

# AUTORIDADE EUROPEIA PARA A PROTEÇÃO DE DADOS

## **Resumo do Parecer da Autoridade Europeia para a Proteção de Dados sobre as Propostas relativas às Ordens Europeias de Entrega ou de Conservação de provas eletrónicas em matéria penal**

*(O texto integral deste parecer encontra-se disponível em alemão, francês e inglês no sítio Web da AEPD em [www.edps.europa.eu](http://www.edps.europa.eu))*

(2020/C 32/04)

Em abril de 2018, a Comissão apresentou duas propostas — de um regulamento e de uma diretiva — para estabelecer um quadro jurídico que facilite e acelere a garantia e obtenção de acesso das autoridades policiais e judiciais às provas eletrónicas em casos transnacionais. Desde então, o Conselho adotou abordagens gerais sobre as propostas e o Parlamento Europeu emitiu vários documentos de trabalho. O Comité Europeu para a Proteção de Dados emitiu o seu parecer. Registraram-se desenvolvimentos conexos a nível internacional, designadamente com o início das negociações de um acordo internacional com os Estados Unidos da América sobre o acesso transnacional a provas eletrónicas, bem como trabalhos sobre um Segundo Protocolo Adicional à Convenção sobre o Cibercrime. Com este parecer, a AEPD deseja prestar ao legislador da União Europeia um novo contributo para os próximos trabalhos sobre as propostas, tendo em conta os desenvolvimentos acima enumerados.

No mundo de hoje transformado pelas novas tecnologias, o tempo é muitas vezes essencial para permitir que aquelas autoridades obtenham dados indispensáveis para a concretização das suas missões. Ao mesmo tempo, mesmo quando investigam casos nacionais, as autoridades responsáveis pela aplicação da lei encontram-se cada vez mais em «situações transnacionais» simplesmente porque se recorreu a um prestador de serviços estrangeiro e a informação é armazenada eletronicamente noutro Estado-Membro. A AEPD apoia o objetivo de garantir que as autoridades responsáveis pela aplicação da lei disponham de instrumentos eficazes para investigar e instaurar ações penais por infrações criminais e congratula-se, em particular, com o objetivo das propostas de acelerar e facilitar o acesso aos dados em casos transnacionais através da simplificação dos procedimentos na UE.

Simultaneamente, a AEPD gostaria de sublinhar que qualquer iniciativa neste domínio deve respeitar integralmente a Carta dos Direitos Fundamentais da UE e o quadro da UE em matéria de proteção de dados, sendo essencial assegurar a existência de todas as salvaguardas necessárias. Em particular, a proteção efetiva dos direitos fundamentais no processo de recolha de provas eletrónicas transnacionais exige um maior envolvimento das autoridades judiciais no Estado-Membro de execução. Estas autoridades devem intervir sistematicamente o mais cedo possível neste processo, ter a possibilidade de analisar a conformidade das ordens com a Carta e ter o dever de fundamentar a recusa nesses termos.

Além disso, devem ser esclarecidas as definições das categorias de dados constantes do regulamento proposto e deve ser assegurada a sua coerência com outras definições de categorias de dados no direito da UE. A AEPD recomenda também que seja reavaliado o equilíbrio entre os tipos de infrações relativamente aos quais podem ser emitidas ordens europeias de entrega e as categorias de dados em causa, à luz da jurisprudência relevante do Tribunal de Justiça da UE.

Acresce que a AEPD faz recomendações específicas sobre vários aspetos das propostas sobre provas eletrónicas que exigem melhorias: a autenticidade e confidencialidade das ordens e dos dados transmitidos, a conservação limitada nos termos das ordens europeias de conservação, o quadro aplicável em matéria de proteção de dados, os direitos dos titulares dos dados, os titulares dos dados que beneficiam de imunidades e privilégios, os representantes legais, os prazos a respeitar nas Ordens Europeias de Entrega e a possibilidade de os prestadores de serviços se oporem às Ordens.

