo penal.

Os serviços para os quais o armazenamento de dados não é uma componente determinante não são abrangidos pela proposta. Embora a maioria dos serviços prestados pelos prestadores envolva algum tipo de armazenamento de dados, nomeadamente quando são serviços em linha prestados à distância, é possível identificar vários serviços em que o armazenamento de dados não constitui a característica principal, assumindo apenas uma natureza auxiliar, nomeadamente serviços jurídicos, de arquitetura, de engenharia e de contabilidade prestados em linha, à distância.

Os dados na posse dos prestadores de serviços de infraestruturas da Internet, como agentes de registo e registos de nomes de domínio e prestadores de serviços de privacidade e de proxy, ou registos regionais da Internet para endereços de protocolo Internet («IP»), podem ser relevantes em matéria penal, pois podem fornecer indícios que permitam identificar uma pessoa singular ou uma entidade envolvida em atividades criminosas.

As categorias de dados que podem ser obtidos com uma ordem europeia de entrega de provas emitida pelas autoridades competentes incluem dados de assinantes, dados de acesso, dados transacionais (as três categorias normalmente designadas conjuntamente por «dados não relacionados com conteúdos») e dados de conteúdo armazenados. Esta distinção, com exceção dos dados de acesso, existe nas ordens jurídicas de muitos Estados-Membros e mesmo em enquadramentos jurídicos fora da UE.

Todas as categorias contêm dados pessoais, sendo, por conseguinte, abrangidas pelas salvaguardas previstas no acervo da UE em matéria de proteção de dados. O impacto em termos de direitos fundamentais varia consoante as categorias, em especial, entre os dados de assinantes, por um lado, e os dados transacionais e de conteúdo, por outro. É essencial que todas estas categorias sejam abrangidas pelo instrumento: os dados de acesso e de assinantes são frequentemente o ponto de partida para encontrar indícios numa investigação sobre a identidade de um suspeito, embora os dados transacionais e de conteúdo possam ser os mais relevantes como material probatório. Dados os diferentes níveis de interferência nos direitos fundamentais, justifica-se a inclusão de condições diferentes quanto aos dados de assinantes, por um lado, e quanto aos dados transacionais e de conteúdo, por outro, como sucede em várias disposições do regulamento.

Importa destacar os dados de acesso como uma categoria de dados específica utilizada no regulamento. Os dados de acesso, conforme definidos no regulamento, são solicitados para o mesmo objetivo que os dados de assinantes, ou seja, para identificar o utilizador, sendo o seu

nível de interferência com os direitos fundamentais semelhante. Por conseguinte, devem ser sujeitos às mesmas condições que os dados de assinantes. A proposta introduz assim uma nova categoria de dados, que deve ser tratada como dados de assinantes, caso seja prosseguido o mesmo objetivo.

O artigo 2.º define os Estados-Membros e as autoridades que podem participar no processo. O artigo 4.º contém a definição de autoridade emissora.

Os casos urgentes são situações excecionais que exigem normalmente uma reação em tempo útil da parte dos prestadores de serviços e em relação aos quais se aplicam condições especiais. Por conseguinte, serão definidos separadamente neste artigo.

Artigo 3.º: Âmbito de aplicação

Este artigo estabelece o âmbito de aplicação da proposta. O regulamento aplica-se a todos os prestadores de serviços que operam na União, incluindo aqueles que não estejam estabelecidos na União. A oferta ativa de serviços na União, com todas as vantagens daí decorrentes, justifica que estes prestadores de serviços sejam igualmente sujeitos ao regulamento, criando condições equitativas entre os participantes nos mesmos mercados. Além disso, a não inclusão desses prestadores de serviços criaria uma lacuna e tornaria mais fácil aos criminosos contornar o âmbito de aplicação do regulamento.

Por forma a verificar se são ou não prestados serviços, as autoridades devem verificar se o prestador permite que pessoas singulares ou coletivas de um ou vários Estados-Membros utilizem os seus serviços. No entanto, a mera acessibilidade do serviço (que também pode resultar da acessibilidade do sítio Web do prestador de serviços, de um intermediário, de um endereço de correio eletrónico e de outras informações de contacto) não deve ser considerada condição suficiente para a aplicação do regulamento. Por conseguinte, é necessária uma ligação significativa a esses Estados-Membros para confirmar que existe uma conexão suficientemente forte entre o prestador e o território onde presta os serviços. Essa ligação significativa existe sempre que um prestador de serviços tenha um estabelecimento num ou vários Estados-Membros. Caso o prestador de serviços não tenha qualquer estabelecimento na União, o critério de ligação significativa à União deve ser avaliado em função da existência de um número significativo de utilizadores num ou vários Estados-Membros ou na orientação das suas atividades para um ou vários Estados-Membros. Esta orientação pode ser determinada com base em todas as circunstâncias relevantes, incluindo fatores como a utilização de uma língua ou de uma moeda geralmente utilizada num Estado-Membro. A orientação das atividades para um determinado Estado-Membro também pode resultar da disponibilização de uma aplicação na loja de aplicações nacional pertinente, da divulgação de publicidade local ou na língua utilizada nesse Estado-Membro, da utilização de todas as informações provenientes de pessoas localizadas em Estados-Membros no decurso das suas atividades, ou da gestão das relações com os clientes, por exemplo, através da prestação de serviços aos clientes na língua geralmente utilizada no Estado-Membro. Deve considerar-se igualmente que existe uma ligação significativa quando um prestador de serviços dirige as suas atividades para um ou vários Estados-Membros, conforme estabelecido no artigo 17.º, n.º 1, alínea c), do Regulamento 1215/2012 relativo à competência judiciária, ao reconhecimento e à execução de decisões em matéria civil e comercial.

A ordem europeia de entrega de provas e a ordem europeia de conservação de provas são medidas de investigação que só podem ser emitidas em investigações ou processos penais relativos a infrações penais específicas. A ligação a uma investigação específica distingue

essas ordens das medidas preventivas ou das obrigações de retenção de dados estabelecidas por lei, assegurando a aplicação dos direitos processuais aplicáveis aos processos penais. A competência para iniciar uma investigação quanto a uma infração específica constitui, portanto, um pré-requisito para a aplicação do regulamento.

Como requisito adicional, os dados solicitados devem estar relacionados com os serviços prestados pelo prestador de serviços na União.

Capítulo 2: Ordem europeia de entrega de provas, ordem europeia de conservação de provas e respetivos certificados

Artigo 4.º: Autoridade emissora

Quando é emitida uma ordem europeia de entrega ou de conservação de provas, deve ser sempre envolvida no processo uma autoridade judicial, na qualidade de autoridade emissora ou de validação. No caso de ordens de entrega de dados transacionais e de conteúdo, é necessária a intervenção de um juiz ou de um tribunal. A entrega de dados de assinantes ou de acesso poderá ser levada acabo igualmente por magistrados do Ministério Público.

Artigo 5.º: Condições de emissão de uma ordem europeia de entrega de provas

O artigo 5.º estabelece as condições de emissão de uma ordem europeia de entrega de provas, as quais devem ser avaliadas pela autoridade judicial emissora.

A ordem europeia de entrega de provas só pode ser emitida se for necessária e proporcionada ao processo em apreço. Além disso, só pode ser emitida se existir uma medida semelhante para a mesma infração penal numa situação nacional comparável no Estado de emissão.

As ordens de entrega de dados de assinantes e de dados de acesso podem ser emitidas para qualquer infração penal. Os dados transacionais e de conteúdo devem ser sujeitos a requisitos mais rigorosos, de modo a refletir a sua natureza mais sensível e, consequentemente, o grau de intrusão mais elevado das ordens relativas a esses dados, comparativamente com os dados de assinantes e de acesso. Por conseguinte, as ordens só podem ser emitidas no caso de infrações puníveis com uma pena privativa de liberdade de duração máxima não inferior a três anos. A fixação de um limiar baseado numa pena privativa de liberdade de duração máxima permite uma abordagem mais proporcionada, juntamente com várias outras condições *ex ante* e *ex post* e salvaguardas, a fim de garantir o respeito da proporcionalidade e dos direitos das pessoas afetadas.

Ao mesmo tempo, esse limiar não deve comprometer a eficácia do instrumento e a sua utilização pelos profissionais da justiça. Os Estados-Membros aplicam penas de duração máxima de acordo com os respetivos sistemas nacionais. Os códigos penais nacionais variam de país para país, não havendo qualquer harmonização. É o que sucede com as infrações penais e das sanções que lhes são aplicáveis. Os códigos processuais nacionais também diferem em relação aos limiares para a obtenção de dados transacionais ou de conteúdo: alguns Estados-Membros não estabelecem qualquer limiar específico; outros preveem uma lista de infrações. Um limiar de três anos limita o âmbito de aplicação do instrumento aos crimes mais graves, sem limitar excessivamente as possibilidades da sua utilização pelos profissionais da justiça. Este limiar exclui do âmbito de aplicação do regulamento uma vasta gama de crimes, consoante o disposto no código penal do Estado-Membro (por exemplo, em alguns Estados-Membros, a participação em atividades de um grupo criminoso organizado ou num rapto, mas também infrações como pequenos furtos, fraudes e assaltos, para os quais

pode ser considerada desproporcionado recorrer a uma ordem de entrega de provas transnacional para obter dados mais sensíveis). Por outro lado, o limiar de três anos abrange crimes que exigem uma abordagem mais eficaz, como a participação numa organização criminosa, o financiamento de grupos terroristas, o apoio ou a publicidade a uma organização criminosa, a formação para a prática de crimes terroristas, certas infrações cometidas com intenção terrorista e a preparação de uma infração com intenção terrorista ou a preparação de tomada de reféns, que de outra forma seriam excluídos se fosse aplicado um limiar mais alto, consoante a legislação do Estado-Membro. Este limiar foi escolhido para garantir um equilíbrio entre a eficiência das investigações penais e a proteção dos direitos e da proporcionalidade em todos os Estados-Membros. Tem também a vantagem de ser facilmente aplicável na prática.

Além disso, também podem ser emitidas ordens de entrega de dados transacionais ou de conteúdo quanto a infrações específicas harmonizadas enumeradas na disposição em relação às quais as provas normalmente estejam disponíveis, na sua maioria, apenas em formato eletrónico. Tal justifica a aplicação do regulamento também nos casos em que as infrações sejam puníveis com uma pena privativa de liberdade de duração máxima inferior ao limiar acima indicado; caso contrário, essas infrações não poderiam ser investigadas adequadamente, o que poderia levar à impunidade. As infrações são objeto das disposições específicas seguintes: i) Decisão-quadro do Conselho 2001/413/JAI, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário, ii) Diretiva 2011/92/UE relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, e que substitui a Decisão-Quadro 2004/68/JAI do Conselho, e iii) Diretiva 2013/40/UE relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho. Podem também ser emitidas ordens para as infrações enumeradas na Diretiva 2017/541/UE relativa à luta contra o terrorismo e que substitui a Decisão-Quadro 2002/475/JAI do Conselho e altera a Decisão 2005/671/JAI do Conselho. Algumas destas infrações têm limiares máximos de, no mínimo, um ano, outras de dois anos, mas nenhuma delas tem limiares máximos inferiores a um ano.

O artigo estabelece igualmente as informações obrigatórias que devem constar da ordem europeia de entrega de provas, a fim de permitir ao prestador de serviços identificar e facultar os dados solicitados. A fundamentação da necessidade e da proporcionalidade desta medida deve integrar igualmente a ordem europeia de entrega de provas.

A ordem europeia de entrega de provas é executada mediante a emissão de um certificado de ordem europeia de entrega de provas (COEEP) (ver artigo 8.º), que deve ser traduzido e enviado ao prestador de serviços. O certificado deve conter as mesmas informações obrigatórias que constam da ordem, salvo a fundamentação da necessidade e da proporcionalidade da medida e outros pormenores do processo.

Quando os dados solicitados sejam armazenados ou tratados como parte de uma infraestrutura fornecida por um prestador de serviços a uma empresa, normalmente no caso de serviços de alojamento ou de *software*, a própria empresa deve ser a principal destinatária do pedido das autoridades de investigação. Caso a empresa não seja um prestador de serviços abrangido pelo âmbito de aplicação do regulamento, poderá ser necessário recorrer a uma decisão europeia de investigação ou a um pedido de auxílio judiciário mútuo. O prestador de serviços só poderá ser notificado da ordem europeia de entrega de provas se não for conveniente notificar o pedido à empresa, sobretudo quando a notificação possa comprometer a investigação, por exemplo, quando a própria empresa está sob investigação.

Antes de emitir uma ordem europeia de entrega de provas, a autoridade emissora deve ter igualmente em conta as imunidades e os privilégios que possam estar previstos no direito do Estado-Membro do prestador de serviços ou qualquer impacto nos interesses fundamentais desse Estado-Membro, como a sua segurança e a defesa nacional. Esta disposição tem por objetivo garantir que as imunidades e os privilégios que protegem os dados solicitados no Estado-Membro do prestador de serviços sejam tidos em conta no Estado de emissão, nomeadamente quando preveem uma proteção mais elevada do que o direito do Estado de emissão.

Artigo 6.º: Condições de emissão de uma ordem europeia de conservação de provas

A ordem europeia de conservação de provas está sujeita a condições semelhantes à ordem europeia de entrega de provas, podendo ser emitida para qualquer infração em conformidade com as restantes condições fixadas no artigo 6.º. O seu objetivo é impedir a remoção, eliminação ou alteração de dados pertinentes em situações em que a obtenção desses dados possa ser mais morosa, por exemplo, quando são utilizados canais de cooperação judiciária. Tendo em conta que uma DEI pode normalmente ser emitida para qualquer infração sem que seja imposto qualquer limiar, a ordem europeia de conservação de provas também não será objeto de qualquer limitação. Caso contrário, este instrumento não seria eficaz. A fim de permitir às autoridades de investigação intervir rapidamente e dado que o pedido relevante para obter os dados será o pedido subsequente, em que todas as condições serão novamente analisadas, as ordens europeias de conservação de provas também podem ser emitidas ou validadas por um magistrado do Ministério Público.

Artigo 7.º: Destinatário da ordem europeia de entrega de provas ou da ordem europeia de conservação de provas

As ordens europeias de entrega de provas e as ordens europeias de conservação de provas devem ser notificadas ao representante legal nomeado pelo prestador de serviços para fins de recolha de provas em processos penais, em conformidade com a Diretiva que estabelece normas harmonizadas relativas à designação de representantes legais para efeitos de recolha de provas em processo penal. A transmissão deve ser efetuada sob a forma de um certificado de ordem europeia de entrega de provas (COEEP) ou de um certificado de ordem europeia de conservação de provas (COECP), como previsto no artigo 8.º. O representante legal será responsável pela sua receção e execução completa em tempo útil, o que permite aos prestadores de serviços escolherem o modo como se organizam para facultar os dados solicitados pelas autoridades dos Estados-Membros.

Caso não tenha sido nomeado um representante legal, as ordens podem ser notificadas a qualquer estabelecimento do prestador de serviços na União. Esta solução de recurso serve para garantir a eficácia do sistema, caso o prestador de serviços (ainda) não tenha nomeado um representante específico, por exemplo, quando não exista a obrigação de nomear um representante legal em conformidade com a diretiva, porque os prestadores de serviços estão estabelecidos e atuam apenas num Estado-Membro, ou nos casos em que ainda não esteja em vigor a obrigação de nomear um representante legal, antes de terminar o prazo de transposição da diretiva.

Em caso de incumprimento pelo representante legal, existem duas situações em que a autoridade emissora se pode dirigir a qualquer estabelecimento do prestador de serviços na União: nas situações de urgência, tal como definidas no artigo 9.º, n.º 2, e nos casos em que o

representante legal não cumpra as obrigações que lhe incumbem por força dos artigos 9.º e 10.º e em que a autoridade emissora considere existirem riscos claros de perda de dados.

