COMISSÃO
EUROPEIA

Bruxelas, 25.11.2021
COM(2021) 719 final

2021/0383 (NLE)

Proposta de

DECISÃO DO CONSELHO

que autoriza os Estados-Membros a ratificar, no interesse da União Europeia, o Segundo Protocolo Adicional à Convenção sobre o Cibercrime relativo ao reforço da cooperação e da divulgação de provas eletrónicas

EXPOSIÇÃO DE MOTIVOS

1. OBJETO DA PROPOSTA

A presente proposta diz respeito à decisão que autoriza os Estados-Membros a ratificar, no interesse da União Europeia, o Segundo Protocolo Adicional à Convenção de Budapeste do Conselho da Europa sobre o Cibercrime relativo ao reforço da cooperação e da divulgação de provas eletrónicas (a seguir designado por «Protocolo»)[1]. O objetivo do Protocolo é estabelecer regras comuns a nível internacional para reforçar a cooperação em matéria de cibercriminalidade e a recolha de provas em formato eletrónico para as investigações e os processos penais.

A presente proposta complementa uma proposta separada da Comissão de uma decisão do Conselho da União Europeia (a seguir designado por «Conselho») que autoriza os Estados-Membros a assinar o Protocolo no interesse da União Europeia.

A cibercriminalidade continua a representar um desafio considerável para a nossa sociedade. Não obstante os esforços das autoridades policiais e judiciais, os ciberataques, incluindo os ataques de programas sequestradores (*ransomware*), estão a aumentar e a tornar-se mais sofisticados[2]. Em especial, devido à natureza sem fronteiras da Internet, quase sempre as investigações em matéria de cibercriminalidade são investigações transnacionais, o que exige uma estreita cooperação entre as autoridades de diferentes países.

As provas eletrónicas assumem cada vez mais importância nas investigações criminais. A Comissão estima que, atualmente, as autoridades policiais e judiciais necessitam do acesso a provas eletrónicas em 85 % das investigações criminais, incluindo em matéria de cibercriminalidade[3]. As provas das infrações penais são conservadas com cada vez maior frequência em formato eletrónico por prestadores de serviços em jurisdições estrangeiras, e para que a justiça penal atue com eficácia são necessárias medidas adequadas para obter tais provas a fim de defender o Estado de direito.

Em todo o mundo se envidam esforços no sentido de melhorar o acesso transfronteiras às provas eletrónicas no âmbito de investigações criminais, a nível nacional, da União Europeia[4] e internacional, nomeadamente através do Protocolo. É importante assegurar a compatibilidade das normas a nível internacional para evitar conflitos de leis quando se solicita o acesso transfronteiras a provas eletrónicas.

2. CONTEXTO DA PROPOSTA

2.1. Contexto

A Convenção de Budapeste do Conselho da Europa sobre o Cibercrime (STCE n.º 185) (a seguir designada por «Convenção») visa facilitar a luta contra as infrações penais cometidas através das redes informáticas. A Convenção tem por objeto, 1) a harmonização dos elementos relativos a infrações no contexto do direito substantivo de âmbito nacional e das disposições conexas na área da cibercriminalidade, 2) a definição, ao abrigo do código de

[1] O texto do Protocolo figura em anexo à presente proposta.

[2] Avaliação 2021 da Ameaça da Criminalidade Grave e Organizada da União Europeia 2021 (SOCTA - (*Serious and Organised Crime Threat Assessment*) da UE 2021).

[3] SWD(2018) 118 final.

[4] COM(2018) 225 e 226 final.

processo penal interno, dos poderes necessários para investigar e intentar ações penais relativamente a tais infrações, assim como a outras infrações cometidas por meio de um sistema informático ou às provas com elas relacionadas e existentes sob a forma eletrónica, e 3) a implantação de um regime rápido e eficaz de cooperação internacional.

A Convenção está aberta aos Estados membros do Conselho da Europa e, mediante convite, aos não membros. Atualmente, 66 países são Partes na Convenção, incluindo 26 Estados-Membros da União Europeia[5]. A Convenção não prevê que a União Europeia possa aderir à Convenção. No entanto, a União Europeia é reconhecida como organização com estatuto de observador junto do Comité da Convenção sobre o Cibercrime (T-CY)[6].

Não obstante os esforços envidados para negociar uma nova convenção sobre o cibercrime a nível das Nações Unidas[7], a Convenção de Budapeste continua a ser a principal convenção multilateral para a luta contra o cibercrime. A União apoia sistematicamente a Convenção[8], designadamente no quadro do financiamento de programas de reforço das capacidades[9].

Na sequência de propostas do Grupo «Provas na Nuvem» (*Cloud Evidence Group*)[10], o Comité da Convenção sobre o Cibercrime adotou várias recomendações para dar resposta, nomeadamente através da negociação de um Segundo Protocolo Adicional à Convenção sobre o Cibercrime relativo ao reforço da cooperação internacional, ao problema colocado pelo facto de as provas eletrónicas relacionadas com a cibercriminalidade e outras infrações serem cada vez mais detidas por prestadores de serviços em jurisdições estrangeiras, enquanto as competências das autoridades policiais continuam a ser limitadas pelas fronteiras territoriais. Em junho de 2017, o Comité da Convenção sobre o Cibercrime aprovou o mandato para a preparação do Segundo Protocolo Adicional durante o período compreendido entre setembro de 2017 e dezembro de 2019[11]. Tendo em conta a necessidade de dispor de mais tempo para finalizar os debates, bem como as limitações impostas pela pandemia de COVID-19 em 2020 e 2021, o Comité da Convenção sobre o Cibercrime prorrogou o mandato por duas vezes, até dezembro de 2020, e posteriormente até maio de 2021.

Na sequência do apelo do Conselho Europeu nas suas conclusões de 18 de outubro de 2018[12], a Comissão adotou, em 5 de fevereiro de 2019, uma recomendação de decisão do Conselho que autoriza a Comissão a participar, em nome da União Europeia, nas negociações relativas a um segundo Protocolo Adicional à Convenção do Conselho da Europa sobre o Cibercrime[13]. A Autoridade Europeia para a Proteção de Dados adotou um parecer sobre a recomendação

---

5 Todos, exceto a Irlanda, que assinou mas não ratificou a Convenção, tendo-se comprometido, no entanto, a prosseguir o processo de adesão.

6 Regulamento interno do Comité da Convenção sobre o Cibercrime (T-CY (2013) 25 rev), disponível em www.coe.int/cybercrime.

7 Resolução 74/247 da Assembleia Geral das Nações Unidas (AGNU), de dezembro de 2019, relativa ao «combate à utilização das tecnologias da informação e da comunicação para fins criminosos».