Por último, a AEPD solicita maior clareza quanto à interação do regulamento proposto com futuros acordos internacionais. O regulamento proposto deverá manter o elevado nível de proteção de dados na UE e tornar-se uma referência na negociação de acordos internacionais sobre o acesso transnacional a provas eletrónicas.

## 1. INTRODUÇÃO E CONTEXTO

1. Em 17 de abril de 2018, a Comissão divulgou duas propostas legislativas (a seguir «propostas»), acompanhadas de uma avaliação de impacto <sup>(1)</sup>, incluindo:
  - uma proposta de regulamento relativo às Ordens Europeias de Entrega ou de Conservação de provas eletrónicas em matéria penal <sup>(2)</sup> (a seguir designado «regulamento proposto»);
  - uma proposta de diretiva que estabelece normas harmonizadas aplicáveis à designação de representantes legais para efeitos de recolha de provas em processo penal <sup>(3)</sup> (a seguir «diretiva proposta»).
2. O regulamento proposto coexistiria com a Diretiva 2014/41/UE relativa à decisão europeia de investigação em matéria penal (a seguir «Diretiva DEI») <sup>(4)</sup>, que visa facilitar o processo de recolha de provas no território de outro Estado-Membro e abrange todos os tipos de recolha de provas, incluindo os dados eletrónicos <sup>(5)</sup>. Todos os Estados-Membros que participaram na adoção da Diretiva DEI <sup>(6)</sup> tinham de a transpor para a sua ordem jurídica interna até maio de 2017 <sup>(7)</sup>.
3. Em 26 de setembro de 2018, o Comité Europeu para a Proteção de Dados <sup>(8)</sup> (a seguir «CEPD») adotou um parecer <sup>(9)</sup> sobre as propostas.
4. Em 7 de dezembro de 2018 e em 8 de março de 2019, o Conselho adotou a sua abordagem geral sobre o regulamento proposto <sup>(10)</sup> e a diretiva proposta <sup>(11)</sup>, respetivamente. O Parlamento Europeu publicou uma série de documentos de trabalho.
5. A Autoridade Europeia para a Proteção de Dados (a seguir «AEPD») congratula-se por ter sido consultada informalmente pelos serviços da Comissão antes da adoção das propostas. A AEPD congratula-se igualmente com as referências ao presente parecer no considerando 66 do regulamento proposto e no considerando 24 da diretiva proposta.
6. Em 5 de fevereiro de 2019, a Comissão adotou duas recomendações de decisões do Conselho: uma recomendação para autorizar a abertura de negociações tendo em vista um acordo internacional entre a União Europeia (UE) e os Estados Unidos da América (EUA) sobre o acesso transfronteiras a provas eletrónicas para fins de cooperação judiciária em matéria penal <sup>(12)</sup> e uma recomendação para autorizar a participação da Comissão, em nome da UE, nas negociações respeitantes a um segundo protocolo adicional à Convenção do Conselho da Europa sobre o Cibercrime (STCE-185) (a seguir «Convenção sobre o Cibercrime») <sup>(13)</sup>. As duas recomendações foram objeto de dois pareceres da AEPD <sup>(14)</sup>. As negociações com os EUA e a nível do Conselho da Europa estão estreitamente ligadas.
7. Em fevereiro de 2019, a Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos do Parlamento Europeu endereçou cartas semelhantes à AEPD e ao CEPD para solicitar uma avaliação jurídica do impacto da Lei CLOUD norte-americana <sup>(15)</sup>, que foi aprovada pelo Congresso dos EUA em março de 2018, sobre o quadro jurídico europeu em matéria de proteção de dados. Em 12 de julho de 2019, a AEPD e o CEPD adotaram uma resposta conjunta a este pedido com a sua avaliação inicial <sup>(16)</sup>.
8. Em 3 de outubro de 2019, o Reino Unido e os Estados Unidos assinaram um acordo bilateral sobre o acesso transnacional a provas eletrónicas para efeitos de luta contra a criminalidade grave <sup>(17)</sup>. Trata-se do primeiro acordo executivo que permite aos prestadores de serviços norte-americanos cumprir os pedidos de dados de conteúdo provenientes de um país estrangeiro ao abrigo da Lei CLOUD norte-americana.