Artigo 8.º: Certificados de ordem europeia de entrega de provas ou de conservação de provas

O COEEP e o COECP destinam-se a transmitir as ordens ao destinatário referido no artigo 7º. Os modelos de ambos os certificados constam dos anexos I e II do regulamento, devendo ser traduzidos para uma das línguas oficiais do Estado-Membro em que o destinatário esteja estabelecido. O prestador de serviços pode declarar que aceita igualmente as ordens redigidas noutras línguas oficiais da União. Os certificados têm por objetivo fornecer todas as informações necessárias a transmitir ao destinatário num formato normalizado, por forma a minimizar eventuais erros, permitir uma fácil identificação dos dados e evitar, tanto quanto possível, o texto livre e, consequentemente, reduzir os custos de tradução. A fundamentação completa quanto à necessidade e à proporcionalidade ou outras informações sobre o processo não devem ser incluídas no certificado, a fim de não comprometer as investigações. Estas informações só devem ser incluídas na ordem, de modo a que, posteriormente, o suspeito as possa contestar no âmbito do processo penal.

Alguns prestadores de serviços já criaram plataformas para a transmissão de pedidos por parte das autoridades policiais. O regulamento não deve impedir a utilização dessas plataformas, uma vez que apresentam muitas vantagens, incluindo a possibilidade de transmissão segura dos dados e de autenticação fácil. No entanto, estas plataformas devem permitir a apresentação do COEEP e do COECP no formato previsto nos anexos I e II, sem solicitar quaisquer dados adicionais quanto à ordem.

As plataformas criadas pelos Estados-Membros ou pelos organismos da União podem igualmente proporcionar meios seguros de transmissão e facilitar a autenticação das ordens e a recolha de dados estatísticos. Deverá ser ponderada a eventual expansão das plataformas eCodex e SIRIUS por forma a incluir uma ligação segura aos prestadores de serviços para efeitos de notificação do COEEP e do COECP e, quando apropriado, para a transmissão das respostas dos prestadores de serviços.

Artigo 9.º: Execução do certificado de ordem europeia de entrega de provas

O artigo 9.º obriga os destinatários a responder aos COEEP e introduz prazos obrigatórios. O prazo normal é de dez dias, embora as autoridades possam fixar um prazo mais curto, quando justificado. Além disso, em situações de urgência, definidas como as situações em que exista uma ameaça iminente à vida ou à integridade física de uma pessoa ou de uma infraestrutura crítica, o prazo é de seis horas.

Esta disposição assegura igualmente a possibilidade de diálogo entre o destinatário e a autoridade emissora. Se o COEEP estiver incompleto, manifestamente incorreto ou não contiver informação suficiente para permitir a sua execução pelo prestador de serviços, o destinatário deve contactar a autoridade emissora e solicitar esclarecimentos, utilizando o formulário constante do anexo III. Deve ainda informar a autoridade emissora quando não possa fornecer os dados por motivos de força maior ou devido a uma impossibilidade de facto, por exemplo, se a pessoa cujos dados são solicitados não for cliente do serviço ou se (por exemplo, devido a outras obrigações de privacidade) os dados tiverem sido legitimamente eliminados pelo prestador de serviços antes de este (ou o seu representante legal) ter recebido a ordem. A autoridade emissora deverá ter conhecimento dessas circunstâncias para poder reagir rapidamente e tentar obter as provas eletrónicas junto de

outro prestador de serviços, evitando assim iniciar um procedimento de execução coerciva quando tal não faria sentido.

Se o destinatário não fornecer a informação, ou não a fornecer de forma exaustiva ou em tempo útil por motivos diferentes dos acima mencionados, deve comunicar esse motivos à autoridade emissora através do formulário constante do anexo III. Os destinatários podem, pois, suscitar qualquer questão relacionada com a execução do COEEP junto da autoridade emissora, permitindo que esta corrija ou reconsidere o COEEP numa fase inicial, antes da fase de execução coerciva.

Se os dados não forem imediatamente transmitidos, nomeadamente quando se encete um diálogo entre o destinatário e a autoridade emissora (o que significa que os prazos do artigo 9.º, n.º 1, já não serão cumpridos), o prestador de serviços deve, após receber o COEEP, conservar os dados a fim de evitar a sua perda, desde que os mesmos possam ser identificados. Os dados devem ser conservados tendo em vista a sua eventual transmissão em virtude do COEEP corrigido ou de um pedido subsequente no âmbito de uma decisão europeia de investigação ou de um procedimento de auxílio judiciário mútuo que possam ser enviados em substituição do certificado inicial.

Artigo 10.º: Execução do certificado de ordem europeia de conservação de provas (COECP)

A execução de um COECP obriga a conservar os dados disponíveis aquando da receção da ordem. Os prestadores de serviços devem conservar os dados durante o período de tempo necessário para serem facultados, mediante pedido, desde que a autoridade emissora confirme, no prazo de 60 dias após a emissão da ordem, que emitiu o pedido de entrega de dados subsequente. Este processo exige que sejam adotadas, pelo menos, algumas medidas formais, como o envio de um pedido de auxílio judiciário mútuo para efeitos de tradução.

Por outro lado, os pedidos de conservação de dados só devem ser apresentados ou mantidos durante o período de tempo necessário para permitir o envio de um pedido subsequente de entrega desses dados. Para evitar que os dados sejam conservados desnecessariamente ou por períodos de tempo excessivamente longos, a autoridade que emitiu a ordem europeia de conservação de provas deve informar o destinatário logo que seja tomada a decisão de não emitir ou de retirar uma ordem de entrega de provas ou um pedido de cooperação judiciária.

Esta disposição assegura igualmente a possibilidade de diálogo entre o destinatário e a autoridade emissora, em condições idênticas às definidas no artigo 9.º. Se o COECP estiver incompleto, manifestamente incorreto ou não contiver informação suficiente para permitir a sua execução pelo prestador de serviços, o destinatário deve contactar a autoridade emissora e solicitar esclarecimentos, utilizando o formulário constante do anexo III. Deve ainda informar a autoridade emissora quando não possa fornecer os dados por motivos de força maior ou devido a uma impossibilidade de facto.

Artigo 11.º: Confidencialidade e informação do utilizador

Deve ser protegida a confidencialidade das investigações em curso, incluindo o facto de ter sido emitida uma ordem de entrega dos dados pertinentes. Este artigo inspira-se no artigo 19.º da Diretiva relativa à DEI. Prevê a obrigação de o destinatário e, se for caso disso, o prestador de serviços preservarem a confidencialidade do COEEP ou do COECP, nomeadamente abstendo-se de informar a pessoa cujos dados sejam solicitados, a pedido da autoridade emissora, a fim de salvaguardar a investigação de infrações penais, em conformidade com o artigo 23.º do Regulamento geral sobre a proteção de dados.

Por outro lado, é importante, nomeadamente para o exercício de vias de recurso, que a pessoa cujos dados foram solicitados seja informada. Se tal não for feito pelo prestador de serviços, a pedido da autoridade emissora, esta deverá informar a pessoa nos termos do artigo 13.º da Diretiva sobre a proteção de dados na aplicação da lei, assim que deixar de existir o risco de comprometer a investigação, incluindo informação sobre as vias de recurso disponíveis. Devido à menor interferência com os direitos envolvidos, não é necessário informar o utilizador no caso de uma ordem europeia de conservação de provas mas apenas no caso de uma ordem europeia de entrega de provas.

Artigo 12.º: Reembolso dos custos incorridos

O prestador de serviços pode reclamar junto do Estado de emissão o reembolso dos custos em que tenha incorrido, desde que tal esteja previsto no direito nacional desse Estado relativamente a ordens nacionais emitidas em situações semelhantes, em conformidade com o direito nacional. Esta disposição garante a igualdade de tratamento entre os prestadores de serviços destinatários de uma ordem nacional e os destinatários de um COEEP do mesmo Estado-Membro, se este tiver decidido reembolsar determinados prestadores de serviços. Por outro lado, o regulamento proposto não harmoniza o reembolso dos custos, uma vez que os Estados-Membros fizeram escolhas divergentes a esse respeito.

Os custos podem ser reclamados diretamente pelo prestador de serviços ou pelo seu representante legal, só podendo ser reembolsados uma única vez.

Capítulo 3: Sanções e execução coerciva

Artigo 13º: Sanções

Os Estados-Membros devem assegurar a aplicação de coimas efetivas, proporcionadas e dissuasoras, sempre que os prestadores de serviços não cumpram as obrigações que lhes incumbem por força dos artigos 9.º, 10.º ou 11.º. Esta disposição não prejudica as disposições do direito nacional que prevejam a imposição de sanções penais para tais situações.

Artigo 14º: Procedimento de execução coerciva

O artigo 14.º prevê um procedimento para a execução coerciva das ordens em caso de incumprimento, com a ajuda do Estado-Membro em que o destinatário do certificado transmitido estiver situado. Consoante o destinatário inicial, trata-se do Estado-Membro do prestador de serviços ou do Estado-Membro do representante legal. A autoridade emissora deve transferir a ordem completa, incluindo a fundamentação quanto à necessidade e proporcionalidade, juntamente com o certificado, para a autoridade competente do Estado de execução, que a executará coercivamente em conformidade com o direito nacional, aplicando, se for caso disso, as sanções previstas no artigo 13.º. Se a ordem for transmitida para ser executada coercivamente pelo Estado de execução, a autoridade de execução poderá decidir não a reconhecer ou executar caso, após a receção da mesma, considerar que se aplica um dos fundamentos limitados de oposição, após consulta da autoridade emissora. Além disso, se for iniciado o procedimento de execução coerciva, o próprio destinatário poderá opor-se à ordem perante a autoridade de execução, com base em qualquer desses fundamentos (com exceção das imunidades e dos privilégios), nomeadamente nos casos em que seja evidente que a ordem não foi emitida ou validada por uma autoridade competente ou nos quais o seu cumprimento violaria manifestamente a Carta dos Direitos Fundamentais da União Europeia, ou seria manifestamente abusivo. Por exemplo, uma ordem em que sejam solicitados dados de conteúdo pertencentes a uma classe indefinida de pessoas localizadas numa área geográfica

ou sem ligação a procedimentos penais específicos ignoraria de forma manifesta as condições aplicáveis à emissão de uma ordem europeia de entrega de provas previstas no regulamento, o que já seria evidente a partir do teor do próprio certificado. Outros fundamentos só podem ser invocados pela pessoa cujos dados são solicitados, no âmbito das vias de recurso que lhe assistem no Estado de emissão (ver artigo 17.º infra). Além disso, os prestadores de serviços devem dispor de vias de recurso contra as decisões das autoridades de execução que lhes imponham sanções.

O procedimento de execução coerciva prevê diferentes prazos para as autoridades de emissão e de execução, a fim de evitar atrasos durante o procedimento.

Capítulo 4: Vias de recurso

Artigos 15.º e 16.º: Procedimento de reexame em caso de obrigações contraditórias resultantes do direito de um país terceiro

Os artigos 15.º e 16.º preveem um procedimento de reexame, caso os prestadores de serviços estabelecidos em países terceiros se deparem com obrigações contraditórias. Estas disposições são também essenciais para garantir a proteção dos direitos individuais e o respeito do princípio da cortesia internacional. Ao estabelecerem normas rigorosas, incentivam os países terceiros a proporcionarem níveis de proteção equivalentes. Na situação oposta, quando as autoridades de um país terceiro procuram obter dados de um cidadão da UE através de um prestador de serviços da UE, a legislação da União ou dos Estados-Membros que protege os direitos fundamentais, como o acervo em matéria de proteção de dados, pode impedir a sua divulgação. A União Europeia espera que os países terceiros respeitem as proibições previstas na presente proposta.

O procedimento previsto no artigo 15.º pode ser desencadeado pelo destinatário, quando o cumprimento de uma ordem europeia de entrega de provas implique a violação do direito de um país terceiro que proíbe a divulgação dos dados em causa com o fundamento de que essa proibição é necessária para proteger os direitos fundamentais das pessoas em causa ou os interesses fundamentais desse país terceiro em matéria de segurança ou de defesa nacional. O destinatário é obrigado a notificar à autoridade emissora a sua oposição fundamentada, apresentando os motivos pelos quais considera existirem obrigações contraditórias. Esta oposição fundamentada não pode assentar no simples facto de não existirem disposições semelhantes no direito do país terceiro nem apenas na circunstância de os dados estarem armazenados num país terceiro. A oposição fundamentada deve ser apresentada nos termos do artigo 9.º, n.º 5, no que respeita à notificação da intenção de não dar cumprimento à ordem, através do formulário constante do anexo III.

Com base na oposição fundamentada, a autoridade emissora reapreciará a ordem emitida. Se optar por revogá-la, o procedimento será encerrado. Contudo, se decidir confirmá-la, o processo será transferido para o tribunal competente do seu Estado-Membro, que avaliará, com base na oposição fundamentada e tendo em conta todos os factos relevantes do processo, se o direito do país terceiro se aplica ao processo específico em causa e, se for caso disso, se existe um conflito. Ao proceder a essa avaliação, o tribunal deve ter em conta se o direito do país terceiro em causa, em vez de ter por objetivo proteger os direitos fundamentais das pessoas em causa ou os interesses fundamentais desse país em matéria de segurança ou defesa nacional, visa antes manifestamente proteger outros interesses ou atividades ilícitas contra pedidos formulados por autoridades policiais no quadro de investigações penais.

Se o tribunal determinar que existe, de facto, um conflito com as obrigações decorrentes da legislação que protege os direitos fundamentais das pessoas ou os interesses fundamentais do país terceiro em matéria de segurança ou defesa nacional, deve solicitar um parecer a esse país, através das respetivas autoridades centrais. Se esse parecer confirmar a existência do conflito e o país terceiro se opuser à execução da ordem, o tribunal deve revogá-la.

Se for suscitado um conflito em virtude de legislação de um país terceiro que não se destine a proteger os direitos fundamentais das pessoas ou os interesses fundamentais do país em matéria de segurança ou defesa nacional, o tribunal tomará a sua decisão com base numa ponderação dos interesses a favor e contra a confirmação da ordem.

As condições definidas no artigo 9.º, nomeadamente as obrigações de conservação de provas previstas no n.º 6, são igualmente aplicáveis nas situações em que existam obrigações contraditórias resultantes do direito de um país terceiro. Se o tribunal determinar que a ordem deve ser confirmada, a autoridade emissora e o prestador de serviços devem ser informados, a fim de procederem à sua execução. Nos casos em que a ordem seja revogada, pode ser emitida uma ordem europeia de conservação de provas distinta, a fim de garantir a disponibilidade dos dados, sempre que possam ser obtidos através de um pedido de auxílio judiciário mútuo.

Tendo em conta que a ordem europeia de conservação de provas não implica a divulgação desses dados e, por conseguinte, não suscita preocupações semelhantes, o procedimento de reexame é limitado à ordem europeia de entrega de provas.

Artigo 17.º: Vias de recurso efetivo

Esta disposição garante que as pessoas afetadas por uma ordem europeia de entrega de provas dispõem de vias de recurso efetivo, que podem ser exercidas no Estado de emissão, em conformidade com o direito nacional. No que respeita às pessoas suspeitas e arguidas, as vias de recurso são normalmente exercidas no âmbito o processo penal. Não estão previstas vias de recurso específicas para a ordem europeia de conservação de provas, a qual, por si só, não permite a divulgação de quaisquer dados, exceto se for seguida de uma ordem europeia de entrega de provas ou de qualquer outro instrumento que possa levar à divulgação dos dados, o que daria então origem a vias de recurso específicas.

As pessoas cujos dados sejam solicitados sem que sejam suspeitas ou arguidas em processo penal devem dispor igualmente de vias de recurso no Estado de emissão. Todos estes direitos são aplicáveis sem prejuízo de eventuais vias de recurso disponíveis ao abrigo da Diretiva sobre a proteção de dados na aplicação da lei e do Regulamento geral sobre a proteção de dados.

