COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Série de Tratados do Conselho da Europa – n.º 224

Relatório explicativo ao Segundo Protocolo Adicional à Convenção sobre o Cibercrime relativo ao reforço da cooperação e da divulgação de provas sob a forma eletrónica

(Estrasburgo, 12 de maio de 2022)

1. O Segundo Protocolo Adicional à Convenção sobre o Cibercrime relativo ao reforço da cooperação e da divulgação de provas sob a forma eletrónica ("o presente Protocolo") foi adotado pelo Comité de Ministros do Conselho da Europa na sua 1417.ª Reunião (17 de novembro de 2021) dos Delegados dos Ministros e o presente Protocolo será aberto à assinatura em Estrasburgo, em 12 de maio de 2022. O Comité de Ministros tomou igualmente nota do relatório explicativo.

2. O texto do presente relatório explicativo destina-se a orientar e assistir as Partes na aplicação do presente Protocolo e reflete o entendimento dos redatores quanto ao seu funcionamento.

Introdução e antecedentes

3. A Convenção sobre o Cibercrime (STCE n.º 185, a seguir designada por "a Convenção"), desde a sua abertura à assinatura em Budapeste, em 23 de novembro de 2001, tornou-se um instrumento com adesão e impacto em todas as regiões do mundo.

4. Em 2003, a Convenção foi complementada pelo Protocolo Adicional à Convenção sobre o Cibercrime relativo à Criminalização de Atos de Natureza Racista e Xenófoba praticados através de Sistemas Informáticos (STCE n.º 189, a seguir designado por "Primeiro Protocolo").

5. As tecnologias da informação e da comunicação evoluíram e transformaram as sociedades a nível mundial de forma extraordinária desde que a Convenção foi aberta à assinatura em 2001. No entanto, desde então, registou-se também um aumento significativo da exploração da tecnologia para fins criminosos. O cibercrime é agora considerado por muitas Partes como uma grave ameaça para os direitos humanos, o Estado de direito e o funcionamento das sociedades democráticas. As ameaças colocadas pelo cibercrime são inúmeras. Os exemplos incluem a violência sexual online contra crianças e outros crimes contra a dignidade e a integridade das pessoas, roubo e uso abusivo de dados pessoais que afetam a vida privada das pessoas, interferência eleitoral e outros ataques contra as instituições democráticas, ataques contra infraestruturas críticas, como a negação de serviço distribuído e ataques de *ransomware*, ou o uso abusivo dessa tecnologia para fins terroristas. Em 2020 e 2021, durante a pandemia de Covid-19, os países observaram um aumento significativo do cibercrime relacionado com a Covid-19, incluindo ataques a hospitais e instalações médicas que desenvolvem vacinas contra o vírus, uso abusivo de nomes de domínio para promover vacinas, tratamentos e curas falsas, e outros tipos de atividades fraudulentas.

6. Apesar do crescimento das tecnologias baseadas em dados e da expansão e evolução perniciosas do cibercrime, os conceitos consagrados na Convenção são tecnologicamente neutros, de modo a que o direito penal substantivo possa ser aplicado tanto às tecnologias atuais como às futuras tecnologias envolvidas, e a Convenção continua a ser fundamental na luta contra o cibercrime. A Convenção visa principalmente: i) a harmonização dos elementos de direito penal substantivo interno das infrações e as disposições conexas no domínio do

cibercrime, ii) a definição, ao abrigo do processo penal nacional, dos poderes necessários para a investigação e a repressão de tais infrações, assim como de outras infrações cometidas por meio de um sistema informático ou relacionadas com a utilização de provas sob a forma eletrónica de outros crimes, e iii) a criação de um regime rápido e eficaz de cooperação internacional.

7. Ao aplicarem a Convenção, as Partes respeitam a responsabilidade que incumbe aos governos de protegerem as pessoas contra a criminalidade, quer esta seja cometida online ou offline, através de investigações e ações penais eficazes. Com efeito, algumas Partes na Convenção consideram que estão vinculadas por uma obrigação internacional a disponibilizar os meios de proteção contra crimes cometidos através de um sistema informático (ver *K.U. vs. Finlândia*, Tribunal Europeu dos Direitos Humanos (Ação n.º 2872/02, acórdão/decisão de 2 de março de 2009), fazendo referência aos procedimentos e poderes para investigações ou processos penais que as Partes devem estabelecer nos termos da Convenção).

8. As Partes têm, constantemente, procurado honrar o seu compromisso de combater o cibercrime recorrendo a vários mecanismos e organismos criados ao abrigo da Convenção e tomando as medidas necessárias para permitir investigações e processos penais mais eficazes. De forma determinante, a utilização e a aplicação da Convenção são facilitadas pelo Comité da Convenção sobre o Cibercrime (T-CY), criado ao abrigo do artigo 46.º da Convenção. Além disso, a Convenção é apoiada por programas de fortalecimento das capacidades implementados pelo Gabinete do Programa de Cibercrime do Conselho da Europa em Bucareste, na Roménia, que prestam assistência a países de todo o mundo na aplicação da Convenção. Esta tríade de: i) normas comuns da Convenção no domínio do cibercrime, em conjunto com ii) um mecanismo sólido para o envolvimento contínuo das Partes através do T-CY e iii) a ênfase nos programas de fortalecimento das capacidades contribuíram significativamente para o alcance e o impacto da Convenção.