8 JOIN(2020) 81 final.

9 Ver, por exemplo, a Ação Global Alargada sobre Cibercriminalidade (GLACY+), em https://www.coe.int/en/web/cybercrime/glacyplus.

10 Relatório final do Grupo «Provas na Nuvem» do Comité da Convenção sobre o Cibercrime: «*Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY*», (Acesso da justiça penal às provas eletrónicas na nuvem: recomendações a ter em conta pelo T-CY), de 16 de setembro de 2016.

11 https://rm.coe.int/t-cy-terms-of-reference-protocol/1680a03690

12 https://www.consilium.europa.eu/en/press/press-releases/2018/10/18/20181018-european-council-conslusions/

13 COM(2019) 71 final.

em 2 de abril de 2019[14]. Por decisão de 6 de junho de 2019, o Conselho da União Europeia autorizou a Comissão a participar, em nome da União Europeia, nas negociações relativas ao Segundo Protocolo Adicional[15].

Tal como expresso na Estratégia da UE para a União da Segurança de 2020[16], na Estratégia de Cibersegurança da UE para a década digital de 2020[17] e na Estratégia da UE para lutar contra a criminalidade organizada de 2021[18], a Comissão comprometeu-se a concluir rapidamente e com êxito as negociações do Protocolo. O Parlamento Europeu reconheceu igualmente a necessidade de concluir os trabalhos sobre o Protocolo na sua Resolução de 2021 sobre a Estratégia de Cibersegurança da UE para a década digital[19].

A Comissão participou, em nome da União Europeia, nas negociações relativas ao Protocolo, em conformidade com a decisão do Conselho da União Europeia. Consultou sistematicamente o comité especial do Conselho para as negociações sobre a posição da União.

Em conformidade com o Acordo-Quadro sobre as relações entre o Parlamento Europeu e a Comissão Europeia[20], a Comissão também manteve o Parlamento Europeu informado das negociações através de relatórios escritos e apresentações orais.

Na reunião plenária de 28 de maio de 2021, o Comité da Convenção sobre o Cibercrime aprovou o projeto de Protocolo ao seu nível e enviou o projeto para adoção pelo Comité de Ministros do Conselho da Europa[21]. Em 17 de novembro de 2021, o Comité de Ministros do Conselho da Europa adotou o Protocolo.

2.2. O Segundo Protocolo Adicional

O objetivo do Protocolo é reforçar a cooperação em matéria de cibercriminalidade e de recolha de provas eletrónicas de uma infração penal para efeitos de investigações ou processos penais específicos. O Protocolo reconhece a necessidade de uma cooperação reforçada e mais eficaz entre os Estados e com o setor privado, bem como de uma maior clareza e segurança jurídica para os prestadores de serviços e outras entidades no que diz respeito às circunstâncias em que podem responder aos pedidos de divulgação de provas eletrónicas das autoridades de justiça penal de outras Partes.

O Protocolo reconhece igualmente que uma cooperação transfronteiras eficaz para fins de justiça penal, incluindo entre as autoridades do setor público e as entidades do setor privado, exige condições efetivas e salvaguardas sólidas para a proteção dos direitos fundamentais. Para o efeito, o Protocolo segue uma abordagem baseada nos direitos e prevê condições e salvaguardas em consonância com os instrumentos internacionais em matéria de direitos humanos, incluindo a Convenção do Conselho da Europa para a Proteção dos Direitos do Homem e das Liberdades Fundamentais de 1950. Uma vez que as provas eletrónicas dizem

[14] Parecer 3/2019 da AEPD sobre a participação nas negociações tendo em vista um Segundo Protocolo Adicional à Convenção de Budapeste sobre o Cibercrime, de 2 de abril de 2019.
[15] Decisão do Conselho com a referência 9116/19.
[16] COM(2020) 605 final.
[17] JOIN(2020) 81 final.
[18] COM(2021) 170 final.
[19] Resolução do Parlamento Europeu, de 10 de junho de 2021, sobre a Estratégia de Cibersegurança da UE para a década digital.
[20] Referência L 304/47.
[21] https://rm.coe.int/0900001680a2aa42

frequentemente respeito a dados pessoais, o Protocolo inclui igualmente salvaguardas sólidas para a proteção da privacidade e dos dados pessoais.

As disposições referidas nos parágrafos seguintes revestem-se de especial importância para o Protocolo. O Protocolo é acompanhado de um relatório explicativo pormenorizado. Embora o relatório explicativo não constitua um instrumento que forneça uma interpretação vinculativa do Protocolo, destina-se a «orientar e assistir as Partes» na aplicação do mesmo[22].

2.2.1. Disposições comuns

O capítulo I do Protocolo prevê disposições comuns. O artigo 2.º determina o âmbito de aplicação do Protocolo, em consonância com o âmbito de aplicação da Convenção: aplica-se a investigações ou processos penais específicos relativos a infrações penais relacionadas com sistemas e dados informáticos, bem como à recolha de provas de uma infração penal em formato eletrónico.

No artigo 3.º, são incluídas definições de «autoridades centrais», «autoridades competentes», «situações de emergência», «dados pessoais» e «Parte que procede à transferência». Estas definições aplicam-se ao Protocolo, juntamente com as definições incluídas na Convenção.

O artigo 4.º determina as línguas em que as Partes devem emitir injunções, pedidos ou notificações ao abrigo do Protocolo.

2.2.2. Medidas de cooperação

O capítulo II do Protocolo prevê medidas destinadas a reforçar a cooperação. Em primeiro lugar, o artigo 5.º, n.º 1, determina que as Partes devem cooperar, tanto quanto possível, com base no Protocolo. O artigo 5.º, n.ºs 2 a 5, determina a aplicação das medidas do Protocolo em relação aos tratados ou convénios de auxílio mútuo em vigor. O artigo 5.º, n.º 7, estabelece que as medidas previstas no capítulo II não restringem a cooperação entre as Partes, ou com prestadores de serviços ou outras entidades, através de outros acordos, convénios, práticas ou legislação nacional aplicáveis.

O artigo 6.º estabelece uma base para a cooperação direta entre as autoridades competentes de uma Parte e as entidades que prestam serviços de registo de nomes de domínio noutra Parte, com vista à divulgação de dados de registo de nomes de domínio.

O artigo 7.º estabelece uma base para a cooperação direta entre as autoridades competentes de uma Parte e os prestadores de serviços de outra Parte para a divulgação de dados relativos aos assinantes.

O artigo 8.º fornece uma base para uma cooperação reforçada entre as autoridades para a divulgação de dados informáticos.

O artigo 9.º fornece uma base para a cooperação entre autoridades com vista à divulgação de dados informáticos em situações de emergência.

O artigo 10.º fornece uma base para o auxílio judiciário mútuo em situações de emergência.

O artigo 11.º fornece uma base para a cooperação por videoconferência.