O presente parecer abrange ambas as propostas, mas centra-se principalmente no regulamento proposto. Em consonância com a missão da AEPD, centra-se principalmente nos direitos à privacidade e à proteção de dados pessoais e visa ser coerente com o Parecer 23/2018 do CEPD e complementar deste, tendo igualmente em conta as abordagens gerais do Conselho e os documentos de trabalho do Parlamento Europeu.

## 5. CONCLUSÕES

70. A AEPD apoia o objetivo de garantir que as autoridades responsáveis pela aplicação da lei e as autoridades judiciais disponham de instrumentos eficazes para investigar e instaurar ações penais por infrações penais num mundo transformado pelas novas tecnologias. Ao mesmo tempo, a AEPD gostaria de assegurar que esta ação respeita plenamente a Carta e o acervo da UE em matéria de proteção de dados. O regulamento proposto exigiria a conservação e a comunicação de dados pessoais dentro e fora da UE entre as autoridades competentes dos Estados-Membros, entidades privadas e, em alguns casos, autoridades de países terceiros. Implicaria limitações aos dois

direitos fundamentais de respeito pela vida privada e de proteção dos dados pessoais garantidos pelos artigos 7.º e 8.º da Carta. Para serem legais, essas limitações devem cumprir as condições estabelecidas no n.º 1 do artigo 52.º da Carta e, nomeadamente, a condição de necessidade.

71. Em primeiro lugar, a AEPD considera que outras alternativas que proporcionariam maiores salvaguardas atingindo em simultâneo os mesmos objetivos deveriam ser objeto de uma avaliação mais aprofundada.
72. Em segundo lugar, a AEPD regista que o regulamento proposto já inclui uma série de salvaguardas processuais. No entanto, a AEPD está preocupada com o facto de a importante responsabilidade de analisar a conformidade do Certificado de Ordem Europeia de Entrega de Provas (COEEP) e do Certificado de Ordem Europeia de Conservação de Provas (COECP) com a Carta ser confiada aos prestadores de serviços, e recomenda a intervenção das autoridades judiciais designadas pelo Estado-Membro de execução o mais cedo possível no processo de recolha de provas eletrónicas.
73. A AEPD recomenda que se assegure uma maior coerência entre as definições das categorias de dados eletrónicos de prova e as definições de categorias de dados específicas já existentes ao abrigo do direito da UE e que seja reconsiderada a categoria de dados de acesso, ou que o acesso a esses dados seja submetido a condições semelhantes às do acesso às categorias de dados transacionais e de dados de conteúdo. O regulamento proposto deverá estabelecer definições claras e simples de cada categoria de dados, a fim de garantir a segurança jurídica a todas as partes interessadas intervenientes. Recomenda também a alteração da proposta de definição da categoria de dados de assinantes, a fim de a especificar mais pormenorizadamente.
74. Recomenda ainda a reavaliação do equilíbrio entre o tipo de infrações relativamente às quais podem ser emitidas OEEP e as categorias de dados em causa, tendo em conta a recente jurisprudência relevante do TJUE. Em particular, a possibilidade de emitir uma OEEP para entregar dados transacionais e de conteúdo deverá ser limitada a crimes graves. Idealmente, a AEPD seria favorável à definição de uma lista fechada de infrações penais graves específicas para que as OEEP facultassem dados transacionais e de conteúdo, o que também aumentaria a segurança jurídica para todas as partes interessadas intervenientes.
75. A AEPD também faz recomendações destinadas a garantir o respeito pela proteção de dados e pelos direitos à privacidade e, em simultâneo, garantir a rápida recolha de provas para efeitos de procedimentos penais específicos. Estas recomendações centram-se na segurança da transmissão de dados entre todas as partes interessadas intervenientes, na autenticidade das ordens e certificados e na conservação limitada de dados no âmbito de uma OEEP.
76. Além das observações gerais e das principais recomendações acima formuladas, a AEPD fez recomendações adicionais no presente parecer sobre os seguintes aspetos das propostas:
  - a referência ao quadro de proteção de dados aplicável;
  - os direitos dos titulares dos dados (maior transparência e o direito a vias de recurso);
  - a atribuição de imunidades e privilégios aos titulares dos dados;
  - a nomeação de representantes legais para a recolha de provas em matéria penal;
  - os prazos para o cumprimento do COEEP e da entrega dos dados;
  - a possibilidade de os prestadores de serviços se oporem às ordens com base em fundamentos limitados.
77. Por último, a AEPD está ciente do contexto mais amplo em que a iniciativa foi apresentada e das duas decisões do Conselho adotadas, uma relativa ao segundo protocolo adicional à Convenção sobre o Cibercrime no Conselho da Europa e outra relativa à abertura de negociações com os Estados Unidos da América. Solicita uma maior clareza sobre a interação do regulamento proposto com os acordos internacionais. A AEPD está ansiosa por contribuir de forma construtiva para assegurar a coerência e a compatibilidade entre os textos finais e o quadro da UE em matéria de proteção de dados.