9. Em 2012, o T-CY, em linha com o seu mandato nos termos do artigo 46.º, n.º 1, da Convenção, de partilhar "informação sobre os desenvolvimentos jurídicos, políticos ou técnicos importantes verificados no domínio do cibercrime e a recolha de provas sob forma eletrónica" e para ponderar a possibilidade de "complementar ou aditar a Convenção", criou o subgrupo *ad hoc* sobre a jurisdição e o acesso transfronteiras a dados ("Transborder Group"). Em dezembro de 2014, o T-CY concluiu igualmente uma avaliação das disposições em matéria de assistência mútua da Convenção sobre o Cibercrime e adotou um conjunto de recomendações, incluindo algumas que deviam ser abordadas num novo protocolo à Convenção. Estes esforços conduziram à criação, em 2015, do grupo de trabalho sobre o acesso da justiça penal aos elementos de prova armazenados na cloud, nomeadamente através da assistência jurídica mútua ("Cloud Evidence Group").

10. Em 2016, o *Cloud Evidence Group* concluiu, entre outros, que "o cibercrime, o número de dispositivos, serviços e utilizadores (incluindo de dispositivos e serviços móveis) e, consequentemente, o número de vítimas atingiu proporções tais que apenas uma pequena parte do cibercrime ou de outras infrações que envolvam provas sob a forma eletrónica será alguma vez registada e investigada. A grande maioria das vítimas de cibercrime não pode esperar que seja feita justiça. Os principais desafios identificados pelo grupo estavam relacionados com a "computação na cloud, a territorialidade e a jurisdição" e, por conseguinte, com as dificuldades em obter um acesso eficiente a provas sob a forma eletrónica ou a sua divulgação.

11. Ao avaliar as conclusões do *Cloud Evidence Group*, as Partes na Convenção concluíram que não era necessário aditar a Convenção ou prever uma criminalização adicional através de disposições de direito penal substantivo. As Partes determinaram, contudo, que eram necessárias medidas adicionais para melhorar a cooperação e a capacidade de as autoridades de justiça penal obterem provas sob a forma eletrónica através de um segundo protocolo adicional, a fim de permitir uma resposta mais eficaz da justiça penal e defender o Estado de direito.

Trabalhos preparatórios

12. A 17.ª reunião plenária do T-CY (8 de junho de 2017) aprovou o mandato para a preparação do presente Protocolo com base numa proposta elaborada pelo *Cloud Evidence Group* do T-CY. Decidiu iniciar a redação do presente Protocolo por sua própria iniciativa, nos termos do artigo 46.º, n.º 1, alínea c), da Convenção. Em 14 de junho de 2017, o Secretário-Geral Adjunto do Conselho da Europa informou o Comité de Ministros (1289.ª Reunião dos Delegados dos Ministros) desta iniciativa do T-CY.

13. O mandato abrangia inicialmente o período compreendido entre setembro de 2017 e dezembro de 2019, tendo sido posteriormente prorrogado pelo T-CY até dezembro de 2020 e novamente até maio de 2021.

14. No âmbito deste mandato, o T-CY criou um Plenário de Redação do Protocolo (PDP – *Protocol Drafting Plenary*), composto por representantes das Partes na Convenção e pelos Estados, organizações e órgãos do Conselho da Europa com estatuto de observadores no T-CY, na qualidade de observadores. O PDP foi assistido na preparação do projeto de protocolo por um Grupo de Redação do Protocolo (PDG – *Protocol Drafting Group*) composto por peritos das Partes na Convenção. Por sua vez, o PDG criou vários subgrupos e grupos *ad hoc* para trabalhar em disposições específicas.

15. Entre setembro de 2017 e maio de 2021, o T-CY realizou 10 reuniões plenárias de redação, 16 reuniões do grupo de redação e numerosas reuniões de subgrupos e de grupos *ad hoc*. Grande parte deste Protocolo foi elaborado durante a pandemia de Covid-19. Devido às restrições relacionadas com a Covid-19, entre março de 2020 e maio de 2021, foram realizadas mais de 65 reuniões em formato virtual.

16. Os métodos de trabalho acima referidos em reuniões plenárias, grupos de redação e grupos e subgrupos *ad hoc* permitiram que representantes e peritos das Partes contribuíssem largamente para a elaboração do presente Protocolo e desenvolvessem soluções inovadoras.

17. A Comissão da União Europeia participou neste trabalho em nome dos Estados Partes na Convenção que são membros da União Europeia ao abrigo de um mandato de negociação conferido pelo Conselho da União Europeia em 6 de junho de 2019.

18. Uma vez preparados os projetos de disposições e adotados provisoriamente pelo PDP, os projetos de artigos foram publicados e os intervenientes foram convidados a apresentar comentários.