[22] Ver ponto 2 do relatório explicativo do Protocolo.

O artigo 12.º fornece uma base para as investigações conjuntas e as equipas de investigação conjuntas.

2.2.3. Salvaguardas

O Protocolo segue uma abordagem baseada nos direitos, com condições e salvaguardas específicas, algumas das quais são incorporadas nas medidas de cooperação específicas, bem como no capítulo III do Protocolo. O artigo 13.º do Protocolo exige que as Partes assegurem que os poderes e procedimentos sejam sujeitos a um nível adequado de proteção dos direitos fundamentais que, em conformidade com o artigo 15.º da Convenção, garanta a aplicação do princípio da proporcionalidade.

O artigo 14.º do Protocolo prevê a proteção dos dados pessoais, tal como definida no artigo 3.º do Protocolo, em consonância com o Protocolo de Alteração da Convenção para a Proteção das Pessoas relativamente ao Tratamento de Dados de Caráter Pessoal (STCE 223) (Convenção 108+) e o direito da União.

Nessa base, o artigo 14.º, n.os 2 a 15, estabelece princípios fundamentais em matéria de proteção de dados, incluindo a limitação da finalidade, a base jurídica, a qualidade dos dados e as regras aplicáveis ao tratamento de categorias especiais de dados, as obrigações aplicáveis aos responsáveis pelo tratamento, nomeadamente em matéria de conservação, manutenção de registos, segurança e no que respeita a transferências ulteriores, direitos individuais oponíveis, incluindo em matéria de notificação, acesso, retificação e tomada de decisões automatizada, supervisão independente e eficaz por uma ou mais autoridades, bem como vias de recurso administrativo e judicial. As salvaguardas abrangem todas as formas de cooperação previstas no Protocolo, com adaptações sempre que necessário para ter em conta as características específicas da cooperação direta (por exemplo, no contexto da notificação de violações). O exercício de certos direitos individuais pode ser adiado, limitado ou recusado sempre que necessário e proporcionado para perseguir objetivos de interesse público importantes, em especial para prevenir riscos para as investigações policiais em curso, o que também está em conformidade com o direito da União.

O artigo 14.º do Protocolo deve também ser lido em conjugação com o artigo 23.º do mesmo. O artigo 23.º reforça a eficácia das salvaguardas previstas no Protocolo, prevendo que o Comité da Convenção sobre o Cibercrime avalie a execução e a aplicação das medidas tomadas na legislação nacional para dar cumprimento às disposições do Protocolo. Em especial, o artigo 23.º, n.º 3, reconhece explicitamente que a aplicação do artigo 14.º pelas Partes será avaliada logo que dez Partes na Convenção tenham manifestado o seu consentimento em ficar vinculadas pelo Protocolo.

Como salvaguarda adicional, nos termos do artigo 14.º, n.º 15, se uma Parte dispuser de provas substanciais de que outra Parte está a violar de forma sistemática ou grave as salvaguardas estabelecidas no Protocolo, pode suspender a transferência de dados pessoais para essa Parte após consulta (o que não é exigido em caso de urgência). Os dados pessoais transferidos antes da suspensão continuam a ser tratados em conformidade com o Protocolo.

Por último, tendo em conta o caráter multilateral do Protocolo, o seu artigo 14.º, n.os 1.b e 1.c, permite às Partes, nas suas relações bilaterais, acordar, em determinadas condições, formas alternativas de assegurar a proteção dos dados pessoais transferidos ao abrigo do Protocolo. Embora as salvaguardas previstas no artigo 14.º, n.os 2 a 15, se apliquem por norma às Partes que recebem dados pessoais, com base no artigo 14.º, n.º 1.b, as Partes vinculadas mutuamente por um acordo internacional que estabeleça um quadro abrangente para a

proteção de dados pessoais, em conformidade com os requisitos aplicáveis da legislação das Partes em causa, podem também basear-se nesse quadro. Trata-se, por exemplo, da Convenção 108+ (para as Partes que autorizam transferências de dados para outras Partes ao abrigo dessa convenção) ou do Acordo-Quadro UE-EUA (no seu âmbito de aplicação, ou seja, para a transferência de dados pessoais entre autoridades e, em combinação com um acordo de transferência específico entre os EUA e a UE, para a cooperação direta entre autoridades e prestadores de serviços). Além disso, com base no artigo 14.º, n.º 1.c, as Partes podem igualmente determinar de comum acordo que a transferência de dados pessoais tem lugar com base noutros acordos ou convénios entre as Partes em causa. Para os Estados-Membros da UE, um acordo ou convénio alternativo deste tipo só pode ser invocado para as transferências de dados ao abrigo do Protocolo se essas transferências cumprirem os requisitos da legislação da União em matéria de proteção de dados, nomeadamente o capítulo V da Diretiva (UE) 2016/680 (Diretiva sobre a Proteção de Dados na Aplicação da Lei) e, para a cooperação direta entre autoridades e prestadores de serviços nos termos dos artigos 6.º e 7.º do Protocolo, o capítulo V do Regulamento (UE) 2016/679 (Regulamento Geral sobre a Proteção de Dados).

2.2.4. Disposições finais

O capítulo IV do Protocolo estabelece as disposições finais. Entre outras coisas, o artigo 15.º, n.º 1.a, estabelece que as Partes podem definir as suas relações sobre as matérias enunciadas no Protocolo de outra forma, em conformidade com o artigo 39.º, n.º 2, da Convenção. O artigo 15.º, n.º 1.b, assegura que os Estados-Membros da UE que são Partes no Protocolo podem continuar a aplicar o direito da União nas suas relações mútuas. O artigo 15.º, n.º 2, determina igualmente que o artigo 39.º, n.º 3, da Convenção se aplica ao Protocolo.

O artigo 16.º, n.º 3, prevê que o Protocolo entrará em vigor logo que cinco Partes na Convenção tiverem manifestado o seu consentimento em ficar por ele vinculadas.

O artigo 19.º, n.º 1, prevê que as Partes possam formular reservas em relação ao artigo 7.º, n.ºs 9.a e 9.b, ao artigo 8.º, n.º 13, e ao artigo 17.º. O artigo 19.º, n.º 2, prevê que as Partes possam formular declarações em relação ao artigo 7.º, n.º 2.b, e n.º 8, ao artigo 8.º, n.º 11, ao artigo 9.º, n.º 1.b, e n.º 5, ao artigo 10.º, n.º 9, ao artigo 12.º, n.º 3, e ao artigo 18.º, n.º 2. O artigo 19.º, n.º 3, determina que uma Parte formula as declarações, notificações ou comunicações identificadas no artigo 7.º, n.ºs 5.a e 5.e, no artigo 8.º, n.º 4 e n.ºs 10.a e 10b, no artigo 14.º, n.º 7.c, e n.º 10.b, e no artigo 17.º, n.º 2.