Ao contrário das disposições aplicáveis aos prestadores de serviços, o regulamento não impõe qualquer limitação aos eventuais fundamentos que estas pessoas podem invocar para contestar a legalidade da ordem. Esses fundamentos incluem a necessidade e a proporcionalidade da ordem.

O exercício das vias de recurso no Estado de emissão não onera as pessoas afetadas de uma forma desproporcionada. Tal como sucede com as ordens executadas através de outras formas de cooperação judiciária, os tribunais do Estado de emissão estão em melhor posição para reapreciar a legalidade das ordens europeias de entrega de provas emitidas pelas suas próprias autoridades, assim como para avaliar a compatibilidade com o respetivo direito nacional. Além disso, durante a fase de execução coerciva, os destinatários podem opor-se,

separadamente, à execução do COEEP ou do COECP no seu Estado-Membro de acolhimento, com base na lista de fundamentos enumerados no regulamento (ver artigo 14.º supra).

Artigo 18.º: Garantia dos privilégios e imunidades reconhecidos pelo Estado de receção

Esta disposição tem, à semelhança do artigo 5.º, n.º 7, o objetivo de garantir que as imunidades e os privilégios que protegem os dados solicitados no Estado-Membro do prestador de serviços são tidos em conta no Estado de emissão, nomeadamente quando existam diferenças entre esses Estados-Membros, bem como os interesses fundamentais desse Estado-Membro em matéria de segurança e defesa nacional. O artigo 18.º prevê que o tribunal do Estado de emissão tenha estes direitos e interesses em conta como se estivessem previstos no respetivo direito nacional. Dadas as diferenças existentes entre os Estados-Membros quando avaliam a pertinência e a admissibilidade das provas, esta disposição deixa alguma flexibilidade aos tribunais quanto à forma de proceder.

Capítulo 5: Disposições finais

Artigo 19.º: Acompanhamento e divulgação de informações sobre a aplicação

Este artigo exige que os Estados-Membros comuniquem informações específicas relacionadas com a aplicação do regulamento, a fim de ajudar a Comissão a exercer as funções que lhe incumbem por força do artigo 24.º. A Comissão estabelecerá um programa pormenorizado para acompanhar as realizações, os resultados e o impacto do regulamento.

Artigo 20.º: Alterações aos certificados e aos formulários

Os certificados e os formulários que constam dos anexos I, II e III facilitam a execução dos COEEP e dos COECP. Por este motivo, é necessário que, no futuro, seja possível dar resposta à eventual necessidade de melhorar o conteúdo dos certificados e formulários o mais rapidamente possível. A alteração dos três anexos através do processo legislativo ordinário não se coaduna com esta exigência. Além disso, estes anexos não são elementos essenciais dos atos legislativos, os quais são definidos no artigo 8.º. O artigo 20.º prevê, por conseguinte, um procedimento de alteração mais rápido e flexível através de atos delegados.

Artigo 21.º: Exercício da delegação

Este artigo define as condições em que a Comissão pode adotar atos delegados a fim de introduzir as alterações necessárias nos certificados e formulários anexos à proposta. Estabelece ainda um procedimento uniforme para a adoção desses atos delegados.

Artigo 22.º: Notificações

Os Estados-Membros devem comunicar à Comissão as suas autoridades emissoras e de execução competentes e os tribunais competentes para responder a oposições fundamentadas apresentadas por prestadores de serviços em caso de conflito de leis.

Artigo 23.º: Relação com as decisões europeias de investigação

Esta disposição esclarece que o regulamento não impede as autoridades dos Estados-Membros de emitirem decisões europeias de investigação, em conformidade com a Diretiva 2014/41/UE, a fim de obterem provas eletrónicas.

Artigo 24.º: Avaliação

Esta disposição estabelece que a Comissão deve proceder à avaliação do regulamento em conformidade com as orientações «Legislar Melhor» da Comissão e o n.º 22 do Acordo Interinstitucional de 13 de abril de 2016[25]. Cinco anos após a entrada em vigor do regulamento, a Comissão deve informar o Parlamento Europeu e o Conselho sobre as conclusões da avaliação, incluindo uma análise da necessidade de alargar o seu âmbito a serviços ainda não abrangidos mas que se possam mostrar pertinentes para as investigações.

Artigo 25.º: Entrada em vigor

O regulamento proposto entrará em vigor no vigésimo dia seguinte ao da sua publicação no Jornal Oficial da União Europeia. Será aplicável seis meses após a data de entrada em vigor.

[25] Acordo interinstitucional entre o Parlamento Europeu, o Conselho da União Europeia e a Comissão Europeia sobre «Legislar Melhor», 13 de abril de 2016; JO L 123, 12.5.2016, p. 1–14.

2018/0108 (COD)

Proposta de

REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

relativo às ordens europeias de entrega ou de conservação de provas eletrónicas em matéria penal

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 82.º, n.º 1,

Tendo em conta a proposta da Comissão Europeia,

Após transmissão do projeto de ato legislativo aos parlamentos nacionais,

Tendo em conta o parecer do Comité Económico e Social Europeu[26],

Deliberando de acordo com o processo legislativo ordinário,

Considerando o seguinte:

(1) A União estabeleceu como objetivo manter e desenvolver um espaço de liberdade, segurança e justiça. A fim de criar progressivamente esse espaço, a União deve adotar medidas no domínio da cooperação judiciária em matéria penal, com base no princípio do reconhecimento mútuo das sentenças e decisões judiciais, comummente designado como a pedra angular da cooperação judiciária em matéria penal na União desde o Conselho Europeu de Tampere, de 15 e 16 de outubro de 1999.

(2) As medidas destinadas a obter e a conservar provas eletrónicas têm uma importância cada vez maior para as investigações e as ações penais na União. Para combater a criminalidade, é essencial que existam mecanismos eficazes para obter provas eletrónicas, juntamente com condições que garantam o pleno respeito dos princípios e direitos fundamentais consagrados nos Tratados e na Carta dos Direitos Fundamentais da União Europeia, nomeadamente, os princípios da necessidade e da proporcionalidade, o direito a um processo equitativo, o direito à proteção dos dados, o direito ao sigilo da correspondência e o direito à privacidade.

(3) A Declaração Comum dos Ministros da Justiça e dos Assuntos Internos e dos representantes das instituições da União sobre os ataques terroristas perpetrados em Bruxelas em 22 de março de 2016 sublinhou a necessidade de encontrar, com caráter prioritário, formas de assegurar e obter provas eletrónicas com mais rapidez e eficácia e de identificar medidas concretas para resolver este problema.

[26] JO C , , p. .

(4) As conclusões do Conselho de 9 de junho de 2016 salientaram a crescente importância das provas eletrónicas em processo penal, bem como da proteção do ciberespaço contra abusos e atividades criminosas, em benefício das economias e das sociedades, e, por conseguinte, a necessidade de as autoridades policiais e judiciais disporem de instrumentos eficazes para investigar e reprimir infrações penais relacionadas com o ciberespaço.

(5) Na comunicação conjunta sobre resiliência, dissuasão e defesa, de 13 de setembro de 2017[27], a Comissão sublinhou que a eficácia da investigação e da ação penal contra a criminalidade possibilitada pelo ciberespaço era um importante elemento dissuasor de ciberataques e que o atual quadro processual deveria ser mais bem adaptado à era da Internet. Por vezes, os procedimentos atuais não conseguem acompanhar a rapidez dos ciberataques, o que cria necessidades específicas de rápida cooperação transnacional.

(6) O Parlamento Europeu fez eco desses receios na sua resolução sobre a luta contra a cibercriminalidade, de 3 de outubro de 2017[28], destacando os problemas que a atual fragmentação do quadro jurídico pode criar aos prestadores de serviços que procuram satisfazer os pedidos das autoridades policiais e exortando a Comissão a apresentar um quadro jurídico da União em matéria de provas eletrónicas que contemple salvaguardas suficientes dos direitos e liberdades de todos os interessados.

(7) Os serviços baseados em rede podem ser prestados a partir de qualquer lugar, não requerendo a presença de estruturas físicas, instalações ou pessoal no país em causa. Consequentemente, os elementos de prova pertinentes são muitas vezes armazenados fora do Estado que conduz a investigação ou por um prestador de serviços estabelecido fora desse Estado. Frequentemente, não existe outra ligação entre o processo em investigação no Estado em causa e o Estado do local de armazenamento dos dados ou do estabelecimento principal do prestador de serviços em causa.

(8) Devido a esta falta de ligação, os pedidos de cooperação judiciária são frequentemente endereçados a Estados que acolhem um grande número de prestadores de serviços, mas que não têm qualquer relação específica com o processo em causa. Além disso, o número de pedidos multiplicou-se, devido à utilização cada vez maior de serviços em rede, que são transnacionais por natureza. Consequentemente, a obtenção de provas eletrónicas através dos canais de cooperação judiciária é muitas vezes morosa, levando mais tempo do que aquele durante o qual os indícios poderão estar disponíveis. Além disso, não existe um quadro claro para a cooperação com os prestadores de serviços, embora alguns prestadores de países terceiros aceitem pedidos diretos quanto aos dados não relacionados com conteúdos, na medida do permitido pelo respetivo direito nacional. Por conseguinte, todos os Estados-Membros dependem do canal de cooperação com os prestadores de serviços, quando exista, utilizando instrumentos, condições e procedimentos nacionais diferentes. Além disso, no que respeita aos dados de conteúdo, alguns Estados-Membros adotaram medidas unilaterais, enquanto outros continuam a recorrer à cooperação judiciária.

(9) A fragmentação do quadro jurídico cria problemas aos prestadores de serviços que procuram satisfazer pedidos formulados por autoridades policiais. Importa, por conseguinte, criar um quadro jurídico europeu em matéria de provas eletrónicas, a fim

---

27 JOIN(2017) 450 final.

28 2017/2068 (INI).

de impor aos prestadores de serviços abrangidos pelo âmbito de aplicação do instrumento a obrigação de responderem diretamente às autoridades competentes sem o envolvimento de uma autoridade judicial no Estado-Membro do prestador de serviços.

(10) As ordens previstas no regulamento devem ser notificadas aos representantes legais dos prestadores de serviços, nomeados para esse efeito. Se um prestador de serviços estabelecido na União não tiver nomeado um representante legal, as ordens poderão ser notificadas a qualquer estabelecimento desse prestador de serviços na União. Esta opção de recurso serve para garantir a eficácia do sistema, caso o prestador de serviços (ainda) não tenha nomeado um representante específico.

(11) O mecanismo das ordens europeias de entrega ou de conservação de provas eletrónicas em matéria penal só poderá funcionar eficazmente se tiver por base um nível elevado de confiança mútua entre os Estados-Membros, que é uma pré-condição essencial para o seu correto funcionamento.

(12) O presente regulamento respeita os direitos fundamentais e observa os princípios reconhecidos, nomeadamente na Carta dos Direitos Fundamentais da União Europeia, incluindo o direito à liberdade e à segurança, o direito ao respeito pela vida privada e familiar, a proteção dos dados pessoais, a liberdade de empresa, o direito de propriedade, o direito à ação e a um tribunal imparcial, a presunção de inocência e o direito de defesa, os princípios da legalidade e da proporcionalidade dos delitos e das penas, bem como o direito a não ser julgado ou punido penalmente mais do que uma vez pelo mesmo delito. Caso o Estado-Membro de emissão tenha a indicação de que poderão estar em curso processos penais paralelos noutro Estado-Membro, deverá consultar as autoridades desse Estado-Membro, em conformidade com a Decisão-Quadro 2009/948/JAI do Conselho[29].

(13) A fim de garantir o pleno respeito dos direitos fundamentais, o regulamento faz referência explícita às normas que devem ser imperativamente aplicadas à obtenção de quaisquer dados pessoais, ao tratamento desses dados, ao reexame jurisdicional do recurso às medidas de investigação previstas neste instrumento, assim como às vias de recurso disponíveis.

(14) O regulamento deve ser aplicado sem prejuízo dos direitos processuais em processo penal previstos nas Diretivas 2010/64/UE[30], 2012/13/UE[31], 2013/48/UE[32], 2016/343[33], 2016/800[34] e 2016/1919[35] do Parlamento Europeu e do Conselho.

---

29 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).

30 Diretiva 2010/64/UE do Parlamento Europeu e do Conselho, de 20 de outubro de 2010, relativa ao direito à interpretação e tradução em processo penal (JO L 280 de 26.10.2010, p. 1).

31 Diretiva 2012/13/UE do Parlamento Europeu e do Conselho, de 22 de maio de 2012, relativa ao direito à informação em processo penal (JO L 142 de 1.6.2012, p. 1).

32 Diretiva 2013/48/UE do Parlamento Europeu e do Conselho, de 22 de outubro de 2013, relativa ao direito de acesso a um advogado em processo penal e nos processos de execução de mandados de detenção europeus, e ao direito de informar um terceiro aquando da privação de liberdade e de comunicar, numa situação de privação de liberdade, com terceiros e com as autoridades consulares (JO L 294 de 6.11.2013, p. 1).

(15) Este instrumento estabelece as normas segundo as quais uma autoridade judicial competente na União Europeia pode, através de uma ordem europeia de entrega de provas ou de uma ordem europeia de conservação de provas, ordenar a um prestador de serviços que opera na União que entregue ou conserve em seu poder provas eletrónicas. O regulamento é aplicável em todos os casos em que o prestador de serviços esteja estabelecido ou representado noutro Estado-Membro. No que respeita a situações nacionais em que a utilização dos instrumentos previstos no regulamento não seja possível, este não deverá limitar as competências das autoridades nacionais já estabelecidas pelo direito nacional para obrigar os prestadores de serviços estabelecidos ou representados no seu território a cumprirem as disposições aplicáveis.

(16) Os prestadores de serviços mais importantes em matéria de processo penal são os prestadores de serviços de comunicações eletrónicas e os prestadores específicos de serviços da sociedade da informação que facilitam a interação entre os utilizadores. Por conseguinte, ambos os grupos devem ser abrangidos pelo regulamento. A definição de prestadores de serviços de comunicações eletrónicas é estabelecida na proposta de Diretiva que estabelece o Código Europeu das Comunicações Eletrónicas. Estes serviços incluem as comunicações interpessoais como, por exemplo, os serviços de comunicações de voz sobre IP, de mensagens instantâneas e de correio eletrónico. As categorias de serviços da sociedade da informação abrangidas pelo âmbito de aplicação do regulamento são aquelas para as quais o armazenamento de dados é uma componente determinante do serviço prestado ao utilizador e referem-se, em particular, às redes sociais (na medida em que não sejam consideradas serviços de comunicações eletrónicas), aos mercados em linha que facilitam transações entre os seus utilizadores (consumidores ou empresas) e outros prestadores de serviços de alojamento, incluindo os casos em que o serviço é prestado através de computação em nuvem. Os serviços da sociedade de informação para os quais o armazenamento de dados não constitui uma componente determinante do serviço prestado ao utilizador e tem uma natureza meramente auxiliar, tais como serviços jurídicos, de arquitetura, de engenharia e de contabilidade prestados em linha, à distância, devem ser excluídos do âmbito de aplicação do regulamento, mesmo que sejam abrangidos pela definição de serviços da sociedade da informação constante da Diretiva (UE) 2015/1535.

(17) Em muitos casos, os dados já não são armazenados ou tratados num dispositivo do utilizador, mas sim disponibilizados numa infraestrutura baseada na nuvem para serem acedidos a partir de qualquer lugar. Para executar esses serviços, os prestadores de serviços não precisam de estar estabelecidos ou de ter servidores numa determinada jurisdição. Por conseguinte, a aplicação do presente regulamento não deverá depender da localização efetiva do estabelecimento do prestador ou da instalação de tratamento ou armazenamento dos dados em causa.