19. O T-CY realizou seis rondas de consultas com intervenientes da sociedade civil e do setor privado, bem como com peritos em proteção de dados. Tal foi realizado em conjunto com a Conferência Octopus sobre a cooperação contra o cibercrime, realizada em Estrasburgo, em julho de 2018; com peritos em proteção de dados em Estrasburgo, em novembro de 2018; através de um convite à apresentação de comentários escritos sobre os projetos de artigos, em fevereiro de 2019; em conjunto com a Conferência Octopus sobre a cooperação contra o cibercrime, em Estrasburgo, em novembro de 2019; através de um convite à apresentação de comentários por escrito sobre outros projetos de artigos, em dezembro de 2020; e em maio de 2021, através de comentários escritos e de uma reunião virtual realizada em 6 de maio de 2021.

20. Além disso, o T-CY consultou o Comité Europeu para os Problemas Criminais (CDPC) e o Comité Consultivo da Convenção para a Proteção das Pessoas no que diz respeito ao Tratamento Automatizado de Dados Pessoais (T-PD) do Conselho da Europa.

21. A 24.ª sessão plenária do T-CY, em 28 de maio de 2021, aprovou este projeto de Protocolo e decidiu apresentá-lo ao Comité de Ministros, tendo em vista a sua adoção.

Considerações de ordem substantiva

22. Em termos de conteúdo, o ponto de partida para o trabalho sobre este Protocolo foi o resultado da avaliação do T-CY das disposições da Convenção relativas à assistência mútua em 2014 e as análises e recomendações do *Transborder Group* e do *Cloud Evidence Group* do T-CY em 2014 e 2017, respetivamente. Os desafios que suscitaram uma preocupação particular referem-se à territorialidade e à jurisdição relacionadas com as provas sob a forma eletrónica, ou seja, que os dados especificados necessários para uma investigação criminal podem ser armazenados em jurisdições múltiplas, móveis ou desconhecidas ("na cloud") e a necessidade de soluções para obter a divulgação desses dados de forma eficaz e eficiente para efeitos de investigações ou processos penais específicos.

23. Tendo em conta a complexidade destes desafios, os redatores do presente Protocolo acordaram em centrar-se nas seguintes questões específicas:

- Aquando da redação do presente Protocolo, os pedidos de assistência mútua eram o principal método de obtenção de provas sob a forma eletrónica de uma infração penal junto de outros Estados, incluindo os instrumentos de assistência jurídica mútua contemplados na Convenção. No entanto, a assistência mútua nem sempre é uma forma eficiente de tratar um número crescente de pedidos de provas sob a forma eletrónica voláteis. Por conseguinte, considerou-se necessário desenvolver um mecanismo mais simplificado para a emissão de injunções ou pedidos a fornecedores de serviços de outras Partes para produzir informação sobre subscritores e dados de tráfego.

- Informação sobre subscritores – por exemplo, para identificar o utilizador de uma determinada conta de e-mail ou de redes sociais ou de um endereço específico de protocolo de Internet (IP) utilizado na prática de uma infração – é a informação mais frequentemente procurada em investigações criminais nacionais e internacionais relacionadas com cibercrime e outros crimes que envolvem provas sob a forma eletrónica.
  Sem esta informação, é muitas vezes impossível prosseguir uma investigação. A obtenção de informação sobre subscritores através da assistência mútua não é, na maioria dos casos, eficaz e sobrecarrega o sistema de assistência mútua. A informação relativa aos subscritores é normalmente detida pelos fornecedores de serviços. Embora o artigo 18.º da Convenção já aborde alguns aspetos da obtenção de informação sobre subscritores junto dos fornecedores de serviços (ver a nota de orientação do T-CY sobre o artigo 18.º), incluindo noutras Partes, foram considerados necessários instrumentos complementares para obter a divulgação de informação sobre subscritores diretamente junto de um fornecedor de serviços de outra Parte. Estes instrumentos aumentarão a eficiência do processo e aliviarão também a pressão sobre o sistema de assistência mútua.

- Os dados de tráfego são também, com frequência, procurados em investigações criminais e a sua rápida divulgação pode ser necessária para detetar a fonte de uma comunicação como o ponto de partida para a recolha de novas provas ou para a identificação de um suspeito.

- Similarmente, uma vez que muitas formas de criminalidade online são facilitadas por domínios criados ou explorados para fins criminosos, é necessário identificar a pessoa que registou esse domínio. Essa informação é detida por entidades que prestam serviços de registo de nomes de domínio, ou seja, em geral, por empresas de registo e registos. Por conseguinte, é necessário um quadro eficiente para obter essa informação junto de entidades relevantes de outras Partes.

- Numa situação de emergência, em que exista um risco significativo e iminente para a vida ou a segurança de qualquer pessoa singular, é necessária uma ação rápida, quer através da prestação de assistência mútua de emergência, quer recorrendo aos pontos de contacto da rede 24/7 criada ao abrigo da Convenção (artigo 35.º).