O artigo 23.º, n.º 1, constitui uma base para as consultas entre as Partes, nomeadamente através do Comité da Convenção sobre o Cibercrime, em conformidade com o artigo 46.º da Convenção. O artigo 23.º, n.º 2, também estabelece uma base para a avaliação da utilização e da aplicação das disposições do Protocolo. O artigo 23.º, n.º 3, estabelece que a avaliação da utilização e da aplicação do artigo 14.º relativo à proteção de dados tem início logo que dez Partes tiverem manifestado o seu consentimento em ficar vinculadas pelo Protocolo.

2.3. Direito e política da União neste domínio

O domínio regido pelo Protocolo é, em grande medida, abrangido por normas comuns baseadas no artigo 82.º, n.º 1, e no artigo 16.º do TFUE. O atual quadro jurídico da União Europeia inclui, nomeadamente, instrumentos relativos à cooperação das autoridades policiais e judiciárias em matéria penal, tais como a Diretiva 2014/41/UE relativa à decisão europeia de investigação em matéria penal, a Convenção relativa ao auxílio judiciário mútuo em matéria penal entre os Estados-Membros da União Europeia e a Decisão-Quadro 2002/465/JAI do Conselho relativa às equipas de investigação conjuntas. A nível externo, a União Europeia

celebrou uma série de acordos bilaterais entre a União e países terceiros, tais como os acordos sobre auxílio judiciário mútuo entre a União Europeia e os Estados Unidos da América, entre a União Europeia e o Japão e entre a União Europeia e a Noruega e a Islândia. O atual quadro jurídico da União Europeia inclui também o Regulamento (UE) 2017/1939 que dá execução a uma cooperação reforçada para a instituição da Procuradoria Europeia. Os Estados-Membros que participam na cooperação reforçada deverão assegurar que a Procuradoria Europeia, no exercício das suas competências, tal como previstas nos artigos 22.º, 23.º e 25.º do Regulamento (UE) 2017/1939, possa solicitar cooperação ao abrigo do Protocolo da mesma forma que os procuradores nacionais desses Estados-Membros. Estes instrumentos e acordos dizem respeito, nomeadamente, aos artigos 8.º, 9.º, 10.º, 11.º e 12.º do Protocolo.

Além disso, a União adotou várias diretivas que reforçam os direitos processuais dos suspeitos e arguidos[23]. Estes instrumentos dizem respeito, em especial, aos artigos 6.º, 7.º, 8.º, 9.º, 10.º, 11.º, 12.º e 13.º do Protocolo. Um conjunto específico de salvaguardas diz respeito à proteção dos dados pessoais, que é um direito fundamental consagrado nos Tratados da UE e na Carta dos Direitos Fundamentais da União Europeia. Os dados pessoais só podem ser tratados em conformidade com o Regulamento (UE) 2016/679 (Regulamento Geral sobre a Proteção de Dados) e com a Diretiva (UE) 2016/680 (Diretiva sobre a Proteção de Dados na Aplicação da Lei). O direito fundamental de todas as pessoas ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações inclui o respeito pela privacidade das suas comunicações como elemento essencial. Os dados das comunicações eletrónicas só podem ser tratados em conformidade com a Diretiva 2002/58/CE (Diretiva Privacidade Eletrónica). Estes instrumentos dizem respeito, nomeadamente, ao artigo 14.º do Protocolo.

O artigo 14.º, n.os 2 a 15, do Protocolo estabelece salvaguardas adequadas em matéria de proteção de dados na aceção das normas da União neste domínio, nomeadamente o artigo 46.º do Regulamento Geral sobre a Proteção de Dados e o artigo 37.º da Diretiva sobre a Proteção de Dados na Aplicação da Lei, bem como a jurisprudência pertinente do Tribunal de Justiça Europeu. Em conformidade com os requisitos do direito da União[24] e a fim de garantir a

[23] 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); 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); 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); 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); 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); 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); Diretiva 2012/13/UE do Parlamento Europeu e do Conselho, de 22 de maio de 2012, relativa ao direito à informação em processo penal.

[24] Ver Tribunal de Justiça (Grande Secção), Parecer 1/15, ECLI:EU:C:2017:592, n.º 220. Ver também o contributo do Comité Europeu para a Proteção de Dados para a consulta sobre um projeto de Segundo Protocolo Adicional à Convenção do Conselho da Europa sobre o Cibercrime (Convenção de Budapeste), 13 de novembro de 2019, p. 6 («As autoridades nacionais competentes às quais foi concedido acesso aos dados devem notificar as pessoas afetadas, nos termos dos procedimentos nacionais aplicáveis, logo que essa notificação deixar de ser suscetível de comprometer as investigações realizadas por essas autoridades. [...] A notificação é necessária para permitir que as pessoas afetadas exerçam, nomeadamente, o seu direito de

eficácia das salvaguardas estabelecidas no artigo 14.º do Protocolo, os Estados-Membros devem assegurar a notificação das pessoas cujos dados tenham sido transferidos, sob reserva de determinadas restrições, por exemplo, para evitar comprometer as investigações em curso. O artigo 14.º, n.º 11.c, do Protocolo constitui uma base para que os Estados-Membros cumpram este requisito.

A compatibilidade do artigo 14.º, n.º 1, do Protocolo com as normas da União em matéria de proteção de dados exige igualmente que os Estados-Membros considerem o seguinte no que respeita a possíveis formas alternativas de assegurar a proteção adequada dos dados pessoais transferidos ao abrigo do Protocolo. No que diz respeito a outros acordos internacionais que estabelecem um quadro abrangente para a proteção de dados pessoais em conformidade com os requisitos aplicáveis da legislação das Partes em causa, nos termos do artigo 14.º, n.º 1.b, os Estados-Membros devem ter em conta que, no que diz respeito à cooperação direta, o Acordo-Quadro UE-EUA necessita de ser complementado com salvaguardas adicionais - a prever num acordo de transferência específico entre os EUA e a UE/seus Estados-Membros - que tenham em conta os requisitos únicos da transferência de provas eletrónicas diretamente pelos prestadores de serviços e não entre as autoridades[25].

Além disso, nos termos do artigo 14.º, n.º 1.b, do Protocolo, os Estados-Membros devem considerar que, para os Estados-Membros da UE que são Partes na Convenção 108+, essa Convenção, por si só, não constitui uma base adequada para as transferências transfronteiras de dados ao abrigo do Protocolo para outras Partes nessa Convenção. A este respeito, devem ter em conta a última frase do artigo 14.º, n.º 1, da Convenção 108+[26].