---

33 Diretiva (UE) 2016/343 do Parlamento Europeu e do Conselho, de 9 de março de 2016, relativa ao reforço de certos aspetos da presunção de inocência e do direito de comparecer em julgamento em processo penal (JO L 65 de 11.3.2016, p. 1).

34 Diretiva (UE) 2016/800 do Parlamento Europeu e do Conselho, de 11 de maio de 2016, relativa a garantias processuais para os menores suspeitos ou arguidos em processo penal (JO L 132 de 21.5.2016, p. 1).

35 Diretiva (UE) 2016/1919 do Parlamento Europeu e do Conselho, de 26 de outubro de 2016, relativa ao apoio judiciário para suspeitos e arguidos em processo penal e para as pessoas procuradas em processos de execução de mandados de detenção europeus (JO L 297 de 4.11.2016, p. 1).

(18) Os prestadores de serviços de infraestruturas da Internet relacionados com a atribuição de nomes e números, tais como agentes de registo e registos de nomes de domínio e prestadores de serviços de proxy, ou registos regionais da Internet para endereços de protocolo Internet («IP»), são particularmente úteis para identificar criminosos responsáveis por sítios Web mal-intencionados ou que tenham sido infiltrados por estes. Estes prestadores de serviços detêm dados de particular relevância em processo penal, já que podem permitir identificar pessoas ou entidades responsáveis por sítios Web que tenham sido utilizados em atividades criminosas, ou as vítimas da atividade criminosa no caso de sítios Web que tenham sido infiltrados por criminosos.

(19) O regulamento incide apenas sobre a recolha de dados armazenados, ou seja, os dados detidos por um prestador de serviços no momento da receção do certificado de ordem europeia de entrega ou de conservação de provas. Não estabelece uma obrigação geral de retenção de dados nem autoriza a interceção de dados ou a obtenção de dados que tenham sido armazenados após a receção de um certificado de ordem europeia de entrega ou de conservação de provas. Os dados devem ser fornecidos, independentemente de estarem encriptados ou não.

(20) As categorias de dados abrangidas pelo presente regulamento incluem dados de assinantes, dados de acesso, dados transacionais (estas três categorias são referidas como «dados não relacionados com conteúdos») e dados de conteúdo. Esta distinção, com exceção dos dados de acesso, existe nos direitos nacionais de muitos Estados-Membros e no atual quadro jurídico dos EUA, que autoriza os prestadores de serviços a partilharem voluntariamente dados não relacionados com conteúdos com autoridades policiais estrangeiras.

(21) Importa destacar os dados de acesso como uma categoria de dados específica utilizada no regulamento. Os dados de acesso são solicitados para o mesmo objetivo que os dados de assinantes, ou seja, para identificar o utilizador, sendo o nível de interferência com os direitos fundamentais semelhante ao dos dados de assinantes. Os dados de acesso são tipicamente registados no âmbito de registos de eventos (por outras palavras, um registo de servidor) para indicar o início e o fim da sessão de acesso de um utilizador a um serviço. Normalmente, trata-se de um endereço IP individual (estático ou dinâmico) ou outro identificador que destaca a interface de rede utilizada durante a sessão de acesso. Se o utilizador for desconhecido, esses dados de acesso devem muitas vezes ser obtidos para que se possa solicitar ao prestador de serviços os dados de assinantes relacionados com esse identificador.

(22) Os dados transacionais, por outro lado, são normalmente solicitados para obter informações sobre os contactos e o paradeiro do utilizador, podendo servir para definir o perfil da pessoa em causa. Assim sendo, os dados de acesso, por si só, não podem ser utilizados para uma finalidade semelhante, por exemplo, não revelam quaisquer informações sobre interlocutores relacionados com o utilizador. A presente proposta introduz assim uma nova categoria de dados, que deve ser tratada como os dados de assinantes, se o objetivo subjacente à obtenção desses dados for semelhante.

(23) Todas as categorias de dados contêm dados pessoais e, portanto, são abrangidas pelas salvaguardas previstas no acervo da UE no domínio da proteção de dados, mas o seu impacto nos direitos fundamentais varia, em especial entre os dados de assinantes e de acesso, por um lado, e entre os dados transacionais e de conteúdo, por outro. Embora os dados de assinantes e de acesso sejam úteis para obter indícios iniciais numa

investigação sobre a identidade de um suspeito, os dados transacionais e de conteúdo são os mais relevantes como material probatório. Sendo assim, é essencial que todas estas categorias de dados sejam abrangidas pelo instrumento. Devido ao diferente grau de interferência com os direitos fundamentais, são impostas condições diferentes para a obtenção de dados de assinantes e de acesso, por um lado, e de dados transacionais e de conteúdo, por outro.

(24) As ordens europeias de entrega ou de conservação de provas são medidas de investigação que só podem ser decretadas no âmbito de processos penais específicos contra os autores específicos conhecidos, ou ainda desconhecidos, de determinada infração penal já cometida, após a avaliação da proporcionalidade e da necessidade em cada caso concreto.

(25) O regulamento não prejudica os poderes de investigação das autoridades em processos civis ou administrativos, incluindo quando esses processos possam conduzir a sanções.

(26) O regulamento deve aplicar-se aos prestadores de serviços que operam na União e as ordens nele previstas só podem ser emitidas para dados pertencentes a serviços prestados na União. Os serviços prestados exclusivamente fora da União não são abrangidos pelo âmbito de aplicação do regulamento, mesmo que o prestador de serviços em causa esteja estabelecido na União.

(27) Para determinar se um prestador de serviços presta serviços na União, é necessário apurar se este permite que pessoas singulares ou coletivas de um ou vários Estados-Membros utilizem os seus serviços. No entanto, a mera acessibilidade de uma interface em linha como, por exemplo, a acessibilidade do sítio Web do prestador de serviços, de um intermediário, de um endereço de correio eletrónico e de outras informações de contacto num ou em vários Estados-Membros, isoladamente, não deve constituir condição suficiente para a aplicação do regulamento.

(28) Uma ligação significativa à União deve ser igualmente pertinente para determinar o âmbito de aplicação do regulamento. Deve considerar-se que tal ligação significativa existe quando o prestador de serviços possui um estabelecimento na União. Na ausência de tal estabelecimento, o critério de ligação significativa deve ser avaliado com base na existência de um número significativo de utilizadores num ou vários Estados-Membros ou na orientação das atividades para um ou vários Estados-Membros. Essa orientação pode ser determinada com base em quaisquer circunstâncias relevantes, incluindo fatores como a utilização de uma língua ou de uma moeda geralmente utilizada num Estado-Membro, ou a possibilidade de encomendar bens ou serviços. A orientação de atividades para um Estado-Membro também pode resultar da disponibilização de uma aplicação («app») na loja de aplicações nacional pertinente, da divulgação de publicidade local ou na língua utilizada nesse Estado-Membro, ou da gestão das relações com os clientes, por exemplo, através da prestação de serviços aos clientes na língua geralmente utilizada nesse Estado-Membro. Deve considerar-se igualmente que existe uma ligação significativa quando um prestador de serviços dirige as suas atividades para um ou vários Estados-Membros, conforme estabelecido no artigo 17.º, n.º 1, alínea c), do Regulamento 1215/2012 relativo à competência judiciária, ao reconhecimento e à execução de decisões em matéria civil e

comercial[36]. Por outro lado, a prestação de um serviço tendo em vista a mera conformidade com a proibição de discriminação imposta pelo Regulamento (UE) 2018/302[37] não pode, unicamente com esse fundamento, ser considerada como direcionamento ou orientação das atividades para um determinado território na União.

(29) Uma ordem europeia de entrega de provas só poderá ser emitida se for considerada necessária e proporcionada. A avaliação deverá ter em conta se a ordem se limita ao necessário para atingir o objetivo legítimo de obter os dados pertinentes e necessários para serem utilizados como elementos de prova unicamente num determinado processo concreto.

(30) Quando é emitida uma ordem europeia de entrega ou de conservação de provas, deve estar sempre envolvida uma autoridade judicial no processo de emissão ou de validação da mesma. Tendo em conta o caráter mais sensível dos dados transacionais e de conteúdo, a emissão ou a validação de ordens europeias de entrega de provas para a obtenção deste tipo de dados exigirá a supervisão de um juiz. Uma vez que os dados de assinantes e de acesso são menos sensíveis, as ordens europeias de entrega de provas para efeitos da divulgação desse tipo de dados também podem ser emitidas ou validadas por magistrados do Ministério Público.

(31) Pelo mesmo motivo, deve ser efetuada uma distinção quanto ao âmbito de aplicação material do regulamento: Poderão ser emitidas ordens de entrega de dados de assinantes e de dados de acesso relativamente a qualquer infração penal, devendo o acesso a dados transacionais e de conteúdo ser sujeito a requisitos mais rigorosos, a fim de refletir a sua natureza mais sensível. A fixação de um limiar permite uma abordagem mais proporcionada, juntamente com uma série de outras condições *ex ante* e *ex post* e com as salvaguardas previstas na proposta, a fim de garantir o respeito pela proporcionalidade e pelos direitos das pessoas afetadas. Ao mesmo tempo, esse limiar não deve limitar a eficácia do instrumento e a sua utilização pelos profissionais da justiça. Permitir a emissão de ordens em relação a investigações quanto a infrações puníveis com, pelo menos, uma pena privativa de liberdade de duração máxima não inferior a três anos limita o âmbito de aplicação do instrumento aos crimes mais graves, sem afetar excessivamente as possibilidades da sua utilização pelos profissionais da justiça. Esse limiar exclui do âmbito de aplicação de regulamento um número significativo de infrações consideradas de menor gravidade pelos Estados-Membros, expressa numa pena máxima inferior, e tem ainda a vantagem de ser facilmente aplicável na prática.

(32) Existem infrações específicas para as quais apenas existem provas em formato eletrónico, cuja natureza é particularmente efémera. É o caso, por exemplo, dos crimes cibernéticos, mesmo daqueles que não podem ser considerados graves por si só, mas que podem provocar danos extensos ou consideráveis, nomeadamente em processos

---

36 Regulamento (UE) n.º 1215/2012 do Parlamento Europeu e do Conselho, de 12 de dezembro de 2012, relativo à competência judiciária, ao reconhecimento e à execução de decisões em matéria civil e comercial (JO L 351 de 20.12.2012, p. 1).

37 Regulamento (UE) 2018/302 do Parlamento Europeu e do Conselho, de 28 de fevereiro de 2018, que visa prevenir o bloqueio geográfico injustificado e outras formas de discriminação baseadas na nacionalidade, no local de residência ou no local de estabelecimento dos clientes no mercado interno, e que altera os Regulamentos (CE) n.º 2006/2004 e (UE) 2017/2394 e a Diretiva 2009/22/CE (JO L 601, de 2.3.2018, p. 1).

com pouco impacto individual mas com danos globais e de elevado volume. Na maioria dos casos em que a infração é cometida através de um sistema da informação, a aplicação do limiar aplicado a outros tipos de infrações levaria, sobretudo, a uma situação de impunidade. Isto justifica a aplicação do regulamento igualmente às infrações cuja moldura penal seja inferior a três anos de prisão. Além disso, as infrações relacionadas com o terrorismo descritas na Diretiva 2017/541/UE não exigem o limiar máximo de, no mínimo, três anos.

(33) Por outro lado, é necessário prever que só possa ser emitida uma ordem europeia de entrega de provas se existir uma ordem semelhante para a mesma infração penal numa situação nacional comparável no Estado de emissão.

(34) Nos casos em que os dados solicitados sejam armazenados ou tratados no contexto de uma infraestrutura fornecida por um prestador de serviços a uma empresa ou a outra entidade que não seja uma pessoa singular (normalmente, no caso de serviços de alojamento), a ordem europeia de entrega de provas apenas pode ser utilizada quando outras medidas de investigação tendo por objeto a empresa ou entidade não sejam adequadas, em especial, se houver risco de estas prejudicarem a investigação. Este aspeto é pertinente, sobretudo, no que se refere às entidades de maior dimensão, como as empresas ou entidades governamentais, que recorrem a prestadores de serviços para fornecer serviços ou infraestruturas de TI empresariais, ou a ambos. Nessas situações, o primeiro destinatário da ordem europeia de entrega de provas deve ser a empresa ou outra entidade, a qual poderá não ser um prestador de serviços abrangido pelo âmbito de aplicação do regulamento. No entanto, nos casos em que não seja oportuno notificar essa entidade, por exemplo, porque é suspeita de envolvimento no caso em apreço ou porque existem indícios de conluio com o alvo da investigação, as autoridades competentes devem poder notificar o prestador de serviços que fornece a infraestrutura em causa para que forneça os dados solicitados. Esta disposição não prejudica o direito de ordenar ao prestador de serviços que conserve os dados.

(35) As imunidades e privilégios, que podem dizer respeito a categorias de pessoas (por exemplo, os diplomatas) ou a relações com uma proteção específica (por exemplo, a relação privilegiada entre o advogado e o cliente), estão previstos noutros instrumentos de reconhecimento mútuo, como a decisão europeia de investigação. O seu âmbito e impacto diferem em função do direito nacional aplicável que deve ser tido em conta aquando da emissão da ordem, uma vez que a autoridade emissora apenas a poderá emitir se existir uma ordem semelhante numa situação nacional comparável. Além deste princípio de base, as imunidades e os privilégios que protegem dados de acesso, transacionais ou de conteúdo no Estado-Membro do prestador de serviço devem, tanto quanto possível, ser tidos em conta no Estado de emissão como se estivessem previstos no seu direito nacional. Este aspeto é pertinente, nomeadamente, se o direito do Estado-Membro no qual o prestador de serviços ou o seu representante for notificado proporcionar uma proteção mais elevada do que o direito do Estado de emissão. Esta disposição também assegura o respeito dos Estados-Membros quando a divulgação dos dados em causa possa afetar os seus interesses fundamentais em matéria de segurança e defesa nacional. Como salvaguarda suplementar, estes aspetos devem ser tidos em conta não só aquando da emissão da ordem como também posteriormente, durante a avaliação da relevância e da admissibilidade dos dados em causa na fase pertinente dos processos penais e, caso seja iniciado um procedimento de execução coerciva, por parte da autoridade de execução.

(36) A ordem europeia de conservação de provas pode ser emitida em relação a qualquer infração. O seu objetivo é impedir a remoção, eliminação ou alteração de dados pertinentes em situações em que a obtenção desses dados possa ser mais morosa, por exemplo, quando são utilizados canais de cooperação judiciária.

(37) As ordens europeias de entrega ou de conservação de provas devem ser notificadas ao representante legal nomeado pelo prestador de serviços. Na sua ausência, as ordens poderão ser notificadas em qualquer estabelecimento do prestador de serviços na União. Tal pode suceder, por exemplo, quando o prestador de serviços não seja legalmente obrigado a nomear um representante legal. Em caso de incumprimento por parte do representante legal, em situações de urgência, a ordem europeia de entrega ou de conservação de provas pode ser notificada ao prestador de serviços juntamente ou em alternativa à execução coerciva da ordem original, nos termos do artigo 14.º. Em caso de incumprimento por parte do representante legal em situações que não sejam de urgência, mas em que existam riscos claros de se perder os dados, a ordem europeia de entrega ou de conservação de provas também poderá ser notificada em qualquer estabelecimento do prestador de serviços na União. Dados estes vários cenários possíveis, nas disposições optou-se pelo termo genérico «destinatário». Quando uma obrigação (por exemplo, em matéria de confidencialidade) seja aplicável não só ao destinatário como também ao prestador de serviços, caso este não seja o destinatário, tal é especificado na respetiva disposição.

(38) As ordens europeias de entrega ou de conservação de provas devem ser transmitidas ao prestador de serviços através de um certificado de ordem europeia de entrega de provas (COEEP) ou de um certificado de ordem europeia de conservação de provas (COECP), que deverá ser traduzido. Os certificados devem conter as mesmas informações obrigatórias que constam da ordem, mas não a fundamentação quanto à necessidade e proporcionalidade da medida ou outras informações sobre o processo, a fim de não prejudicar as investigações. No entanto, se essas informações estiverem incluídas na ordem, permitem que o suspeito a conteste durante o processo penal. Se necessário, o certificado deve ser traduzido para a língua oficial ou para uma das línguas oficiais do Estado-Membro do destinatário, ou para outra língua oficial que o prestador de serviços tenha declarado aceitar.