- Além disso, os instrumentos de cooperação internacional comprovados devem ser utilizados de forma mais ampla e entre todas as Partes. Já estão disponíveis medidas importantes, como a videoconferência ou as equipas de investigação conjuntas, ao abrigo dos tratados do

Conselho da Europa (por exemplo, o Segundo Protocolo Adicional à Convenção Europeia sobre Assistência Mútua em Matéria Penal, STCE n.º 182) ou de outros acordos bilaterais e multilaterais. No entanto, esses mecanismos não estão universalmente disponíveis entre as Partes na Convenção e o presente Protocolo visa colmatar essa lacuna.

- A Convenção prevê a recolha e o intercâmbio de informação e de elementos de prova para investigações ou processos penais específicos. Os redatores reconheceram que o estabelecimento, a execução e a aplicação de poderes e procedimentos relacionados com investigações e ações penais devem estar sempre sujeitos a condições e salvaguardas prescritas que garantam uma proteção adequada dos direitos humanos e das liberdades fundamentais. Por conseguinte, era necessário incluir um artigo sobre condições e salvaguardas, semelhante ao artigo 15.º da Convenção. Além disso, reconhecendo o requisito, em muitas Partes, de proteger a privacidade e os dados pessoais a fim de cumprir as respetivas obrigações constitucionais e internacionais, os redatores decidiram prever salvaguardas específicas em matéria de proteção de dados no presente Protocolo. Essas salvaguardas em matéria de proteção de dados complementam as obrigações de muitas das Partes na Convenção, que são igualmente Partes na Convenção para a Proteção das Pessoas no que diz respeito ao Tratamento Automatizado de Dados Pessoais (STCE n.º 108). O protocolo de alteração a essa convenção (STCE n.º 223) foi aberto à assinatura durante a redação do referido Protocolo em outubro de 2018. De salientar igualmente que o processo de redação deste Protocolo incluiu Partes não sujeitas, na altura, aos instrumentos do Conselho da Europa em matéria de proteção de dados ou às regras da União Europeia em matéria de proteção de dados. Por conseguinte, foram envidados esforços significativos para assegurar um protocolo equilibrado que reflita os muitos sistemas jurídicos dos Estados suscetíveis de serem Partes no presente Protocolo, respeitando, simultaneamente, a importância de garantir a proteção da privacidade e dos dados pessoais, tal como exigido pelas constituições e obrigações internacionais de outras Partes na Convenção.

24. Os redatores analisaram igualmente outras medidas que, após uma discussão aprofundada, não foram incluídas no presente Protocolo. Duas destas disposições, a saber, "investigações infiltradas ou por meio de sistema informático" e "extensão das buscas", eram de grande interesse para as Partes, mas foram consideradas como necessitando de trabalho, tempo e consultas adicionais com os intervenientes, pelo que não foram consideradas viáveis no prazo estabelecido para a preparação do presente Protocolo. Os redatores propuseram que estas medidas fossem prosseguidas num formato diferente e, eventualmente, num instrumento jurídico distinto.

25. De um modo geral, os redatores consideraram que as disposições deste Protocolo adicionariam muito valor, tanto do ponto de vista operacional como político. O presente Protocolo melhorará significativamente a capacidade das Partes para reforçar a cooperação entre as Partes e entre as Partes e os fornecedores de serviços e outras entidades, bem como para obter a divulgação de provas sob a forma eletrónica para efeitos de investigações ou processos penais específicos. Assim, o presente Protocolo, tal como a Convenção, visa aumentar a capacidade das autoridades responsáveis pela aplicação da lei de combater o cibercrime e outras formas de criminalidade, respeitando plenamente os direitos humanos e as liberdades fundamentais, e salienta a importância e o valor de uma Internet assente na livre circulação de informação.

O presente Protocolo

26. Tal como referido no preâmbulo, o presente Protocolo visa reforçar a cooperação em matéria de cibercrime e a capacidade das autoridades de justiça penal de recolherem provas sob forma eletrónica de uma infração penal para efeitos de investigações ou processos penais específicos através de instrumentos adicionais relacionados com uma assistência mútua mais eficiente e a outras formas de cooperação entre as autoridades competentes mais eficazes, à cooperação em situações de emergência (ou seja, em situações em que exista um risco significativo e iminente para a vida ou a segurança de qualquer pessoa singular), e à cooperação direta entre as autoridades competentes e os fornecedores de serviços e outras entidades na posse ou controlo de informação pertinente. Por conseguinte, o presente Protocolo tem por objetivo complementar a Convenção e, entre as suas Partes, o Primeiro Protocolo.

27. O presente Protocolo está dividido em quatro capítulos: I. "Disposições comuns"; II. "Medidas para uma cooperação reforçada"; III. "Condições e salvaguardas"; e IV. "Disposições finais".