Por último, no que respeita a outros acordos ou convénios ao abrigo do artigo 14.º, n.º 1.c, os Estados-Membros devem considerar que só podem invocar esses outros acordos ou convénios se a Comissão Europeia tiver adotado uma decisão de adequação nos termos do artigo 45.º do Regulamento (UE) 2016/679 (Regulamento Geral sobre a Proteção de Dados) ou do artigo 36.º da Diretiva (UE) 2016/680 (Diretiva sobre a Proteção de Dados na Aplicação da Lei) para o país terceiro em causa, que abranja as respetivas transferências de dados, ou se esse outro acordo ou convénio estabelecer salvaguardas adequadas em matéria de proteção de dados nos termos do artigo 46.º do Regulamento Geral sobre a Proteção de Dados ou do artigo 37.º, n.º 1.a, da Diretiva sobre a Proteção de Dados na Aplicação da Lei.

Há que ter em conta não só o direito da União no seu estado atual no domínio em causa, mas também a sua evolução futura, na medida em que tal seja previsível no momento da análise. O domínio abrangido pelo Protocolo é diretamente relevante para a evolução previsível do

---

recurso e os seus direitos em matéria de proteção de dados no que diz respeito ao tratamento dos seus dados»).

[25] É por esta razão que a Decisão do Conselho, de 21 de maio de 2019, que autoriza a abertura de negociações tendo em vista a celebração de 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 (9114/19) contém, nas suas diretrizes de negociação, uma série de salvaguardas adicionais em matéria de proteção de dados. Em especial, as diretrizes de negociação estipulam que «[o] acordo deverá completar o Acordo-Quadro através de garantias adicionais que tenham em conta o nível de sensibilidade das categorias de dados em questão e os requisitos únicos da transferência de provas eletrónicas efetuada diretamente pelos prestadores de serviços e não entre autoridades e as transferências das autoridades competentes efetuadas diretamente para os prestadores de serviços».

[26] Ver também o Relatório Explicativo do Protocolo que altera a Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, 10 de outubro de 2018, pontos 106-107.

direito da União no futuro. A este respeito, importa referir as propostas da Comissão sobre o acesso transfronteiras a provas eletrónicas, de abril de 2018[27]. Estes instrumentos dizem respeito, nomeadamente, aos artigos 6.º e 7.º do Protocolo.

A Comissão, ao participar nas negociações em nome da União, velou por que o Protocolo seja plenamente compatível com o direito da União e com as obrigações que incumbem aos Estados-Membros por força do mesmo. Em especial, a Comissão garantiu que as disposições do Protocolo permitam aos Estados-Membros respeitar os direitos fundamentais, as liberdades e os princípios gerais do direito da União consagrados nos Tratados da UE e na Carta dos Direitos Fundamentais, incluindo a proporcionalidade, os direitos processuais, a presunção de inocência e os direitos de defesa das pessoas sujeitas a processos penais, bem como a privacidade e a proteção dos dados pessoais e dos dados de comunicações eletrónicas, quando esses dados são tratados, incluindo transferências para as autoridades responsáveis pela aplicação da lei de países situados fora da União Europeia, e quaisquer obrigações que incumbam às autoridades policiais e judiciais a este respeito. A Comissão teve igualmente em conta o parecer da Autoridade Europeia para a Proteção de Dados[28] e do Comité Europeu para a Proteção de Dados[29].

Além disso, a Comissão assegurou que as disposições do Protocolo e as propostas da Comissão em matéria de provas eletrónicas fossem compatíveis, nomeadamente à medida que o projeto de legislação evoluiu nos debates com os colegisladores, e que o Protocolo não desse origem a conflitos de leis. Em especial, a Comissão assegurou que o Protocolo incluísse salvaguardas adequadas em matéria de proteção de dados e privacidade, que permitam aos prestadores de serviços da UE cumprir as suas obrigações ao abrigo da legislação da UE em matéria de proteção de dados e privacidade, na medida em que o Protocolo constitui um fundamento jurídico para as transferências de dados em resposta a injunções ou pedidos emitidos por uma autoridade de uma Parte no Protocolo não pertencente à UE que exijam que um responsável pelo tratamento ou um subcontratante da UE divulgue dados pessoais ou dados de comunicações eletrónicas.

2.4. Reservas, declarações, notificações, comunicações e outras considerações

O Protocolo constitui uma base para as Partes formularem determinadas reservas e para fazerem declarações, notificações ou comunicações em relação a determinados artigos. Os Estados-Membros devem adotar uma abordagem uniforme relativamente a certas reservas, declarações, notificações e comunicações, tal como estabelecido no anexo da presente decisão. A fim de assegurar a compatibilidade da aplicação do Protocolo com o direito da União, os Estados-Membros da UE devem tomar a posição a seguir exposta no que diz respeito a essas reservas e declarações. Sempre que o Protocolo constitua uma base para outras reservas, declarações, notificações ou comunicações, a presente proposta autoriza os

[27] COM(2018) 225 e 226 final.

[28] Parecer 3/2019 da AEPD sobre a participação nas negociações tendo em vista um Segundo Protocolo Adicional à Convenção de Budapeste sobre o Cibercrime, de 2 de abril de 2019.

[29] Incluindo o «Contributo do Comité Europeu para a Proteção de Dados para a consulta sobre um projeto de segundo protocolo adicional à Convenção do Conselho da Europa sobre o Cibercrime (Convenção de Budapeste), 13 de novembro de 2019»; a «Declaração 2/2021 sobre o novo projeto de disposições do Segundo Protocolo Adicional à Convenção do Conselho da Europa sobre o Cibercrime (Convenção de Budapeste), adotada em 2 de fevereiro de 2021»; o «Contributo do Comité Europeu para a Proteção de Dados para a 6.ª ronda de consultas sobre o projeto de Segundo Protocolo Adicional à Convenção de Budapeste do Conselho da Europa sobre o Cibercrime, de 4 de maio de 2021».

Estados-Membros a examinar e formular as suas próprias reservas, declarações, notificações ou comunicações.

A fim de assegurar a compatibilidade entre as disposições do Protocolo e o direito e as políticas pertinentes da União, os Estados-Membros não devem formular reservas nos termos do artigo 7.º, n.os 9.a[30] e 9.b[31]. Além disso, os Estados-Membros devem fazer a declaração nos termos do artigo 7.º, n.º 2.b[32], e a notificação nos termos do artigo 7.º, n.º 5.a[33]. A ausência dessas reservas, bem como a apresentação da declaração e da notificação, são importantes para assegurar a compatibilidade do Protocolo com as propostas legislativas da Comissão em matéria de provas eletrónicas, nomeadamente à medida que o projeto legislativo evolui nos debates com os colegisladores.