Bruxelas, 6 de novembro de 2019.

Wojciech Rafał WIEWIÓROWSKI  
*Autoridade Adjunta*

(<sup>1</sup>) Documento de trabalho dos serviços da Comissão: Avaliação de impacto, SWD(2018) 118 final (a seguir «avaliação de impacto»), disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2018%3A118%3AFIN>

(<sup>2</sup>) Proposta de Regulamento do Parlamento Europeu e do Conselho relativo às Ordens Europeias de Entrega ou de Conservação de provas eletrónicas em matéria penal, COM(2018) 225 final.

- (<sup>3</sup>) Proposta de Diretiva do Parlamento Europeu e do Conselho que estabelece normas harmonizadas aplicáveis à designação de representantes legais para efeitos de recolha de provas em processo penal, COM(2018) 226 final.
- (<sup>4</sup>) 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); ver artigo 23.º do regulamento proposto.
- (<sup>5</sup>) A Diretiva DEI prevê uma cooperação direta entre a autoridade de emissão de um Estado-Membro e a autoridade de execução de outro Estado-Membro ou, se for caso disso, através da autoridade ou autoridades centrais designadas pelo(s) Estado(s)-Membro(s) em causa. Visa facilitar e acelerar esta cooperação prevendo formas normalizadas e prazos rigorosos e eliminando vários obstáculos à cooperação transnacional; por exemplo, «[a] autoridade de emissão pode emitir uma DEI para tomar qualquer medida destinada a impedir provisoriamente a destruição, transformação, deslocação, transferência ou alienação de um elemento que possa servir de prova» e «[a] autoridade de execução decide e comunica a sua decisão sobre a medida provisória o mais rapidamente possível e, sempre que tal for praticável, no prazo de 24 horas a contar da receção da DEI» (artigo 32.º); além disso, a execução de uma DEI para a identificação de pessoas que tenham uma assinatura de um número de telefone ou um endereço IP específicos não está sujeita ao requisito de dupla incriminação [artigo 10.º, n.º 2, alínea e), conjugado com o artigo 11.º, n.º 2].
- (<sup>6</sup>) Todos os Estados-Membros da UE, com exceção da Dinamarca e da Irlanda.
- (<sup>7</sup>) Todos os Estados-Membros participantes transpuseram a Diretiva DEI para as respetivas ordens jurídicas nacionais em 2017 ou 2018. Ver o estado de implementação da Rede Judiciária Europeia: [https://www.ejn-crimjust.europa.eu/ejn/EJN\\_Library\\_StatusOfImpByCat.aspx?CategoryId=120](https://www.ejn-crimjust.europa.eu/ejn/EJN_Library_StatusOfImpByCat.aspx?CategoryId=120)
- (<sup>8</sup>) O CEPD criado pelo artigo 68.º do RGPD sucedeu ao Grupo de Trabalho instituído pelo artigo 29.º da Diretiva 95/46/CE, que foi revogada. Tal como o Grupo de Trabalho do Artigo 29.º, o CEPD é composto por representantes das autoridades nacionais de proteção de dados e da AEPD.
- (<sup>9</sup>) Parecer 23/2018, de 26 de setembro de 2018, sobre as propostas da Comissão relativas às Ordens Europeias de Entrega e de Conservação de provas eletrónicas em matéria penal [artigo 70.º, n.º 1, alínea b)] (a seguir «Parecer 23/2018 da AEPD»), disponível em: [https://edpb.europa.eu/sites/edpb/files/files/file1/eevidence\\_opinion\\_final\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/eevidence_opinion_final_en.pdf)