(39) A autoridade emissora competente deve transmitir o COEEP ou o COECP diretamente ao destinatário através de qualquer meio que permita produzir um registo escrito em condições que permitam ao prestador de serviços verifica a sua autenticidade, por exemplo, correio registado, correio eletrónico, plataformas ou outros canais seguros, incluindo os disponibilizados pelo prestador de serviços, em conformidade com a legislação em matéria de proteção de dados pessoais.

(40) Os dados solicitados devem ser transmitidos às autoridades, o mais tardar, no prazo de dez dias a contar da receção do COEEP. O prestador de serviços deve respeitar prazos mais curtos em situações de urgência, e sempre que a autoridade emissora indique outros motivos para que não seja aplicado o prazo de dez dias. Além do perigo iminente da eliminação dos dados solicitados, esses motivos podem incluir circunstâncias que estejam relacionadas com uma investigação em curso, por exemplo, quando os dados solicitados estão associados a outras medidas de investigação urgentes que não possam ser executadas sem os dados em falta ou deles dependam.

(41) A fim de permitir que os prestadores de serviços possam resolver problemas formais, importa criar um procedimento de comunicação entre o prestador de serviços e a autoridade judicial emissora, quando o COEEP possa estar incompleto ou conter erros manifestos ou informação insuficiente para executar a ordem. Além disso, se o prestador de serviços não fornecer as informações de forma exaustiva ou adequada por qualquer outro motivo, por exemplo, por considerar existir um conflito com uma obrigação ao abrigo do direito de um país terceiro, ou considerar que a ordem europeia de entrega de provas não foi emitida em conformidade com as condições previstas no regulamento, deve contactar as autoridades emissoras e fornecer as justificações necessárias. O procedimento de comunicação deve, portanto, permitir a correção ou reavaliação do COEEP pela autoridade emissora logo numa fase inicial. Caso consiga identificar os dados solicitados, o prestador de serviços deve conservá-los, a fim de garantir a sua disponibilidade.

(42) Após a receção de um certificado de ordem europeia de conservação de provas (COECP), o prestador de serviços deve conservar os dados solicitados durante um período máximo de 60 dias, a menos que a autoridade emissora o informe de que iniciou o procedimento de emissão do pedido de entrega de provas subsequente, caso em que a conservação deve manter-se. O período de 60 dias foi calculado de modo a possibilitar a emissão de um pedido oficial. Este processo exige que tenham sido adotadas, pelo menos, algumas medidas formais, por exemplo, o envio de um pedido de auxílio judiciário mútuo para efeitos de tradução. Após a receção dessa informação, os dados devem ser conservados durante o período de tempo necessário para a sua transmissão no âmbito do pedido de entrega de provas subsequente.

(43) Os prestadores de serviços e respetivos representantes legais devem assegurar a confidencialidade e, quando solicitado pela autoridade emissora, abster-se de informar a pessoa cujos dados são solicitados, a fim de salvaguardar a investigação das infrações penais, nos termos do artigo 23.º do Regulamento (UE) 2016/679[38]. No entanto, as informações relativas ao utilizador são um elemento essencial para permitir o controlo e o recurso jurisdicionais e, caso tenha sido solicitado ao prestador de serviços que não informe o utilizador, devem ser fornecidas a este último pela autoridade assim que deixar de existir o risco de comprometer investigações em curso, em conformidade com a medida nacional que aplica o artigo 13.º da Diretiva (UE) 2016/680[39].

(44) Em caso de incumprimento por parte do destinatário, a autoridade emissora pode transferir a ordem completa, incluindo a fundamentação quanto à necessidade e proporcionalidade, juntamente com o certificado, à autoridade competente do Estado-Membro no qual o destinatário do certificado reside ou está estabelecido. Este Estado-Membro deverá fazê-la executar em conformidade com o direito nacional. Os Estados-

---

38 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).

39 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).

Membros devem prever a aplicação de coimas eficazes, proporcionadas e dissuasoras em caso de incumprimento das obrigações impostas pelo regulamento.

(45) O procedimento de execução coerciva permite que o destinatário se oponha à execução, com base em determinados fundamentos limitados. A autoridade de execução pode recusar o reconhecimento e a execução da ordem com base nos mesmos fundamentos caso sejam aplicáveis imunidades e privilégios ao abrigo do respetivo direito nacional ou a divulgação seja suscetível de afetar interesses fundamentais, como a segurança e a defesa nacional. A autoridade de execução deve consultar a autoridade emissora antes de se recusar a reconhecer ou a executar a ordem com base nesses fundamentos. Em caso de incumprimento, as autoridades podem impor sanções, as quais devem ser proporcionadas e ter em conta circunstâncias específicas como o incumprimento repetido ou sistémico.

(46) Não obstante as obrigações que lhes incumbem em matéria de proteção de dados, os prestadores de serviços não poderão ser considerados responsáveis no Estado-Membro pelos prejuízos incorridos pelos seus utilizadores ou por terceiros em virtude do cumprimento de boa-fé de um certificado de ordem europeia de entrega ou de conservação de provas.

(47) Além das pessoas cujos dados são solicitados, os prestadores de serviços e os países terceiros podem ser afetados pela medida de investigação. A fim de assegurar o princípio de cortesia internacional em relação a interesses soberanos de países terceiros, proteger a pessoa em causa e resolver as questões relativas a obrigações contraditórias dos prestadores de serviços, o instrumento prevê um mecanismo específico de recurso judicial quando o cumprimento de uma ordem europeia de entrega de provas possa impedir os prestadores de serviços de cumprirem uma obrigação legal decorrente do direito de um país terceiro.

(48) Para o efeito, sempre que o destinatário considere que, no caso concreto em apreço, a ordem europeia de entrega de provas implicaria a violação de uma obrigação legal decorrente do direito de um país terceiro, deve informar a autoridade emissora deduzindo oposição fundamentada, utilizando os formulários fornecidos para esse efeito. A autoridade emissora deve, em seguida, apreciar a ordem europeia de entrega de provas à luz da oposição fundamentada, tendo em conta os mesmos critérios que seriam adotados pelo tribunal competente. Sempre que a autoridade decida confirmar a ordem, o processo deve ser enviado ao tribunal competente indicado pelo Estado-Membro em causa, que deverá apreciar a ordem.

(49) Ao verificar a existência de obrigações contraditórias nas circunstâncias específicas do processo em causa, o tribunal competente deve, quando necessário, recorrer a peritos externos competentes, por exemplo, se a apreciação suscitar questões relativas à interpretação do direito do país terceiro em causa. Se necessário, poderão ser consultadas as autoridades centrais desse país.

(50) O tribunal competente também pode recorrer a pareceres de peritos relativos à interpretação do direito de países terceiros, quando disponíveis. As informações e a jurisprudência neste domínio e em matéria de procedimentos de resolução de litígios nos Estados-Membros devem ser disponibilizadas numa plataforma central, como o projeto SIRIUS e/ou a Rede Judiciária Europeia. Tal permitirá aos tribunais beneficiar da experiência e dos conhecimentos especializados adquiridos por outros tribunais

sobre as mesmas questões ou sobre questões semelhantes. Se necessário, deve ser possível consultar novamente o país terceiro.

(51) Sempre que existam obrigações contraditórias, o tribunal deve determinar se as obrigações contraditórias do país terceiro proíbem a divulgação dos dados em apreço com o fundamento de que essa proibição é necessária para proteger os direitos fundamentais das pessoas em causa ou os interesses fundamentais do país terceiro em matéria de segurança ou defesa nacional. Ao proceder a essa avaliação, o tribunal deve ter em conta se o direito do país terceiro em causa, em vez de ter por objetivo proteger os direitos fundamentais das pessoas em causa ou os interesses fundamentais desse país em matéria de segurança ou defesa nacional, visa antes manifestamente proteger outros interesses ou atividades ilícitas contra pedidos formulados por autoridades policiais no quadro de investigações penais. Se que o tribunal concluir que as disposições contraditórias do país terceiro proíbem a divulgação dos dados em apreço com o fundamento de que essa proibição é necessária para proteger os direitos fundamentais das pessoas em causa ou os interesses fundamentais desse país em matéria de segurança ou defesa nacional, deve consultar o país terceiro através das suas autoridades centrais, que já existem para fins de auxílio judiciário mútuo em muitos países. O tribunal deve estabelecer um prazo para que o país terceiro se oponha à execução da ordem europeia de entrega de provas; caso as autoridades do país terceiro não respondam dentro do prazo (alargado), apesar de serem novamente notificadas das consequências da ausência de uma resposta, o tribunal deve confirmar a ordem. Se as autoridades do país terceiro se opuserem à divulgação dos dados, o tribunal deve revogar a ordem.

(52) Em todos os restantes casos de obrigações contraditórias, não relacionadas com direitos fundamentais de pessoas ou interesses fundamentais do país terceiro em matéria de segurança ou de defesa nacional, o tribunal deve decidir se confirma a ordem europeia de entrega de provas, ponderando uma série de aspetos para determinar a importância da ligação com qualquer das duas jurisdições envolvidas, os respetivos interesses em obter os dados ou em impedir a sua divulgação e as eventuais consequências para o prestador de serviços resultantes da necessidade de dar cumprimento à ordem. No que respeita às infrações no domínio da cibercriminalidade, o local onde o crime foi cometido abrange tanto o(s) local(/is) em que a ação teve lugar como aquele(s) no(s) qual(/is) os efeitos da infração se materializaram.

(53) As condições definidas no artigo 9.º são igualmente aplicáveis às situações em que existam obrigações contraditórias resultantes do direito de um país terceiro. Durante este procedimento, os dados devem ser conservados. Se a ordem for revogada, deve ser emitida uma nova ordem europeia de conservação de provas para permitir à autoridade emissora obter os dados por outras vias, nomeadamente o auxílio judiciário mútuo.

(54) É essencial que todas as pessoas cujos dados sejam solicitados em investigações ou processos penais tenham acesso a vias de recurso efetivo, em conformidade com o artigo 47.º da Carta dos Direitos Fundamentais da União Europeia. No que respeita às pessoas suspeitas e arguidas, o direito a vias de recurso efetivo deve ser exercido no âmbito do processo penal, o que pode afetar a admissibilidade, ou consoante o caso, o valor das provas obtidas por esses meios. Além disso, beneficiam de todas as garantias processuais que lhes são aplicáveis, como o direito à informação. As outras pessoas (que não sejam suspeitas ou arguidas) também devem ter direito a vias de recurso

efetivo. Por conseguinte, deve ser prevista, no mínimo, a possibilidade de contestar a legalidade de uma ordem europeia de entrega de provas, incluindo a necessidade e a proporcionalidade da mesma. O regulamento não deve limitar os fundamentos possíveis para contestar a legalidade da ordem. O direito a ação deve ser exercido no Estado de emissão, em conformidade com o direito nacional. As regras relativas à aplicação de medidas provisórias devem reger-se pelo direito nacional.

(55) Além disso, durante o procedimento de execução coerciva e a via de recurso subsequente, o destinatário pode opor-se à execução de uma ordem europeia de entrega ou de conservação de provas com base em fundamentos limitados, nomeadamente esta não ter sido emitida ou validada por uma autoridade competente ou ser evidente que o seu cumprimento viola manifestamente a Carta dos Direitos Fundamentais da União Europeia ou é manifestamente abusivo. Por exemplo, uma ordem em que se solicite dados de conteúdo pertencentes a uma classe indefinida de pessoas localizadas numa área geográfica ou sem ligação a procedimentos penais específicos ignoraria de forma manifesta as condições aplicáveis à emissão de uma ordem europeia de entrega de provas.

(56) A proteção das pessoas singulares, no que respeita ao tratamento de dados pessoais, é um direito fundamental. Em conformidade com o artigo 8.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia e o artigo 16.º, n.º 1, do TFUE, todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. Ao aplicarem o regulamento, os Estados-Membros devem assegurar que os dados pessoais são protegidos e só poderão ser tratados nos termos do Regulamento (UE) 2016/679 e da Diretiva (UE) 2016/680.

(57) Os dados pessoais obtidos ao abrigo do regulamente só devem ser tratados quando for necessário e devem ser proporcionados em relação aos fins de prevenção, investigação, deteção de crimes e exercício da ação penal, ou com a aplicação de sanções penais e o exercício do direito de defesa. Concretamente, os Estados-Membros devem assegurar que, para efeitos do regulamento, serão aplicadas políticas e medidas adequadas em matéria de proteção de dados quanto à transmissão de dados pessoais pelas autoridades competentes a prestadores de serviços, incluindo medidas para garantir a segurança desses dados. Os prestadores de serviços devem assegurar o mesmo no que se refere à transmissão de dados pessoais às autoridades competentes. Só as pessoas autorizadas podem ter acesso a informações que contenham dados pessoais passíveis de ser obtidos por processos de autenticação. Deve ser ponderada a possibilidade de utilizar mecanismos que garantam a autenticidade, como os sistemas nacionais de identificação eletrónica ou os serviços de confiança previstos no 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.

(58) A Comissão deverá efetuar uma avaliação do regulamento com base em cinco critérios – eficiência, eficácia, pertinência, coerência e valor acrescentado da UE –, que servirá de base às avaliações de impacto de eventuais medidas futuras. Devem ser recolhidas regularmente informações que possam servir de base à avaliação do regulamento.

(59) A utilização de formulários normalizados pré-traduzidos facilita a cooperação e o intercâmbio de informações entre as autoridades judiciais e os prestadores de serviços, permitindo-lhes proteger e transmitir provas eletrónicas de forma mais rápida e eficaz

e, ao mesmo tempo, cumprir os necessários requisitos de segurança de uma forma acessível. Permite igualmente reduzir os custos de tradução, contribuindo para que sejam apresentados pedidos de elevada qualidade. De forma idêntica, os formulários de resposta devem permitir um intercâmbio de informações normalizado, nomeadamente nos casos em que os prestadores de serviços não possam cumprir as suas obrigações porque a conta não existe ou porque não existem dados disponíveis. Os formulários devem permitir igualmente a recolha de dados estatísticos.

(60) A fim de poder responder eficazmente à eventual necessidade de melhorar o conteúdo dos COEEP e dos COECP, bem como do formulário a utilizar para fornecer informações sobre a impossibilidade de executar o COEEP ou o COECP, deve ser delegado na Comissão o poder de adotar atos em conformidade com o artigo 290.º do Tratado sobre o Funcionamento da União Europeia no que se refere à alteração dos anexos I, II e III do regulamento. É especialmente importante que a Comissão proceda às consultas adequadas durante os trabalhos preparatórios, nomeadamente a nível de peritos, e que essas consultas sejam conduzidas de acordo com os princípios consagrados no Acordo Interinstitucional «Legislar Melhor», de 13 de abril de 2016[40]. Mais concretamente, a fim de assegurar a igualdade de participação na preparação dos atos delegados, o Parlamento Europeu e o Conselho deverão receber todos os documentos ao mesmo tempo que os peritos dos Estados-Membros, e os respetivos peritos deverão ter sistematicamente acesso às reuniões dos grupos de peritos da Comissão que tratam da preparação dos atos delegados.

(61) As medidas tomadas com base no regulamento não podem substituir as decisões europeias de investigação previstas na Diretiva 2014/41/UE do Parlamento Europeu e do Conselho[41] para a obtenção de provas eletrónicas. As autoridades dos Estados-Membros devem adotar o instrumento mais adaptado à respetiva situação; podem optar por recorrer a uma decisão europeia de investigação para solicitar um conjunto de diferentes tipos de medidas de investigação e, nomeadamente, a obtenção de provas eletrónicas junto de outro Estado-Membro.