Além disso, a fim de assegurar uma aplicação uniforme do Protocolo pelos Estados-Membros da UE no âmbito da sua cooperação com as Partes que não são Estados-Membros da UE, os Estados-Membros são convidados a não formular uma reserva nos termos do artigo 8.º, n.º 13[34], também porque tal reserva teria efeitos recíprocos[35]. Os Estados-Membros devem formular a declaração nos termos do artigo 8.º, n.º 4, a fim de garantir que as injunções possam ser executadas caso sejam necessárias informações adicionais de apoio, por exemplo, sobre as circunstâncias do caso em apreço, a fim de avaliar a proporcionalidade e a necessidade[36].

Os Estados-Membros são igualmente incentivados a abster-se de fazer a declaração prevista no artigo 9.º, n.º 1.b[37], a fim de assegurar uma aplicação eficaz do Protocolo.

Os Estados-Membros devem efetuar as comunicações nos termos do artigo 7.º, n.º 5.e[38], do artigo 8.º, n.os 10.a e 10.b[39], do artigo 14.º, n.º 7.c e n.º 10.b, a fim de assegurar uma aplicação globalmente eficaz do Protocolo[40].

---

[30] Que permite que as Partes se reservem o direito de não aplicar o artigo 7.º (divulgação de dados relativos aos assinantes).

[31] Que permite que as Partes se reservem o direito de não aplicar o artigo 7.º (divulgação de dados relativos aos assinantes) a determinados tipos de números de acesso, se tal for incompatível com os princípios fundamentais da sua ordem jurídica interna.

[32] Que permite que as Partes declarem que a injunção emitida ao abrigo do artigo 7.º, n.º 1 (divulgação de dados relativos aos assinantes), deve ser emitida por um procurador ou outra autoridade judicial, ou sob a sua supervisão, ou ser emitida sob supervisão independente.

[33] Que permite que as Partes notifiquem o Secretário-Geral do Conselho da Europa de que, quando é emitida uma injunção nos termos do artigo 7.º, n.º 1, (divulgação de dados relativos aos assinantes) a um prestador de serviços no seu território, a Parte exige, em todos os casos ou em determinadas circunstâncias, a notificação simultânea da injunção, as informações suplementares e um resumo dos factos relacionados com a investigação ou o procedimento.

[34] Que permite que as Partes se reservem o direito de não aplicar o artigo 8.º (execução das ordens emitidas por outra Parte) aos dados de tráfego.

[35] Ver o n.º 147 do relatório explicativo do Protocolo, que determina que «[a] Parte que formula uma reserva ao presente artigo não está autorizada a transmitir ordens relativas aos dados de tráfego a outras Partes nos termos do [artigo 8.º,] n.º 1».

[36] Que permite que as Partes declarem que são necessárias informações de apoio adicionais para dar cumprimento às ordens ao abrigo do artigo 8.º, n.º 1 (execução das ordens emitidas por outra Parte).

[37] Que permite que as Partes declarem que não executarão os pedidos ao abrigo do artigo 9.º, n.º 1.a (divulgação expedita de dados informáticos em caso de emergência), que visem apenas a divulgação de dados relativos aos assinantes.

[38] Que permite que as Partes comuniquem os dados de contacto das autoridades por elas designadas para receber notificações nos termos do artigo 7.º, n.º 5.a, e executar as ações descritas no artigo 7.º, n.os 5.b, 5.c e 5.d (divulgação de dados relativos aos assinantes).

[39] Que permite que as Partes comuniquem os dados de contacto das autoridades designadas para apresentar e receber ordens ao abrigo do artigo 8.º (execução das junções emitidas por outra Parte). Em conformidade

Por último, os Estados-Membros devem também tomar as medidas necessárias nos termos do artigo 14.º, n.º 11.c, para assegurar que a Parte recetora é informada, no momento da transferência, da obrigação, prevista no direito da União, de notificar a pessoa a quem os dados dizem respeito[41], bem como de fornecer os dados de contacto adequados para permitir à Parte recetora informar a autoridade competente do Estado-Membro da UE logo que deixem de se aplicar as restrições de confidencialidade e a notificação possa ser enviada.

2.5. Justificação da proposta

O Protocolo entrará em vigor logo que cinco Partes tiverem manifestado o seu consentimento em ficar vinculadas pelo Protocolo, em conformidade com o disposto no artigo 16.º, n.os 1 e 2. A cerimónia de assinatura do Protocolo está prevista para março de 2022.

Os Estados-Membros da UE devem tomar as medidas necessárias para assegurar a rápida entrada em vigor e ratificação do Protocolo, o que é importante tendo em conta uma série de fatores.

Em primeiro lugar, o Protocolo permitirá melhorar os meios de que dispõem as autoridades policiais e judiciais para obter as provas eletrónicas necessárias para as investigações criminais. Tendo em conta a importância crescente das provas eletrónicas para as investigações criminais, é urgente que as autoridades policiais e judiciais disponham dos instrumentos adequados para obter acesso às provas eletrónicas de forma eficaz, a fim de garantir que possam combater eficazmente a criminalidade em linha.

Em segundo lugar, o Protocolo assegurará que essas medidas para obter acesso às provas eletrónicas sejam utilizadas de forma a permitir que os Estados-Membros respeitem os direitos fundamentais, incluindo os direitos processuais no âmbito de processos penais, o direito à privacidade e o direito à proteção dos dados pessoais. Na ausência de normas claras a nível internacional, as práticas existentes podem colocar desafios em termos de segurança jurídica, transparência, responsabilização e respeito pelos direitos fundamentais e pelas garantias processuais dos suspeitos nas investigações criminais.

Em terceiro lugar, o Protocolo permitirá resolver e prevenir conflitos de leis, que afetam tanto as autoridades como os prestadores de serviços do setor privado e outras entidades, estabelecendo normas compatíveis a nível internacional para o acesso transfronteiras a provas eletrónicas.

Em quarto lugar, o Protocolo demonstrará a importância que a Convenção continua a assumir enquanto principal quadro multilateral para a luta contra a cibercriminalidade. Este aspeto será fundamental no processo subsequente à Resolução 74/247 da Assembleia Geral das Nações Unidas (AGNU), de dezembro de 2019, relativa ao combate à utilização das tecnologias da informação e da comunicação para fins criminosos, que criou um comité intergovernamental *ad hoc* aberto composto por peritos encarregados de elaborar uma

---

com os requisitos do Regulamento (UE) 2017/1939, os Estados-Membros que participam na cooperação reforçada para a instituição da Procuradoria Europeia devem incluir a Procuradoria Europeia na comunicação.

[40] Que permite que as Partes comuniquem a autoridade ou autoridades que devem, respetivamente, ser notificadas em caso de incidente de segurança, ou ser contactadas para obter autorização prévia em caso de transferências ulteriores para outro Estado ou organização internacional.

[41] Ver nota de rodapé 24.

convenção internacional abrangente sobre o combate à utilização das tecnologias da informação e da comunicação para fins criminosos.