- (<sup>10</sup>) <https://www.consilium.europa.eu/pt/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/#>
- (<sup>11</sup>) <https://www.consilium.europa.eu/pt/press/press-releases/2019/03/08/e-evidence-package-council-agrees-its-position-on-rules-to-appoint-legal-representatives-for-the-gathering-of-evidence/>
- (<sup>12</sup>) Recomendação de Decisão do Conselho que autoriza a abertura de negociações tendo em vista um acordo entre a União Europeia e os Estados Unidos da América sobre o acesso transfronteiras a provas eletrónicas para fins de cooperação judiciária em matéria penal, COM(2019) 70 final.
- (<sup>13</sup>) Recomendação de Decisão do Conselho que autoriza a participação nas negociações respeitantes ao Segundo Protocolo Adicional à Convenção do Conselho da Europa sobre o Cibercrime (STCE-185), COM(2019) 71 final. Até à data, todos os Estados-Membros da UE assinaram a Convenção do Conselho da Europa sobre o reforço da cooperação internacional em matéria de cibercrime e de provas eletrónicas, tendo sido ratificada por quase todos. A Irlanda e a Suécia ainda estão em vias de ratificar a Convenção sobre o Cibercrime. A Convenção sobre o Cibercrime é um instrumento internacional vinculativo que exige que as partes contratantes prevejam na sua legislação nacional infrações penais específicas cometidas contra ou através de redes eletrónicas e que estabeleçam poderes e procedimentos específicos que permitam às suas autoridades nacionais efetuar as suas investigações criminais, incluindo a recolha de provas de uma infração em formato eletrónico. Incentiva igualmente a cooperação internacional entre as partes contratantes. Existem medidas específicas para fazer face aos desafios decorrentes da volatilidade dos dados. A este respeito, a Convenção prevê a conservação rápida dos dados informáticos armazenados. Uma vez que a transferência dos elementos de prova protegidos para o Estado requerente está sujeita a uma decisão final sobre o pedido formal de auxílio judiciário mútuo, a conservação não está sujeita ao conjunto completo de fundamentos de recusa; em particular, a dupla incriminação só é exigida em casos excecionais (artigo 29.º).
- (<sup>14</sup>) Parecer 2/2019 da AEPD sobre o mandato de negociação de um acordo UE-EUA sobre o acesso transfronteiras a provas eletrónicas e Parecer 3/2019 da AEPD relativo à participação nas negociações tendo em vista um segundo protocolo adicional à Convenção de Budapeste sobre o Cibercrime.
- (<sup>15</sup>) Disponível em: <https://www.congress.gov/bill/115th-congress/house-bill/1625/text>
- (<sup>16</sup>) [https://edpb.europa.eu/our-work-tools/our-documents/letters/epdb-edps-joint-response-libe-committee-impact-us-cloud-act\\_fr](https://edpb.europa.eu/our-work-tools/our-documents/letters/epdb-edps-joint-response-libe-committee-impact-us-cloud-act_fr)
- (<sup>17</sup>) <https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019>
-