(62) Em virtude da evolução tecnológica, poderão vir a surgir novas formas de instrumentos de comunicação dentro de alguns anos ou surgir lacunas na aplicação do regulamento. Por conseguinte, importa prever uma revisão da sua aplicação.

(63) Atendendo a que o objetivo do regulamento, nomeadamente melhorar a obtenção e a conservação a nível transnacional de provas eletrónicas, não pode ser suficientemente alcançado pelos Estados-Membros em virtude do seu caráter transnacional, mas pode ser mais bem alcançado à escala da União, a União pode tomar medidas em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do Tratado da União Europeia. Em conformidade com o princípio da proporcionalidade consagrado no mesmo artigo, o presente regulamento não excede o necessário para alcançar esses objetivos.

(64) Nos termos do artigo 3.º do Protocolo sobre a 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, [*o Reino Unido e a*

---

40 JO L 123 de 12.5.2016, p. 1.

41 Diretiva 2014/41/UE, de 3 de abril de 2014, relativa à ordem europeia de investigação em matéria penal (JO L 130, 1.5.2014, p. 1).

Irlanda notificaram que desejam participar na aprovação e aplicação do presente regulamento] ou [sem prejuízo do disposto no artigo 4.º do mesmo Protocolo, o Reino Unido e a Irlanda não participam na aprovação do presente regulamento, não ficando por ele vinculados nem sujeitos à sua aplicação.].

(65) 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, este país não participa na adoção do presente regulamento, não ficando por ele vinculado nem sujeito à sua aplicação.

(66) A Autoridade Europeia para a Proteção de Dados foi consultada em conformidade com o artigo 28.º, n.º 2, do Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho[42], tendo emitido parecer em (...)[43],

ADOTARAM O PRESENTE REGULAMENTO:

Capítulo 1: Objeto, definições e âmbito de aplicação

Artigo 1.°
Objeto

1. O presente regulamento estabelece as normas segundo as quais uma autoridade de um Estado-Membro pode ordenar a um prestador de serviços que opera na União que entregue ou conserve em seu poder provas eletrónicas, independentemente da localização dos dados em causa. O presente regulamento não prejudica as competências das autoridades nacionais para obrigar os prestadores de serviços estabelecidos ou representados no seu território a cumprir medidas nacionais semelhantes.

2. O presente regulamento não afeta a obrigação de respeitar os direitos fundamentais e os princípios jurídicos consagrados no artigo 6.º do TUE, incluindo os direitos de defesa das pessoas sujeitas a ação penal, nem prejudica as obrigações que nesta matéria incumbam às autoridades policiais ou judiciais.

Artigo 2.°
Definições

Para efeitos do presente regulamento, entende-se por:

---

42 Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos da Comunidade e à livre circulação desses dados (JO L 8 de 12.1.2001, p. 1).

43 JO C , , p. .

(1) «ordem europeia de entrega de provas» uma decisão vinculativa de uma autoridade emissora de um Estado-Membro que obriga um prestador de serviços que opere na União e esteja estabelecido ou representado noutro Estado-Membro a fornecer provas eletrónicas;

(2) «ordem europeia de conservação de provas» uma decisão vinculativa de uma autoridade emissora de um Estado-Membro que obriga um prestador de serviços que opere na União e esteja estabelecido ou representado noutro Estado-Membro a conservar provas eletrónicas, tendo em vista um pedido de entrega de provas subsequente;

(3) «prestador de serviços» uma pessoa singular ou coletiva que presta uma ou mais das seguintes categorias de serviços:

(a) serviços de comunicações eletrónicas, na aceção do artigo 2.º, n.º 4, da [Diretiva que estabelece o Código Europeu das Comunicações Eletrónicas];

(b) serviços da sociedade da informação, na aceção do artigo 1.º, n.º 1, alínea b), da Diretiva (UE) 2015/1535 do Parlamento Europeu e do Conselho[44], para os quais o armazenamento de dados seja uma componente determinante do serviço prestado ao utilizador, incluindo as redes sociais, os mercados em linha que facilitam transações entre os utilizadores, e outros serviços de alojamento;

(c) serviços de nomes de domínio da Internet e de numeração IP, tais como fornecedores de endereços IP, registos de nomes de domínio, agentes de registo de nomes de domínio e serviços de privacidade e de proxy;

(4) «prestação de serviços na União»:

(a) uma atividade que permite às pessoas singulares ou coletivas localizadas num ou mais Estados-Membros utilizar os serviços enumerados no ponto 3 supra; e ainda

(b) uma atividade que possui uma ligação significativa ao(s) Estado-Membro(s) a que se refere a alínea a);

(5) «estabelecimento» o exercício efetivo de uma atividade económica por tempo indeterminado e através de uma infraestrutura estável a partir da qual a prestação de serviços é assegurada, ou uma infraestrutura estável a partir da qual a atividade é gerida;

(6) «prova eletrónica» uma prova armazenada em formato eletrónico por ou em nome de um prestador de serviços no momento da receção de um certificado de ordem europeia de entrega ou de conservação de provas, constituída por dados de assinantes, dados de acesso, dados transacionais ou dados de conteúdo armazenados;

(7) «dados de assinantes» dados relativos:

---

[44] Diretiva (UE) 2015/1535 do Parlamento Europeu e do Conselho, de 9 de setembro de 2015, relativa a um procedimento de informação no domínio das regulamentações técnicas e das regras relativas aos serviços da sociedade da informação (JO L 241 de 17.9.2015, p. 1).

(a) à identidade de um assinante ou cliente, tais como o nome fornecido, a data de nascimento, o endereço postal ou geográfico, os dados de faturação e pagamento, o número de telefone ou o endereço eletrónico;

(b) ao tipo de serviço e respetiva duração, incluindo dados técnicos e dados que identifiquem medidas técnicas associadas ou interfaces fornecidas ao assinante ou cliente ou por ele utilizadas, e dados relacionados com a validação da utilização do serviço, com exceção de palavras-passe ou outros meios de identificação utilizados em substituição de uma palavra-passe, que sejam fornecidos por um utilizador ou criados a pedido do mesmo;

(8) «dados de acesso» dados relacionados com o início e o fim da sessão de acesso de um utilizador a um serviço, os quais são estritamente necessários apenas para identificar o utilizador do serviço, tais como a data e hora da utilização ou do início (*log-in*) e do fim (*log-off*) da ligação ao serviço, juntamente com o endereço do protocolo IP atribuído pelo fornecedor do serviço de acesso à Internet ao utilizador de um serviço, dados que identifiquem a interface utilizada e o código de identificação do utilizador. Estes dados incluem os metadados das comunicações eletrónicas, na aceção do artigo 4.º, n.º 3, alínea c), do [Regulamento relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas];

(9) «dados transacionais» dados relacionados com a prestação de um serviço por um prestador de serviços que servem para fornecer contexto ou informações adicionais sobre esse serviço e são gerados ou tratados por um sistema de informação do prestador de serviços, tais como o remetente e o destinatário de uma mensagem ou de outro tipo de interação, dados sobre a localização do dispositivo, a data, a hora, a duração, o tamanho, a via, o formato, o protocolo utilizado e o tipo de compressão, exceto se se tratar de dados de acesso. Estes dados incluem os dados das comunicações eletrónicas, na aceção do artigo 4.º, n.º 3, alínea c), do [Regulamento relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas];

(10) «dados de conteúdo» dados armazenados num formato digital, como texto, voz, vídeos, imagens e som, que não sejam dados de assinantes, dados de acesso ou dados transacionais;

(11) «sistema de informação» um sistema de informação na aceção do artigo 2.º, alínea a), da Diretiva 2013/40/UE do Parlamento Europeu e do Conselho[45];

(12) «Estado de emissão», o Estado-Membro que emitiu a ordem europeia de entrega de provas ou a ordem europeia de conservação de provas;

(13) «Estado de execução», o Estado-Membro no qual reside ou está estabelecido o destinatário da ordem europeia de entrega ou de conservação de provas e ao qual a ordem em causa e respetivo certificado devem ser transmitidos para execução;

---

[45] Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho (JO L 218 de 14.8.2013, p. 8).

(14) «autoridade de execução», a autoridade competente do Estado de execução à qual a ordem europeia de entrega de provas e o respetivo certificado ou a ordem europeia de conservação de provas e o respetivo certificado devem ser transmitidos pela autoridade emissora, para execução.

(15) «situações de urgência», as situações em que existe uma ameaça iminente à vida ou à integridade física de uma pessoa ou a uma infraestrutura crítica, na aceção do artigo 2.º, alínea a), da Diretiva 2008/114/CE do Conselho[46].

Artigo 3.°
Âmbito de aplicação

1. O presente regulamento é aplicável aos prestadores de serviços que operam na União.

2. As ordens europeias de entrega ou de conservação de provas só podem ser emitidas no âmbito de processos penais, tanto durante a fase de instrução como durante a fase de julgamento. Também podem ser emitidas no âmbito de processos relacionados com infrações penais pelas quais uma pessoa coletiva possa ser responsabilizada ou punida no Estado de emissão.

3. As ordens previstas no presente regulamento só podem emitidas em relação a dados relativos a serviços, tal como definidos no artigo 2.º, n.º 3, prestados na União.

Capítulo 2: Ordem europeia de entrega de provas, ordem europeia de conservação de provas e respetivos certificados

Artigo 4.°
Autoridade emissora

1. A ordem europeia de entrega de dados de assinantes ou de dados de acesso pode ser emitida por:

   (a) um juiz, um tribunal, um juiz de instrução ou um magistrado do Ministério Público que seja competente no processo em causa; ou

   (b) qualquer outra autoridade competente, tal como definida pelo Estado de emissão, e que, no processo em causa, intervenha enquanto autoridade de investigação num processo penal com competência para ordenar a recolha de elementos de prova de acordo com a lei nacional. A ordem deve ser validada, após a análise da sua conformidade com as condições de emissão de uma ordem europeia de entrega de provas ao abrigo do presente regulamento, por

[46] Diretiva 2008/114/CE do Conselho, de 8 de dezembro de 2008, relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção (JO L 345 de 23.12.2008, p. 75).

um juiz, um tribunal, um juiz de instrução ou um magistrado do Ministério Público do Estado de emissão.

2. A ordem europeia de entrega de dados transacionais ou de dados de conteúdo pode ser emitida por:

(a) um juiz, um tribunal ou um juiz de instrução que seja competente no processo em causa; ou

(b) qualquer outra autoridade competente, tal como definida pelo Estado de emissão, e que, no processo em causa, intervenha enquanto autoridade de investigação num processo penal com competência para ordenar a recolha de elementos de prova de acordo com a lei nacional. A ordem deve ser validada, após a análise da sua conformidade com as condições de emissão de uma ordem europeia de entrega de provas ao abrigo do presente regulamento, por um juiz, um tribunal ou um juiz de instrução do Estado de emissão.

3. A ordem europeia de conservação de provas pode ser emitida por:

(a) um juiz, um tribunal, um juiz de instrução ou um magistrado do Ministério Público que seja competente no processo em causa; ou

(b) qualquer outra autoridade competente, tal como definida pelo Estado de emissão, e que, no processo em causa, intervenha enquanto autoridade de investigação num processo penal com competência para ordenar a recolha de elementos de prova de acordo com a lei nacional. A ordem deve ser validada, após a análise da sua conformidade com as condições de emissão de uma ordem europeia de conservação de provas ao abrigo do presente regulamento, por um juiz, um tribunal, um juiz de instrução ou um magistrado do Ministério Público do Estado de emissão.

4. Sempre que a ordem tenha sido validada por uma autoridade judicial nos termos do n.º 1, alínea b), do n.º 2, alínea b), e do n.º 3, alínea b), essa autoridade também pode ser considerada como autoridade emissora para efeitos da transmissão do certificado de ordem europeia de entrega de provas ou do certificado de ordem europeia de conservação de provas.

Artigo 5.°
Condições de emissão de uma ordem europeia de entrega de provas

1. A autoridade emissora só pode emitir uma ordem europeia de entrega de provas se estiverem preenchidas as condições previstas no presente artigo.

2. A ordem europeia de entrega de provas deve ser necessária e proporcionada para efeitos dos processos a que se refere o artigo 3.º, n.º 2, só podendo ser emitida se existir uma medida semelhante para a mesma infração penal numa situação nacional comparável no Estado de emissão.

3. As ordens europeias de entrega de dados de assinantes e de dados de acesso podem ser emitidas para todas as infrações penais.

4. As ordens europeias de entrega de dados transacionais ou de dados de conteúdo só podem ser emitidas

(a) para infrações penais puníveis no Estado de emissão com uma pena privativa de liberdade de duração máxima não inferior a três anos, ou

(b) para as infrações seguintes, se forem cometidas, total ou parcialmente, através de um sistema de informação:

– as infrações definidas nos artigos 3.º, 4.º e 5.º da Decisão-Quadro 2001/413/JAI do Conselho[47];

– as infrações definidas nos artigos 3.º a 7.º da Diretiva 2011/93/UE do Parlamento Europeu e do Conselho[48];

– as infrações definidas nos artigos 3.º a 8.º da Diretiva 2013/40/UE do Parlamento Europeu e do Conselho;

(c) as infrações definidas nos artigos 3.º a 12.º e no 14.º da Diretiva (UE) 2017/541 do Parlamento Europeu e do Conselho[49]

5. A ordem europeia de entrega de provas deve incluir as seguintes informações:

(a) a autoridade emissora e, se for caso disso, a autoridade de validação;

(b) o destinatário da ordem europeia de entrega de provas a que se refere o artigo 7.º;

(c) a pessoa cujos dados são solicitados, salvo quando o objetivo único da ordem seja identificar uma pessoa;

(d) o tipo de dados solicitados (dados de assinantes, dados de acesso, dados transacionais ou dados de conteúdo);

(e) se aplicável, o período de tempo fixado para os dados serem facultados:

(f) as disposições aplicáveis do direito penal do Estado de emissão;

(g) em caso de urgência ou de pedido de divulgação antecipada, a respetiva fundamentação;

(h) nos casos em que os dados solicitados sejam armazenados ou tratados no contexto de uma infraestrutura fornecida por um prestador de serviços a uma

---

47 Decisão-Quadro 2001/413/JAI do Conselho, de 28 de maio de 2001, relativa ao combate à fraude e à falsificação de meios de pagamento que não em numerário (JO L 149 de 2.6.2001, p. 1).

48 Diretiva 2011/93/UE do Parlamento Europeu e do Conselho, de 13 de dezembro de 2011, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, e que substitui a Decisão-Quadro 2004/68/JAI do Conselho (JO L 335 de 17.12.2011, p. 1).

49 Diretiva (UE) 2017/541 do Parlamento Europeu e do Conselho, de 15 de março de 2017, relativa à luta contra o terrorismo e que substitui a Decisão-Quadro 2002/475/JAI do Conselho e altera a Decisão 2005/671/JAI do Conselho (JO L 88 de 31.3.2017, p. 6).

empresa ou a outra entidade que não seja uma pessoa singular, a confirmação de que a ordem é emitida em conformidade com o disposto no n.º 6;

(i) a fundamentação quanto à necessidade e à proporcionalidade da medida.

6. Quando os dados solicitados sejam armazenados ou tratados no contexto de uma infraestrutura empresarial fornecida por um prestador de serviços a uma empresa ou a outra entidade que não seja uma pessoa singular, a ordem europeia de entrega de provas só pode ser notificada ao prestador de serviços se as medidas de investigação dirigidas à empresa ou à entidade não forem adequadas, nomeadamente porque podem comprometer a investigação.