3. BASE JURÍDICA, SUBSIDIARIEDADE E PROPORCIONALIDADE

- *Base jurídica*

A competência da União para legislar sobre questões relacionadas com a facilitação da cooperação entre autoridades judiciárias ou equivalentes no âmbito de processos penais e da execução das decisões decorre do artigo 82.º, n.º 1, do TFUE. A competência da União em matéria de proteção de dados de caráter pessoal decorre do artigo 16.º do TFUE.

Em conformidade com o artigo 3.º, n.º 2, do TFUE, a União dispõe de competência exclusiva para celebrar acordos internacionais quando tal celebração seja suscetível de afetar regras comuns da UE ou de alterar o alcance das mesmas. As disposições do Protocolo inserem-se num domínio abrangido, em grande medida, por normas comuns, tal como estabelecido na secção 2.3 supra.

O Protocolo é, por conseguinte, da competência externa exclusiva da União. A ratificação do Protocolo pelos Estados-Membros, no interesse da União, pode, assim, ter lugar com base no artigo 16.º, no artigo 82.º, n.º 1, e no artigo 218.º, n.º 6, do TFUE.

- *Subsidiariedade (no caso de competência não exclusiva)*

Não aplicável.

- *Proporcionalidade*

Os objetivos da União no que respeita à presente proposta, enunciados na secção 2.5, só podem ser alcançados através da celebração de um acordo internacional vinculativo que preveja as medidas de cooperação necessárias, garantindo simultaneamente uma proteção adequada dos direitos fundamentais. O Protocolo atinge este objetivo. As disposições do Protocolo limitam-se ao necessário para atingir os seus principais objetivos. Uma ação unilateral não constitui uma alternativa, uma vez que não proporcionaria uma base suficiente para a cooperação com os países terceiros e não poderia assegurar a necessária proteção dos direitos fundamentais. Além disso, a adesão a um acordo multilateral como o Protocolo, que a União pôde negociar, é mais eficaz do que encetar negociações com vários países terceiros a nível bilateral. Partindo do pressuposto de que as 66 Partes, bem como as futuras novas Partes, ratificarão o Protocolo, este proporcionará um quadro jurídico comum para a cooperação dos Estados-Membros da UE com os seus parceiros internacionais mais importantes na luta contra a criminalidade.

- ***Escolha do instrumento***

Não aplicável.

4. RESULTADOS DAS AVALIAÇÕES *EX POST*, DAS CONSULTAS DAS PARTES INTERESSADAS E DAS AVALIAÇÕES DE IMPACTO

- *Avaliações ex post/balanços de qualidade da legislação existente*

Não aplicável.

- *Consultas das partes interessadas*

O Conselho da Europa organizou seis rondas de consultas públicas sobre as negociações do Protocolo, em julho e novembro de 2018, fevereiro e novembro de 2019, dezembro de 2020 e maio de 2021[42]. As Partes analisaram os contributos recebidos no âmbito dessas consultas.

A Comissão, na sua qualidade de negociadora em nome da União, também trocou pontos de vista com as autoridades responsáveis pela proteção de dados e organizou reuniões de consulta específicas ao longo de 2019 e 2021 com organizações da sociedade civil, prestadores de serviços e associações comerciais. A Comissão teve em conta os contributos recebidos no âmbito desta troca de pontos de vista.

- *Recolha e utilização de conhecimentos especializados*

No decurso das negociações, a Comissão consultou com regularidade o Comité Especial do Conselho para as negociações, em conformidade com a Decisão do Conselho da União Europeia, de 6 de junho de 2019, que autoriza a Comissão a participar nas negociações em nome da União, o que constituiu uma oportunidade para os peritos dos Estados-Membros contribuírem para o processo de elaboração da posição da União. Alguns peritos dos Estados-Membros continuaram também a participar nas negociações, juntamente com a Comissão, que participou em nome da União. Foram igualmente realizadas consultas às partes interessadas (ver supra).

- *Avaliação de impacto*

Em 2017 e 2018, foi realizada uma avaliação de impacto para acompanhar as propostas da Comissão em matéria de provas eletrónicas[43]. Neste contexto, a negociação de um acordo sobre um Segundo Protocolo Adicional à Convenção de Budapeste sobre o Cibercrime fazia parte da opção preferida. Os impactos relevantes são, além disso, apresentados na presente exposição de motivos.

- *Adequação da regulamentação e simplificação*

O Protocolo pode ter implicações para certas categorias de prestadores de serviços, incluindo as pequenas e médias empresas (PME), uma vez que podem ser objeto de pedidos e ordens relativos a provas eletrónicas ao abrigo do Protocolo. No entanto, estes prestadores recebem já frequentemente pedidos deste tipo através de outros canais existentes, que por vezes são transmitidos por outras autoridades, nomeadamente com base na Convenção[44], noutros tratados de auxílio judiciário mútuo ou noutros quadros, incluindo as políticas multissetoriais de governação da Internet[45]. Além disso, os prestadores de serviços, incluindo as PME, beneficiarão de um quadro jurídico claro a nível internacional e de uma abordagem comum de todas as Partes no Protocolo.

- *Direitos fundamentais*

Os instrumentos de cooperação previstos pelo Protocolo são suscetíveis de afetar os direitos fundamentais quando os dados de uma pessoa podem ser obtidos no contexto de um processo

[42] https://www.coe.int/en/web/cybercrime/protocol-consultations

[43] SWD(2018) 118 final.

[44] Ver, por exemplo, a nota de orientação 10 do Comité da Convenção sobre o Cibercrime, de 1 de março de 2017, relativa às injunções de comunicação de dados relativos aos assinantes (artigo 18.º da Convenção de Budapeste).

[45] Ver, por exemplo, a Resolução do Conselho de Administração da Sociedade Internet para os Nomes e Números Atribuídos (ICANN) de 15 de maio de 2019, relativa às recomendações sobre a especificação temporária para os dados de registo gTLD, disponível em www.icann.org.

penal, incluindo, por exemplo, o direito a um processo equitativo, o direito à privacidade e o direito à proteção dos dados pessoais. O Protocolo segue uma abordagem baseada nos direitos e prevê condições e salvaguardas em consonância com os instrumentos internacionais em matéria de direitos humanos, incluindo a Convenção do Conselho da Europa para a Proteção dos Direitos do Homem e das Liberdades Fundamentais de 1950. Em especial, o Protocolo prevê salvaguardas específicas em matéria de proteção de dados. Sempre que necessário, o Protocolo constitui também uma base para as Partes formularem determinadas reservas, declarações ou notificações e prevê os motivos para recusar a cooperação em resposta a um pedido em situações específicas. Tal garante a compatibilidade do Protocolo com a Carta dos Direitos Fundamentais da União Europeia.