28. As disposições comuns do Capítulo I abrangem o objetivo e o âmbito deste Protocolo. Tal como acontece com a Convenção, o presente Protocolo diz respeito a investigações ou processos penais específicos e não apenas no tocante ao cibercrime, mas também a qualquer infração penal que envolva provas sob a forma eletrónica, em geral designadas por "prova eletrónica" ou "prova digital". O presente capítulo determina igualmente a aplicação das definições da Convenção ao presente Protocolo e inclui definições adicionais dos termos frequentemente utilizados no presente Protocolo. Além disso, tendo em conta que esses requisitos linguísticos para a assistência mútua e outras formas de cooperação dificultam, com frequência, a eficácia dos procedimentos, foi adicionado um artigo sobre a "língua" para permitir uma abordagem mais pragmática a este respeito.

29. O Capítulo II contém os principais artigos substantivos do presente Protocolo, que descrevem os diversos métodos de cooperação à disposição das Partes. São aplicáveis diferentes princípios a cada tipo de cooperação. Por este motivo, foi necessário dividir este capítulo em secções com: 1) princípios gerais aplicáveis ao Capítulo II, 2) procedimentos que reforcem a cooperação direta com fornecedores e entidades de outras Partes, 3) procedimentos que reforcem a cooperação internacional entre as autoridades para a divulgação de dados informáticos armazenados, 4) procedimentos relativos à assistência mútua de emergência e 5) procedimentos relativos à cooperação internacional na ausência de acordos internacionais aplicáveis.

30. O Capítulo III estabelece as condições e salvaguardas que requerem que as Partes apliquem condições e salvaguardas semelhantes às do artigo 15.º da Convenção também aos poderes e procedimentos do presente Protocolo. Além disso, este capítulo inclui um conjunto pormenorizado de salvaguardas para a proteção dos dados pessoais.

31. A maior parte das disposições finais do Capítulo IV é semelhante às disposições-tipo finais dos Tratados do Conselho da Europa ou tornam as disposições da Convenção aplicáveis ao presente Protocolo. No entanto, o artigo 15.º relativo aos "Efeitos do presente Protocolo", o artigo 17.º relativo à "Cláusula federal" e o artigo 23.º relativo às "Consultas das Partes e avaliação da aplicação" diferem em diferentes graus das disposições análogas da Convenção.
Este último artigo não só torna aplicável o artigo 46.º da Convenção, como também prevê que a utilização e a aplicação efetivas das disposições do presente Protocolo sejam periodicamente avaliadas pelas Partes.

Comentários sobre os artigos do presente

Protocolo

Capítulo I – Disposições comuns

Artigo 1.º – Objeto

32. O presente Protocolo tem por objetivo complementar: i) a Convenção entre as Partes no presente Protocolo e ii) o Primeiro Protocolo entre as Partes que são igualmente Partes no presente Protocolo.

Artigo 2.º – Âmbito de aplicação

33. O âmbito de aplicação geral do presente Protocolo é o mesmo do da Convenção: as medidas do presente Protocolo devem ser aplicadas, entre as Partes no presente Protocolo, a investigações ou processos penais específicos relativos a infrações penais relacionadas com sistemas e dados informáticos (ou seja, as infrações abrangidas pelo artigo 14.º, n.º 2, alíneas a) e b) da Convenção), bem como à recolha de provas sob a forma eletrónica de uma infração penal (artigo 14.º, n.º 2, alínea c) da Convenção). Tal como explicado nos n.os 141 e 243 do relatório explicativo da Convenção, isto significa que, quer quando o crime é cometido através da utilização de um sistema informático, quer quando um crime não é cometido através da

utilização de um sistema informático (por exemplo, um homicídio) mas envolve provas sob a forma eletrónica, os poderes, procedimentos e medidas de cooperação criados pelo presente Protocolo devem estar disponíveis.

34. O n.º 1, alínea b), estabelece que, entre as Partes no Primeiro Protocolo que são igualmente Partes no presente Protocolo, o presente Protocolo é igualmente aplicável a investigações ou processos penais específicos relativos a infrações penais estabelecidas nos termos do Primeiro Protocolo. As Partes no presente Protocolo que não sejam Partes no Primeiro Protocolo não são obrigadas a aplicar as disposições do presente Protocolo a essas infrações.

35. Em virtude do n.º 2, cada Parte deverá dispor da base jurídica necessária para cumprir as obrigações estabelecidas no presente Protocolo, caso os seus referidos tratados, legislações ou acordos não incluam já tais disposições. Tal não altera as disposições explicitamente discricionárias em disposições obrigatórias e algumas disposições permitem declarações ou a formulação de reservas. Algumas Partes podem não exigir qualquer legislação de execução para aplicar as disposições do presente Protocolo.

Artigo 3.º – Definições

36. O n.º 1 incorpora no presente Protocolo as definições constantes do artigo 1.º ("sistema informático", "dados informáticos", "fornecedor de serviços" e "dados de tráfego") e do artigo 18.º, n.º 3 ("informação sobre subscritores") da Convenção. Os redatores incluíram estas definições da Convenção porque estes termos são utilizados na parte dispositiva e no relatório explicativo do presente Protocolo. A intenção dos redatores foi igualmente de que as explicações fornecidas no relatório explicativo da Convenção e nas notas de orientação (adotadas pelo T-CY) relacionadas com esses termos se aplicassem igualmente ao presente Protocolo.