7. Se a autoridade emissora tiver razões para crer que os dados transacionais ou de conteúdo solicitados estão protegidos por imunidades e privilégios reconhecidos pelo direito do Estado-Membro do prestador de serviços destinatário, ou que a sua divulgação pode afetar interesses fundamentais desse Estado-Membro em matéria de segurança ou defesa nacional, deve solicitar esclarecimentos antes de emitir a ordem europeia de entrega de provas, nomeadamente consultando as autoridades competentes desse Estado-Membro, quer diretamente quer através da Eurojust ou da Rede Judiciária Europeia. Se a autoridade emissora considerar que os dados de acesso, transacionais ou de conteúdo solicitados estão protegidos por tais imunidades e privilégios ou que a sua divulgação afetaria interesses fundamentais do Estado-Membro, deve abster-se de emitir a ordem europeia de entrega de provas.

Artigo 6.°
Condições de emissão de uma ordem europeia de conservação de provas

1. A autoridade emissora só pode emitir uma ordem europeia de conservação de provas se estiverem preenchidas as condições previstas no presente artigo.

2. A ordem só pode ser emitida se for necessária e proporcionada para impedir a remoção, a eliminação ou a alteração dos dados, tendo em vista um pedido subsequente para a sua entrega através de auxílio judiciário mútuo, de uma decisão europeia de investigação ou de uma ordem europeia de entrega de provas. As ordens europeias de conservação de provas podem ser emitidas para todas as infrações penais.

3. A ordem europeia de conservação de provas deve incluir as seguintes informações:

(a) a autoridade emissora e, se for caso disso, a autoridade de validação;

(b) o destinatário da ordem europeia de conservação de provas a que se refere o artigo 7.º;

(c) a pessoa cujos dados devem ser conservados, exceto se o objetivo único da ordem for identificar uma pessoa;

(d) o tipo de dados a conservar (dados de assinantes, dados de acesso, dados transacionais ou dados de conteúdo);

(e) se for caso disso, o período de tempo solicitado para a conservação dos dados;

(f) as disposições aplicáveis do direito penal do Estado de emissão;

(g) a fundamentação quanto à necessidade e à proporcionalidade da medida.

Artigo 7.°
Destinatário da ordem europeia de entrega de provas ou da ordem europeia de conservação de provas

1. A ordem europeia de entrega de provas e a ordem europeia de conservação de provas devem ser notificadas diretamente ao representante legal designado pelo prestador de serviços para efeitos de recolha de provas em processo penal.

2. Caso não tenha sido designado um representante legal, a ordem europeia de entrega de provas e a ordem europeia de conservação de provas podem ser notificadas em qualquer estabelecimento do prestador de serviços na União.

3. Se o representante legal não der cumprimento a um COEEP numa situação de urgência nos termos do artigo 9.º, nº 2, poderá ser notificado em qualquer estabelecimento do prestador de serviços na União.

4. Se o representante legal não cumprir as suas obrigações nos termos dos artigos 9.º ou 10.º e a autoridade emissora considerar que existe um risco grave de perda de dados, a ordem europeia de entrega de provas e a ordem europeia de conservação de provas podem ser notificadas em qualquer estabelecimento do prestador de serviços na União.

Artigo 8.°
Certificados de ordem europeia de entrega de provas ou de conservação de provas

1. A ordem europeia de entrega ou de conservação de provas deve ser transmitida ao destinatário a que se refere o artigo 7.º através de um certificado de ordem europeia de entrega de provas (COEEP) ou de um certificado de ordem europeia de conservação de provas (COECP).

   A autoridade emissora ou a autoridade de validação deve preencher e assinar o COEEP que consta do anexo I ou o COECP que consta do anexo II, atestando a veracidade e a exatidão do seu conteúdo.

2. O COEEP ou o COECP deve ser transmitido diretamente através de qualquer meio que permita produzir um registo escrito em condições que permitam ao destinatário verificar a sua autenticidade.

   Se os prestadores de serviços, os Estados-Membros ou a União tiverem criado plataformas específicas ou outros canais seguros para tratar os pedidos de dados

apresentados pelas autoridades policiais e judiciais, a autoridade emissora pode optar por transmitir o certificado através desses canais.

3. O COEEP deve conter as informações enumeradas no artigo 5.º, n.º 5, alíneas a) a h), bem como informações suficientes que permitam ao destinatário identificar e contactar a autoridade emissora. Não deve ser incluída a fundamentação quanto à necessidade e à proporcionalidade da medida ou outras informações relativas às investigações.

4. O COECP deve conter as informações enumeradas no artigo 6.º, n.º 3, alíneas a) a f), bem como informações suficientes que permitam ao destinatário identificar e contactar a autoridade emissora. Não deve ser incluída a fundamentação quanto à necessidade e à proporcionalidade da medida ou outras informações relativas às investigações.

5. Se necessário, o COEEP ou o COECP deve ser traduzido para uma língua oficial da União aceite pelo destinatário. Caso não seja indicada qualquer língua, o COEEP ou o COECP deve ser traduzido para uma das línguas oficiais do Estado-Membro no qual o representante legal reside ou está estabelecido.

Artigo 9.°
Execução do certificado de ordem europeia de entrega de provas

1. Após a receção do COEEP, o destinatário deve assegurar que os dados solicitados são transmitidos diretamente à autoridade emissora ou às autoridades policiais, conforme indicado no certificado, o mais tardar, no prazo de dez dias após a sua receção, a menos que esta autoridade indique motivos para a sua divulgação antecipada.

2. Em situações de urgência, o destinatário deve transmitir os dados solicitados sem demora indevida, o mais tardar seis horas após ter recebido o COEEP.

3. Se o destinatário não puder cumprir a sua obrigação por o COEEP estar incompleto, conter erros manifestos ou não conter informações suficientes para a sua execução, deve informar a autoridade emissora indicada no certificado sem demora indevida e solicitar esclarecimentos, utilizando o formulário constante do anexo III, bem como comunicar à autoridade emissora se foi ou não possível efetuar a identificação e conservação dos dados, como previsto no n.º 6. A autoridade emissora deve responder de forma expedita e, o mais tardar, no prazo de cinco dias. Os prazos fixados nos n.ºs 1 e 2 não são aplicáveis enquanto não forem prestados os esclarecimentos solicitados.

4. Se o destinatário não puder cumprir a obrigação por motivo de força maior ou devido a uma impossibilidade de facto que não lhe seja imputável ou, se for caso disso, ao prestador de serviços, nomeadamente porque a pessoa cujos dados são solicitados não é seu cliente ou os dados foram eliminados antes da receção do COEEP, deve informar a autoridade emissora indicada no certificado sem demora indevida e explicar os motivos, utilizando o formulário constante do anexo III. Se as condições pertinentes estiverem preenchidas, a autoridade emissora deve revogar o COEEP.

5. Se o destinatário não fornecer as informações solicitadas de forma exaustiva e dentro do prazo previsto por outros motivos, deve comunicá-los à autoridade emissora sem demora indevida e, o mais tardar, nos prazos fixados nos n.os 1 e 2, utilizando o formulário constante do anexo III. A autoridade emissora reaprecia a ordem em função das informações fornecidas pelo prestador de serviços e, se necessário, fixa um novo prazo para a entrega dos dados em causa.

   Se o destinatário considerar que o COEEP não pode ser executado devido ao facto de ser evidente, com base unicamente nas informações nele contidas, que viola manifestamente a Carta dos Direitos Fundamentais da União Europeia ou é manifestamente abusivo, deve igualmente enviar o formulário constante do anexo III à autoridade de execução competente do seu Estado-Membro. Nesses casos, a autoridade de execução competente pode solicitar à autoridade emissora esclarecimentos sobre a ordem europeia de entrega de provas, quer diretamente quer através da Eurojust ou da Rede Judiciária Europeia.

6. O destinatário deve conservar os dados solicitados, se não os entregar de imediato, a menos que as informações constantes do COEEP não lhe permitam identificar esses dados, caso em que deve solicitar esclarecimentos em conformidade com o n.º 3. Os dados deve ser conservados até serem entregues, independentemente dessa entrega ter lugar com base na ordem europeia de entrega de provas clarificada e no respetivo certificado ou por outras vias, nomeadamente o auxílio judiciário mútuo. Se a entrega e conservação dos dados deixarem de ser necessárias, a autoridade emissora e, se for caso disso, nos termos do artigo 14.º, n.º 8, a autoridade de execução devem informar o destinatário sem demora indevida.

Artigo 10.°
Execução do certificado de ordem europeia de conservação de provas (COECP)

1. Após a receção do COECP, o destinatário deve, sem demora indevida, conservar os dados solicitados. Os dados devem ser conservados por um prazo de 60 dias, salvo se a autoridade emissora entretanto confirmar que foi emitido o pedido de entrega de provas subsequente.

2. Se a autoridade emissora confirmar, dentro do prazo fixado no n.º 1, que foi emitido o pedido de entrega de provas subsequente, o destinatário deve conservar os dados durante o tempo necessário para os dados serem entregues, uma vez recebido o referido pedido.

3. Se a conservação deixar de ser necessária, a autoridade emissora deve informar o destinatário sem demora indevida.

4. Se o destinatário não puder cumprir a sua obrigação por o certificado estar incompleto, conter erros manifestos ou não conter informações suficientes para a sua execução, deve informar a autoridade emissora indicada no COECP sem demora indevida e solicitar esclarecimentos, utilizando o formulário constante do anexo III. A autoridade emissora deve responder de forma expedita e, o mais tardar, no prazo de cinco dias. O destinatário deve assegurar que, do seu lado, pode receber os esclarecimentos necessários para cumprir a obrigação prevista no n.º 1.

5. Se o destinatário não puder cumprir a sua obrigação por motivo de força maior ou devido uma impossibilidade de facto que não lhe seja imputável ou, se for caso disso, ao prestador de serviços, nomeadamente porque a pessoa cujos dados são solicitados não é seu cliente ou os dados foram eliminados antes da receção da ordem, deve informar a autoridade emissora indicada no COECP sem demora indevida e explicar os motivos, utilizando o formulário constante do anexo III. Se as condições pertinentes estiverem preenchidas, a autoridade emissora deve revogar o COECP.

6. Se o destinatário não conservar os dados solicitados por qualquer outro motivo, dos enumerados no formulário constante do anexo III, deve comunicar o motivo à autoridade emissora sem demora indevida, utilizando o formulário constante do anexo III. Esta deve reapreciar a ordem à luz da justificação fornecida pelo prestador de serviços.

Artigo 11.°
Confidencialidade e informação do utilizador

1. Os destinatários e, quando seja caso disso, os prestadores de serviços devem adotar todas as medidas necessárias para garantir a confidencialidade do COEEP ou do COECP e dos dados entregues ou conservados e, se solicitado pela autoridade emissora, abster-se de informar a pessoa cujos dados foram solicitados, a fim de não obstruir o processo penal em causa.

2. Se a autoridade emissora tiver instado o destinatário a abster-se de informar a pessoa cujos dados foram solicitados no COEEP, deve informar essa pessoa, sem demora indevida, da entrega dos dados em causa. Essa informação pode ser protelada durante o tempo necessário e proporcionado para impedir a obstrução do processo penal em causa.

3. Ao informar a pessoa, a autoridade emissora deve incluir informações sobre as vias de recurso disponíveis a que se refere o artigo 17.º.

Artigo 12.°
Reembolso dos custos incorridos

O prestador de serviços pode reclamar o reembolso dos custos suportados junto do Estado de emissão, desde que tal esteja previsto no direito nacional desse Estado relativamente às ordens nacionais em situações semelhantes, em conformidade com as disposições nacionais pertinentes.

Capítulo 3: Sanções e execução coerciva

Artigo 13.°
Sanções

Sem prejuízo das disposições de direito nacional que prevejam a imposição de sanções penais, os Estados-Membros devem estabelecer os regimes de coimas aplicáveis à violação das

obrigações impostas pelos artigos 9.º, 10.º e 11.º do presente regulamento, devendo adotar todas as medidas necessárias para garantir a sua aplicação. As coimas previstas devem ser eficazes, proporcionadas e dissuasivas. Os Estados-Membros devem notificar imediatamente à Comissão esses regimes e medidas, bem como qualquer alteração dos mesmos, sem demora indevida.

Artigo 14.°
Procedimento de execução coerciva

1. Se o destinatário não der cumprimento a um COEEP no prazo previsto ou não der cumprimento a um COECP sem indicar motivos aceites pela autoridade emissora, esta poderá transferir para a autoridade competente do Estado de execução a ordem europeia de entrega de provas, acompanhada do COEEP, ou a ordem europeia de conservação de provas, acompanhada do COECP, bem como o formulário constante do anexo III preenchido pelo destinatário e qualquer outro documento pertinente para a sua execução coerciva, por qualquer meio que permita produzir um registo escrito em condições que permitam à autoridade de execução determinar a sua autenticidade. Para o efeito, a autoridade emissora deve traduzir a ordem, o formulário e quaisquer outros documentos que os acompanhem para uma das línguas oficiais desse Estado-Membro e informar o destinatário da realização dessa transferência.

2. Após a sua receção, a autoridade de execução deve, sem outras formalidades, reconhecer uma ordem europeia de entrega de provas ou uma ordem europeia de conservação de provas transmitida em conformidade com o n.º 1, adotando as medidas necessárias para a sua execução, a menos que considere que se aplica qualquer dos fundamentos previstos nos n.os 4 ou 5 ou que os dados em causa estão protegidos por uma imunidade ou privilégio reconhecido pelo direito nacional ou que a sua divulgação pode afetar os seus interesses fundamentais em matéria de segurança e defesa nacional. A autoridade de execução deve reconhecer a ordem sem demora indevida e, o mais tardar, cinco dias úteis após a receção da mesma.

3. Se a autoridade de execução reconhecer a ordem emitida, deve solicitar formalmente ao destinatário que cumpra as obrigações em causa, informando-o da possibilidade de se opor à execução invocando um dos fundamentos enumerados nos n.os 4 ou 5, bem como das sanções aplicáveis em caso de incumprimento, fixando um prazo para este dar cumprimento ou deduzir oposição.

4. O destinatário só pode opor-se à execução da ordem europeia de entrega de provas com base num dos seguintes fundamentos:

   (a) a ordem não tenha sido emitida ou validada por uma autoridade emissora, como previsto no artigo 4.º;

   (b) a ordem não tenha sido emitida para uma das infrações penais previstas no artigo 5.º, n.º 4;

(c) o destinatário não tenha podido dar cumprimento ao COEEP em virtude de uma impossibilidade de facto ou de um motivo de força maior, ou por o certificado conter erros manifestos;

(d) a ordem não diga respeito a dados armazenados por ou em nome do prestador de serviços à data da receção do COEEP;

(e) o serviço não seja abrangido pelo âmbito de aplicação do presente regulamento;

(f) com base unicamente nas informações constantes do COEEP, seja evidente que viola manifestamente a Carta dos Direitos Fundamentais ou é manifestamente abusivo.

5. O destinatário só pode opor-se à execução da ordem europeia de conservação de provas com base nos seguintes fundamentos:

(a) a ordem não tenha sido emitida ou validada por uma autoridade emissora, como previsto no artigo 4.º;

(b) o destinatário não tenha podido dar cumprimento ao COECP em virtude de uma impossibilidade de facto ou de um motivo de força maior, ou por o certificado conter erros manifestos;

(c) a ordem não diga respeito a dados armazenados por ou em nome do prestador de serviços à data da receção do COECP;

(d) o serviço não seja abrangido pelo âmbito de aplicação do presente regulamento;

(e) com base unicamente nas informações constantes do COECP, seja evidente que viola manifestamente a Carta dos Direitos Fundamentais ou é manifestamente abusivo.

6. Em caso de oposição do destinatário, a autoridade de execução deve decidir se faz executar a ordem com base nas informações prestadas por este e, se necessário, com base em informações suplementares obtidas junto da autoridade emissora, nos termos do n.º 7.

7. Antes de decidir não reconhecer ou fazer executar a ordem em conformidade com o disposto nos n.os 2 e 6, a autoridade de execução deve consultar a autoridade emissora por um meio adequado. Se for caso disso, deve solicitar-lhe informações suplementares, devendo esta responder no prazo de cinco dias úteis.