5. INCIDÊNCIA ORÇAMENTAL

A presente proposta não tem incidência no orçamento da União. A aplicação do Protocolo pode gerar custos pontuais para os Estados-Membros, e os custos para as autoridades dos Estados-Membros poderão ser mais elevados devido ao aumento previsto do número de casos.

6. OUTROS ELEMENTOS

- *Planos de execução e acompanhamento, avaliação e prestação de informações*

Não existe um plano de execução do Protocolo, uma vez que, após a sua assinatura e ratificação, os Estados-Membros serão obrigados a aplicá-lo.

No que diz respeito ao acompanhamento, a Comissão participará nas reuniões do Comité da Convenção sobre o Cibercrime, no qual a União Europeia é reconhecida como organização com estatuto de observador.

2021/0383 (NLE)

Proposta de

DECISÃO DO CONSELHO

que autoriza os Estados-Membros a ratificar, no interesse da União Europeia, o Segundo Protocolo Adicional à Convenção sobre o Cibercrime relativo ao reforço da cooperação e da divulgação de provas eletrónicas

O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 16.º, o artigo 82.º, n.º 1, e o artigo 218.º, n.º 6,

Tendo em conta a proposta da Comissão Europeia,

Tendo em conta a aprovação do Parlamento Europeu,

Considerando o seguinte:

(1) Em 9 de junho de 2019, o Conselho autorizou a Comissão a participar, em nome da União, nas negociações relativas ao Segundo Protocolo Adicional à Convenção de Budapeste sobre o Cibercrime do Conselho da Europa.

(2) O texto do Segundo Protocolo Adicional à Convenção sobre o Cibercrime relativo ao reforço da cooperação e da divulgação de provas eletrónicas (a seguir designado «Protocolo») foi adotado pelo Comité de Ministros do Conselho da Europa em 17 de novembro de 2021 e deverá estar aberto à assinatura em março de 2022.

(3) As disposições do Protocolo inserem-se num domínio abrangido, em grande medida, por regras comuns na aceção do artigo 3.º, n.º 2, do TFUE, incluindo instrumentos que facilitam a cooperação judiciária em matéria penal, garantindo normas mínimas em matéria de direitos processuais, bem como salvaguardas em matéria de proteção de dados e da privacidade.

(4) A Comissão apresentou igualmente propostas legislativas respeitantes a um regulamento relativo às ordens europeias de entrega ou de conservação de provas eletrónicas em matéria penal [COM(2018) 225 final] e a uma diretiva que estabelece regras harmonizadas aplicáveis à designação de representantes legais para efeitos de recolha de provas em processo penal, [COM(2018) 226 final], que introduzem a obrigatoriedade de as ordens europeias de entrega ou de conservação de provas transfronteiras serem dirigidas diretamente a um representante de um prestador de serviços noutro Estado-Membro.

(5) Graças à sua participação nas negociações, em nome da União, a Comissão assegurou a compatibilidade do Segundo Protocolo Adicional com as regras comuns pertinentes da União Europeia.

(6) Várias reservas, declarações, notificações e comunicações são relevantes para assegurar a compatibilidade do Protocolo com o direito e as políticas da União, a aplicação uniforme do Protocolo entre os Estados-Membros da UE nas suas relações com as Partes que não são membros da UE, bem como a aplicação efetiva do Protocolo.

(7) Uma vez que o Protocolo prevê procedimentos rápidos que melhoram o acesso transfronteiras a provas eletrónicas e um elevado nível de salvaguardas, a sua entrada em vigor contribuirá para a luta contra o cibercrime e outras formas de criminalidade a nível mundial, facilitando a cooperação entre as Partes que são Estados-Membros da UE e as que não o são, assegurará um elevado nível de proteção das pessoas e permitirá resolver os conflitos de leis.

(8) Dado que o Protocolo estabelece salvaguardas adequadas, em consonância com os requisitos aplicáveis às transferências internacionais de dados pessoais ao abrigo do Regulamento (UE) 2016/679 e da Diretiva (UE) 2016/680, a sua entrada em vigor contribuirá para promover as normas da União em matéria de proteção de dados a nível mundial, facilitará os fluxos de dados entre as Partes que são Estados-Membros da UE e as que não o são e assegurará o cumprimento, por parte dos Estados-Membros da UE, das obrigações que lhes incumbem por força das regras da União em matéria de proteção de dados.

(9) A rápida entrada em vigor confirmará, além disso, a importância da Convenção de Budapeste do Conselho da Europa enquanto principal quadro multilateral para a luta contra a cibercriminalidade.

(10) A União Europeia não pode tornar-se Parte no Protocolo, uma vez que tanto o Protocolo como a Convenção do Conselho da Europa sobre o Cibercrime estão abertos apenas aos Estados.

(11) Os Estados-Membros devem, pois, ser autorizados a ratificar o Protocolo, agindo conjuntamente no interesse da União.

(12) A Autoridade Europeia para a Proteção de Dados foi consultada nos termos do disposto no artigo 42.º, n.º 1, do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho e emitiu parecer em …

(13) [Nos termos dos artigos 1.º e 2.º do Protocolo n.º 21 relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, segurança e justiça, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União Europeia, e sem prejuízo do artigo 4.º do Protocolo acima referido, a Irlanda não participa na adoção da presente decisão, não ficando por ela vinculada nem sujeita à sua aplicação.]

[OU]

[Nos termos dos artigos 1.º e 2.º do Protocolo n.º 21 relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, segurança e justiça, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União Europeia, e sem prejuízo do artigo 4.º do Protocolo acima referido, a Irlanda notificou [por carta de ... ,] a sua intenção de participar na adoção e aplicação da presente decisão.]

(14) Nos termos dos artigos 1.º e 2.º do Protocolo n.º 22 relativo à posição da Dinamarca, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União Europeia, a Dinamarca não participa na adoção da presente decisão, não ficando por ela vinculada nem sujeita à sua aplicação,

ADOTOU A PRESENTE DECISÃO:

Artigo 1.º

Os Estados-Membros são autorizados a ratificar, no interesse da União Europeia, o Segundo Protocolo Adicional à Convenção sobre o Cibercrime, relativo ao reforço da cooperação e da divulgação de provas eletrónicas (a seguir designado «Protocolo»).

Artigo 2.º

Ao ratificarem o Protocolo, os Estados-Membros formulam as reservas, declarações, notificações ou comunicações constantes do anexo.

Artigo 3.º

A presente decisão entra em vigor no dia da sua adoção.

Artigo 4.º

A presente decisão é publicada no Jornal Oficial da União Europeia.

Artigo 5.º

Os Estados-membros são os destinatários da presente decisão.

Feito em Bruxelas, em

Pelo Conselho
O Presidente