37. As definições de infrações e de outros termos incluídos no texto da Convenção destinam-se a ser aplicadas para efeitos de cooperação entre as Partes no presente Protocolo, e as definições de infrações e de outros termos incluídos no texto do Primeiro Protocolo destinam-se a ser aplicadas para efeitos de cooperação entre as Partes no Primeiro Protocolo. Por exemplo, o artigo 2.º, n.º 1, prevê que "as medidas descritas no presente Protocolo são aplicáveis... entre as Partes na Convenção que são Partes no presente Protocolo, em investigações ou processos penais específicos relativos a infrações penais relacionadas com sistemas e dados informáticos". Por conseguinte, ao cooperar ao abrigo do presente Protocolo no que diz respeito a infrações relacionadas com pornografia infantil, aplica-se a definição de "pornografia infantil" constante do artigo 9.º, n.º 2, da Convenção, sendo aplicável a definição de "menor" estabelecida no artigo 9.º, n.º 3, da Convenção. À semelhança do que se verifica entre as Partes no Primeiro Protocolo que são Partes no presente Protocolo, aplica-se a definição de "material racista e xenófobo" constante do artigo 2.º do Primeiro Protocolo. As Partes no presente Protocolo que não sejam Partes no Primeiro Protocolo não são obrigadas a aplicar os termos ou definições nele estabelecidos.

38. O artigo 3.º, n.º 2, inclui definições adicionais aplicáveis ao presente Protocolo e à cooperação ao abrigo do presente Protocolo. O n.º 2, alínea a), define "autoridade central" como a "autoridade ou autoridades designadas ao abrigo de um tratado ou acordo de assistência mútua com base na legislação uniforme ou recíproca em vigor entre as Partes interessadas ou, na sua ausência, a autoridade ou autoridades designadas por uma Parte nos termos do artigo 27.º, n.º 2, alínea a), da Convenção". O presente Protocolo recorre às autoridades centrais em vários artigos, a fim de prestar cooperação através de um canal que as Partes já utilizam e com o qual estão familiarizadas. Por conseguinte, as Partes que tenham tratados ou acordos de assistência mútua com base em legislação uniforme ou recíproca devem recorrer às autoridades centrais designadas ao abrigo desses tratados ou acordos. Na ausência de um tratado ou acordo em vigor entre as Partes em causa, estas são obrigadas a utilizar o mesmo canal da autoridade central que utilizam atualmente nos termos do artigo 27.º, n.º 2, alínea a), da Convenção. Embora nem todos os tratados ou acordos de assistência mútua baseados em legislação uniforme ou recíproca utilizem o termo "autoridade central", a intenção dos redatores era que este termo se referisse às autoridades coordenadoras designadas nesses tratados ou acordos, independentemente da sua denominação.

39. Salvo disposição específica estabelecida no presente Protocolo, o facto de as Partes recorrerem a esses canais da autoridade central para efeitos do presente Protocolo não significa que sejam aplicáveis outras disposições desses tratados ou acordos de assistência mútua.

40. A definição de "autoridade competente" constante no n.º 2, alínea b), baseia-se no n.º 138 do relatório explicativo da Convenção. Uma vez que este termo é frequentemente utilizado no presente Protocolo, a definição foi introduzida na parte dispositiva para facilitar a referência.

41. O n.º 2, alínea c), define "emergência" como "uma situação na qual existe um risco significativo e iminente para a vida ou a segurança de uma pessoa singular". Este termo é utilizado nos artigos 9.º, 10.º e 12.º. A definição de "emergência" no presente Protocolo visa impor um limiar significativamente mais elevado do que "circunstâncias urgentes" na aceção do artigo 25.º, n.º 3, da Convenção. Esta definição foi igualmente redigida de modo a permitir que as Partes tenham em conta os diferentes contextos em que o termo é utilizado no presente Protocolo, considerando simultaneamente a legislação e as políticas aplicáveis das Partes.

42. A definição de emergência visa abranger as situações em que o risco é significativo e iminente, no sentido em que não abrange as situações nas quais o risco para a vida ou a segurança da pessoa já tenha passado ou seja insignificante, ou nas quais possa existir um risco futuro que não seja iminente. A razão para estes requisitos de importância e iminência explica-se pelo facto de os artigos 9.º e 10.º imporem obrigações intensivas em termos de trabalho às Partes requerentes e às Partes requeridas no sentido de reagir de forma muito acelerada em situações de emergência, o que exige, por conseguinte, que seja dada maior prioridade aos pedidos de emergência do que a outros casos importantes, mas um pouco menos urgentes, mesmo que tenham sido apresentados anteriormente. As situações que impliquem "um risco significativo e iminente para a vida ou a segurança de qualquer pessoa singular" podem envolver, por exemplo, situações de reféns em que exista um risco credível de perda iminente de vidas humanas, ferimentos graves ou outros danos semelhantes para a vítima; abuso sexual em curso de uma criança; cenários imediatos pós-ataque terrorista em que as autoridades procuram determinar com quem os atacantes comunicaram para determinar se estão iminentes novos ataques; e ameaças à segurança de infraestruturas críticas em que exista um risco significativo e iminente para a vida ou a segurança de uma pessoa singular.