8. Todas as decisões devem ser notificadas de imediato à autoridade emissora e ao destinatário, por um meio que permita produzir um registo escrito.

9. Se a autoridade de execução obtiver os dados junto do destinatário, deve transmiti-los à autoridade emissora no prazo de dois dias úteis, a menos que estes estejam protegidos por uma imunidade ou um privilégio ao abrigo do direito nacional ou afetem os interesses fundamentais nacionais em matéria de segurança e defesa.

Nesse caso, deve comunicar à autoridade emissora os motivos para não transmitir os dados.

10. Se o destinatário não cumprir as obrigações que lhe incumbem por força de uma ordem reconhecida cuja força executória tenha sido confirmada pela autoridade de execução, essa autoridade deve impor uma coima em conformidade com o direito nacional, o qual deverá prever vias de recurso efetivo contra a decisão de imposição da coima.

Capítulo 4: Vias de recurso

Artigo 15.°
Procedimento de reexame em caso de obrigações contraditórias em virtude dos direitos fundamentais ou dos interesses fundamentais de um país terceiro

1. Se o destinatário considerar que o cumprimento da ordem europeia de entrega de provas entraria em conflito com o direito aplicável de um país terceiro que proíba a divulgação dos dados em apreço com o fundamento de que essa proibição é necessária para proteger os direitos fundamentais das pessoas em causa ou os interesses fundamentais desse país em matéria de segurança e defesa nacional, deve comunicar à autoridade de execução os motivos para não cumprir a ordem europeia de entrega de provas, em conformidade com o procedimento previsto no artigo 9.º, n.º 5.

2. A oposição fundamentada deve incluir todas as informações pertinentes relativas ao direito do país terceiro, à sua aplicabilidade ao processo em apreço e à natureza da obrigação contraditória. Não pode assentar no facto de não existirem disposições semelhantes relativas às condições, formalidades e procedimentos de emissão de uma ordem de entrega de provas no direito aplicável do país terceiro, nem na circunstância única de os dados estarem armazenados num país terceiro.

3. A autoridade emissora deve reapreciar a ordem europeia de entrega de provas com base na oposição fundamentada. Se pretender confirmar a ordem europeia de entrega de provas, deve solicitar um reexame pelo tribunal competente do seu Estado-Membro. A execução da ordem ficará suspensa na pendência desse reexame.

   O tribunal competente deve primeiro determinar se existe ou não um conflito, com base numa avaliação sobre se

   (a) o direito do país terceiro se aplica nas circunstâncias específicas do processo em apreço e, se for esse o caso,

   (b) o direito do país terceiro, quando aplicado às circunstâncias específicas do processo em apreço, proíbe a divulgação dos dados em causa.

4. Ao proceder a essa avaliação, o tribunal deve ter em conta se o direito do país terceiro em causa, em vez de ter por objetivo proteger os direitos fundamentais das pessoas em causa ou os interesses fundamentais desse país em matéria de segurança

ou defesa nacional, visa antes manifestamente proteger outros interesses ou atividades ilícitas contra pedidos formulados por autoridades policiais no quadro de investigações penais.

5. Se o tribunal competente concluir que não existe qualquer conflito relevante na aceção dos n.os 1 e 4, deve confirmar a ordem. Se o tribunal competente concluir que existe um conflito relevante na aceção dos n.os 1 e 4, deve transmitir todos os elementos de facto e de direito relativos ao processo, incluindo a sua avaliação, às autoridades centrais do país terceiro em causa, através da sua autoridade central nacional, com um prazo de 15 dias de resposta. Mediante pedido fundamentado da autoridade central do país terceiro, esse prazo poderá ser prorrogado por 30 dias.

6. Se a autoridade central do país terceiro informar o tribunal competente, dentro do prazo previsto, de que se opõe à execução da ordem europeia de entrega de provas no processo em causa, o tribunal competente deve revogar a ordem e informar a autoridade emissora e o destinatário. Caso não seja apresentada qualquer oposição no prazo (prorrogado) aplicável, o tribunal competente deve enviar à autoridade central do país terceiro uma notificação concedendo-lhe um prazo suplementar de cinco dias para responder e a informá-la das consequências dessa omissão. Caso não seja apresentada qualquer oposição dentro desse prazo suplementar, o tribunal competente deve confirmar a ordem.

7. Se decidir que a ordem deve ser confirmada, informará a autoridade emissora e o destinatário, o qual deverá prosseguir com a execução da ordem.

Artigo 16.°

Procedimento de reexame em caso de obrigações contraditórias em virtude de fundamentos

1. Se o destinatário considerar que o cumprimento da ordem europeia de entrega de provas entraria em conflito com o direito aplicável de um país terceiro que proíba a divulgação dos dados em apreço com fundamentos diferentes dos referidos no artigo 15.º, deve comunicar à autoridade de execução os motivos para não dar cumprimento à ordem europeia de entrega de provas, em conformidade com o procedimento a que se refere o artigo 9.º, n.º 5.

2. A oposição fundamentada deve incluir todas as informações pertinentes relativas ao direito do país terceiro, à sua aplicabilidade ao processo em apreço e à natureza da obrigação contraditória. Não pode assentar no facto de não existirem disposições semelhantes relativas às condições, formalidades e procedimentos de emissão de uma ordem de entrega de provas no direito aplicável do país terceiro, nem na circunstância única de os dados estarem armazenados num país terceiro.

3. A autoridade emissora deve reapreciar a ordem europeia de entrega de provas com base na oposição fundamentada. Se pretender confirmar a ordem europeia de entrega de provas, deve solicitar um reexame pelo tribunal competente do seu Estado-Membro. A execução da ordem ficará suspensa na pendência desse reexame.

4. O tribunal competente deve primeiro determinar se existe ou não um conflito, com base numa avaliação sobre se

(a) o direito do país terceiro se aplica nas circunstâncias específicas do processo em apreço e, se for esse o caso,

(b) o direito do país terceiro, quando aplicado às circunstâncias específicas do processo em apreço, proíbe a divulgação dos dados em causa.

5. Se o tribunal competente concluir que não existe qualquer conflito relevante na aceção dos n.os 1 e 4, deve confirmar a ordem. Se o tribunal competente determinar que o direito do país terceiro, quando aplicado às circunstâncias específicas do caso em apreço, proíbe a divulgação dos dados em causa, deve decidir se confirma ou revoga a ordem, nomeadamente, com base nos seguintes fatores:

(a) o interesse protegido pelo direito pertinente do país terceiro, incluindo o interesse do país terceiro em evitar a divulgação dos dados;

(b) o grau de ligação do processo penal para o qual a ordem foi emitida a ambas as jurisdições, indicado, nomeadamente, pelos seguintes elementos:

a localização, nacionalidade e residência da pessoa cujos dados são solicitados e/ou da(s) vítima(s),

o local onde a infração penal foi cometida;

(c) o grau de ligação entre o prestador de serviços e o país terceiro em causa; neste contexto, a localização do armazenamento dos dados, por si só, não é suficiente para estabelecer um grau de ligação importante;

(d) os interesses do Estado de investigação na obtenção das provas em causa, com base na gravidade da infração e na importância da obtenção das provas de forma expedita;

(e) as eventuais consequências para o destinatário ou para o prestador de serviços resultantes do cumprimento da ordem europeia de entrega de provas, incluindo as sanções em que podem incorrer.

6. Se o tribunal competente decidir revogar a ordem, deve informar a autoridade emissora e o destinatário . Se decidir que a ordem deve ser confirmada, informará a autoridade emissora e o destinatário, o qual deverá prosseguir com a execução da ordem.

Artigo 17.°
Vias de recurso efetivo

1. As pessoas suspeitas e arguidas cujos dados tenham sido obtidos através de uma ordem europeia de entrega de provas têm direito a vias de recurso efetivo contra a ordem em causa durante o processo penal para o qual esta tenha sido emitida, sem prejuízo das vias de recurso previstas na Diretiva (UE) 2016/680 e no Regulamento (UE) 2016/679.

2. Se a pessoa cujos dados tenham sido obtidos não for suspeita ou arguida no processo penal para o qual a ordem foi emitida, deve ter direito a vias de recurso efetivo contra

a ordem europeia de entrega de provas no Estado de emissão, sem prejuízo das vias de recurso previstas na Diretiva (UE) 2016/680 e no Regulamento (UE) 2016/679.

3. Esse direito deve ser exercido perante um tribunal do Estado de emissão em conformidade com o direito nacional, devendo incluir a possibilidade de contestar a legalidade da medida, incluindo a sua necessidade e proporcionalidade.

4. Sem prejuízo do disposto no artigo 11.º, a autoridade emissora deve adotar as medidas adequadas para assegurar que são fornecidas informações sobre a possibilidade de interpor recurso ao abrigo do direito nacional e assegurar que este pode ser efetivamente interposto.

5. Os prazos ou outras condições para interpor recurso que sejam aplicáveis em processos nacionais semelhantes também são aplicáveis no âmbito do presente regulamento, de forma a garantir às pessoas em causa o exercício efetivo das vias de recurso.

6. Sem prejuízo do disposto nas normas processuais nacionais, os Estados-Membros devem assegurar que, no processo penal no Estado de emissão, aquando da avaliação dos elementos de prova obtidos através da ordem europeia de entrega de provas, são respeitados os direitos da defesa e a equidade do processo.

Artigo 18.°
Garantia dos privilégios e imunidades reconhecidos pelo Estado de execução

Se os dados transacionais ou de conteúdo obtidos através da ordem europeia de entrega de provas estiverem protegidos por imunidades ou privilégios reconhecidos ao abrigo do direito do Estado-Membro do destinatário, ou afetarem interesses fundamentais desse Estado-Membro em matéria de segurança e defesa nacional, o tribunal do Estado-Membro de emissão deve assegurar que, no processo penal para o qual a ordem foi emitida, esses fundamentos são tidos em conta como se tivessem sido previstos no seu direito nacional aquando da avaliação da relevância e da admissibilidade das provas em causa. O tribunal pode consultar as autoridades do Estado-Membro em causa, a Rede Judiciária Europeia em matéria penal ou a Eurojust.

Capítulo 5: Disposições finais

Artigo 19.°
Acompanhamento e divulgação de informações sobre a aplicação

1. O mais tardar até *[data de aplicação do presente Regulamento]*, a Comissão deve criar um programa pormenorizado de acompanhamento dos resultados e dos impactos do presente regulamento. O programa de acompanhamento deve definir os meios a utilizar e os intervalos a aplicar para a recolha dos dados e outros elementos de prova necessários. Deve especificar as medidas a tomar pela Comissão e pelos Estados-Membros aquando da recolha e análise dos dados e demais elementos de prova.

2. Em qualquer caso, os Estados-Membros devem recolher e manter estatísticas exaustivas por parte das autoridades pertinentes. Os dados recolhidos devem ser enviados anualmente à Comissão até 31 de março, o mais tardar, em relação ao ano civil anterior, devendo incluir

(a) o número de COEEP e de COECP emitidos, por tipo de dados solicitados, prestadores de serviços notificados e situação (de urgência ou não);

(b) o número de COEEP e de COECP executados e o número dos não executados, por tipo de dados solicitados, prestadores de serviços notificados e situação (de urgência ou não);

(c) para os COEEP executados, o tempo médio necessário para obter os dados solicitados, desde a emissão do COEEP até à obtenção dos mesmos, por tipo de dados solicitados, prestadores de serviços notificados e situação (de urgência ou não);

(d) o número de ordens europeias de entrega de provas transmitidas e recebidas para serem executadas num Estado de execução, por tipo de dados solicitados, prestadores de serviços notificados e situação (de urgência ou não), bem como o número de ordens executadas;

(e) o número de recursos interpostos contra ordens europeias de entrega de provas no Estado de emissão e no Estado de execução, por tipo de dados solicitados.

Artigo 20.°
Alterações aos certificados e aos formulários

Nos termos artigo 21.º, a Comissão deve adotar atos delegados para alterar os anexos I, II e II, a fim de responder eficazmente a uma eventual necessidade de melhorar o conteúdo dos formulários COEEP e COECP, bem como do formulário a utilizar para fornecer informações sobre a impossibilidade de executar um COEEP ou COECP.

Artigo 21.°
Exercício da delegação

1. O poder de adotar atos delegados é conferido à Comissão nas condições estabelecidas no presente artigo.

2. A delegação de poderes referida no artigo 20.º é conferida por prazo indeterminado, a partir de [*data de aplicação do presente regulamento*].

3. A delegação de poderes referida no artigo 20.º pode ser revogada em qualquer momento pelo Parlamento Europeu ou pelo Conselho. A decisão de revogação põe termo à delegação dos poderes nela especificados. A decisão de revogação produz efeitos a partir do dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia* ou de uma data posterior nela especificada. A decisão de revogação não afeta os atos delegados já em vigor.

4. Antes de adotar um ato delegado, a Comissão consulta os peritos designados por cada Estado-Membro de acordo com os princípios estabelecidos no Acordo Interinstitucional «Legislar melhor», de 13 de abril de 2016[50].

5. Assim que adotar um ato delegado, a Comissão notifica-o simultaneamente ao Parlamento Europeu e ao Conselho.

6. Os atos delegados adotados em aplicação do disposto no artigo 20.º só entram em vigor se nem o Parlamento Europeu nem o Conselho formularem objeções no prazo de dois meses a contar da notificação do ato a estas duas instituições ou se, antes do termo desse prazo, o Parlamento Europeu e o Conselho informarem a Comissão de que não formularão objeções. O referido prazo pode ser prorrogado por dois meses por iniciativa do Parlamento Europeu ou do Conselho.

Artigo 22.°
Notificações

1. Até *[data de aplicação do presente regulamento]*, cada Estado-Membro comunica à Comissão o seguinte:

   (a) as autoridades que, nos termos do seu direito nacional e em conformidade com o disposto no artigo 4.º, são competentes para emitir e/ou validar ordens europeias de entrega de provas e ordens europeias de conservação de provas;

   (b) a autoridade ou as autoridades de execução competentes para fazer executar as ordens europeias de entrega de provas e as ordens europeias de conservação de provas em nome de outro Estado-Membro;

   (c) os tribunais competentes para deliberar sobre oposições fundamentadas deduzidas por destinatários, em conformidade com o disposto nos artigos 15.º e 16.º.

2. A Comissão disponibilizará publicamente as informações recebidas nos termos do presente artigo num sítio Web dedicado ou no sítio Web da Rede Judiciária Europeia a que se refere o artigo 9.º da Decisão 2008/976/JAI do Conselho[51].

Artigo 23.°
Relação com as decisões europeias de investigação

As autoridades dos Estados-Membros podem continuar a emitir decisões europeias de investigação nos termos da Diretiva 2014/41/UE, para fins de recolha de provas que também seriam abrangidas pelo âmbito de aplicação do presente regulamento.

---

50 JO L 123 de 12.5.2016, p. 13.

51 Decisão 2008/976/JAI do Conselho, de 16 de dezembro de 2008, sobre a Rede Judiciária Europeia (JO L 348 de 24.12.2008, p. 130).

Artigo 24.°
Avaliação

O mais tardar, até [*cinco anos após a data de aplicação do presente regulamento*], a Comissão procederá a uma avaliação da aplicação do regulamento, transmitindo ao Parlamento Europeu e ao Conselho um relatório sobre o seu funcionamento, incluindo uma avaliação da necessidade de se alargar o seu âmbito de aplicação. Se necessário, o relatório deve ser acompanhado de propostas legislativas. A avaliação deve ser efetuada em conformidade com as orientações da Comissão sobre «Legislar Melhor». Os Estados-Membros devem transmitir à Comissão todas as informações necessárias para a elaboração do relatório.

Artigo 25.°
Entrada em vigor

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

É aplicável a partir de [*seis meses após a sua entrada em vigor*].

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

Pelo Parlamento Europeu	*Pelo Conselho*
O Presidente	*O Presidente*