43. Tal como explicado no artigo 10.º, n.º 4, do presente Protocolo e no n.º 154 do presente relatório explicativo relativo ao artigo 9.º, uma Parte requerida ao abrigo desses artigos determinará se existe uma "emergência", aplicando a definição constante do presente artigo.

44. O n.º 2, alínea d), define "dados pessoais" como "informação relativa a uma pessoa singular identificada ou identificável". Entende-se por "pessoa singular identificável" uma pessoa que possa ser identificada, direta ou indiretamente, por referência, nomeadamente, a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, mental, económica, cultural ou social. A definição de "dados pessoais" no âmbito do presente Protocolo é coerente com a de outros instrumentos internacionais, como a Convenção para a Proteção das Pessoas no que diz respeito ao Tratamento Automatizado de Dados Pessoais, com a redação que lhe foi dada pelo seu Protocolo adicional, as Orientações de 2013 da Organização para a Cooperação e Desenvolvimento Económico (OCDE) que regem a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais, o Regulamento geral sobre a Proteção de Dados e a Diretiva Proteção de Dados na aplicação da lei da UE e a Convenção da União Africana sobre Cibersegurança e Proteção de Dados Pessoais ("Convenção de Malabo").

45. Uma pessoa não é considerada "identificável" se a identificação exigir tempo, esforço ou recursos excessivos. Embora determinada informação possa ser única para uma determinada pessoa, estabelecendo assim uma ligação a essa pessoa em si mesma e por si só, outra informação só pode permitir a identificação quando combinada com informação pessoal ou de identificação adicional. Por conseguinte, se a identificação de uma pessoa com base na ligação a essa informação adicional exigir tempo, esforço ou recursos excessivos, a informação em causa não constitui dados pessoais. O facto de uma pessoa singular poder ser identificada ou ser identificável, direta ou indiretamente, depende das circunstâncias específicas no seu contexto específico (e pode mudar ao longo do tempo com a evolução tecnológica ou outra).

46. Os requisitos em matéria de proteção de dados estabelecidos no presente Protocolo não se aplicam aos dados que não sejam "dados pessoais", tais como informação anonimizada que não possa ser reidentificada sem tempo, esforço ou recursos excessivos.

Artigo 4.º – Língua

47. O artigo 4.º estabelece um quadro relativo às línguas que podem ser utilizadas quando se interage com as Partes e os fornecedores de serviços ou outras entidades nos termos do presente Protocolo. Mesmo nos casos em que, na prática, as Partes podem trabalhar em línguas que não as suas línguas oficiais, essa possibilidade pode não estar prevista no direito interno ou nos tratados. O objetivo deste artigo é proporcionar flexibilidade adicional ao abrigo do presente Protocolo.

48. As traduções inexatas ou onerosas dos pedidos de assistência mútua relacionados com provas sob a forma eletrónica constituem uma queixa crónica que requer uma atenção urgente. Este impedimento prejudica os processos legítimos de obtenção de dados e de proteção da segurança pública. As mesmas considerações são aplicáveis fora do âmbito da assistência mútua tradicional, nomeadamente, quando uma Parte transmite um despacho diretamente a um fornecedor de serviços no território da outra Parte ao abrigo do artigo 7.º, ou solicita a execução de um despacho ao abrigo do artigo 8.º. Embora se preveja uma melhoria das capacidades da tradução automática, estas são atualmente inadequadas. Por estas razões, o problema da tradução foi repetidamente mencionado nas propostas relativas aos artigos a incluir no presente Protocolo.

49. A tradução para e a partir de línguas menos comuns constitui um problema especial, uma vez que essas traduções podem atrasar consideravelmente um pedido ou dar origem à impossibilidade efetiva da sua obtenção. Podem também induzir em erro de forma crítica e a sua má qualidade pode conduzir ao desperdício do tempo de ambas as Partes. No entanto, o custo e a dificuldade das traduções recaem desproporcionadamente sobre as Partes que solicitam línguas menos comuns.

50. Devido a este encargo desproporcionado, uma série de Partes não anglófonas solicitaram que o inglês fosse mandatado no presente Protocolo. Observaram que o inglês é uma língua comummente utilizada pelos principais fornecedores de serviços. Além disso, à medida que os dados são deslocados e armazenados de forma mais generalizada no mundo e que cada vez mais países participam na assistência mútua, a tradução pode tornar-se ainda mais onerosa e impraticável. Por exemplo, duas Partes podem utilizar línguas menos comuns, estar geograficamente distantes e ter pouco contacto. Se a Parte A necessitar subitamente da assistência da Parte B, poderá não estar em condições de encontrar um tradutor para a língua de B, ou uma eventual tradução pode ser menos inteligível do que o inglês não nativo. Os redatores salientaram, em especial, que, para acelerar a assistência, devem ser envidados todos os esforços para aceitar, em especial, os pedidos com caráter de emergência ao abrigo do presente Protocolo em inglês ou numa língua partilhada, em vez de exigir a tradução para a língua oficial da Parte requerida.

51. Os redatores deste Protocolo concluíram que o inglês não deve ser mandatado no presente Protocolo. Algumas Partes têm requisitos linguísticos oficiais que excluem esse mandato, muitas Partes partilham uma língua e não têm necessidade do inglês, em algumas Partes, a probabilidade de os funcionários fora das capitais lerem inglês é menor, mas estão frequentemente envolvidos na execução dos pedidos.

52. Assim, o n.º 1 é redigido em termos de "uma língua aceite pela Parte requerida ou pela Parte notificada nos termos do artigo 7.º". Essa Parte pode especificar línguas aceitáveis – por exemplo, línguas amplamente faladas, como o inglês, o espanhol ou o francês – mesmo que estas não estejam contempladas no seu direito interno ou nos seus tratados.

53. Na aceção do n.º 1, "os pedidos, as injunções e a informação que os acompanha" refere-se a:

- o pedido (n.º 3), a injunção (n.º 3, alínea a)), a informação de apoio (n.º 3, alínea b)) e quaisquer instruções processuais especiais (n.º 3, alínea c)) nos termos do artigo 8.º;

- a injunção (n.º 3), informação suplementar (n.º 4) e a síntese dos factos (n.º 5, alínea a)) para as Partes que exigem notificação nos termos do artigo 7.º, n.º 5;

- o pedido (n.º 3) nos termos do artigo 9.º.

"Pedidos" refere-se igualmente ao teor dos pedidos ao abrigo dos artigos 10.º, 11.º e 12.º, que inclui a documentação que integra o pedido.

54. Na prática, alguns países podem estar preparados para aceitar pedidos e injunções numa língua que não uma língua especificada no direito interno ou nos tratados. Assim, uma vez por ano, o T-CY realizará um inquérito informal sobre as línguas aceitáveis para os pedidos e as injunções. As Partes podem alterar a sua informação a qualquer momento, devendo todas as Partes ser informadas dessa alteração. Podem indicar que apenas aceitam as línguas especificadas para determinadas formas de assistência. Os resultados deste inquérito serão divulgados a todas as Partes na Convenção e não apenas às Partes no presente Protocolo.

55. Esta disposição pragmática demonstra a extrema importância de acelerar a cooperação. Constitui uma base do tratado para uma Parte aceitar línguas adicionais para efeitos do presente Protocolo.

56. Em muitos casos, as Partes celebraram tratados de assistência mútua que especificam a língua ou línguas em que os pedidos ao abrigo desses tratados devem ser apresentados. O presente artigo não interfere com os termos desses tratados ou outros acordos entre as Partes. Além disso, espera-se que, para efeitos do presente Protocolo, "uma língua aceite pela Parte requerida ou pela Parte notificada nos termos do artigo 7.º" inclua qualquer língua ou línguas especificadas por esses tratados ou acordos. Por conseguinte, uma Parte requerente deve aplicar a língua especificada nos tratados de assistência mútua ou noutros acordos aos pedidos e notificações apresentados ao abrigo do presente Protocolo, a menos que a Parte requerida ou notificada indique que está igualmente disposta a aceitar esses pedidos ou notificações noutras línguas.

57. A disponibilidade de uma Parte para aceitar outras línguas refletir-se-á através da sua indicação ao T-CY de que tenciona aceitar alguns ou todos os tipos de pedidos ou notificações de injunções ao abrigo do presente Protocolo noutra língua.

58. O n.º 2 determina a língua ou línguas que a Parte emissora deve utilizar para apresentar injunções ou pedidos e informação de acompanhamento aos fornecedores de serviços ou entidades que prestam serviços de registo de nomes de domínio no território da outra Parte, nos termos dos artigos 7.º e 6.º, respetivamente. Esta disposição destina-se a assegurar uma cooperação rápida e uma maior certeza, sem impor encargos adicionais aos fornecedores ou entidades de serviços quando recebem injunções ou pedidos de divulgação de dados. A primeira opção, prevista no n.º 2, alínea a), indica que a injunção ou o pedido podem ser apresentados numa língua que o fornecedor de serviços ou a entidade aceita normalmente injunções ou pedidos nacionais das suas próprias autoridades no âmbito de investigações ou processos penais específicos ("processo nacional comparável"). Para as Partes que tenham uma ou mais línguas oficiais, tal incluirá uma dessas línguas. A segunda opção, prevista no n.º 2, alínea b), indica que, se um fornecedor de serviços ou uma entidade concordar em receber injunções ou pedidos noutra língua, por exemplo, na língua da sua sede, essas injunções e a informação que as acompanham podem ser apresentadas nessa língua. Como terceira opção, o n.º 2, alínea c), prevê que, quando a injunção ou o pedido e a informação que o acompanham não forem emitidos numa das línguas das duas primeiras opções, devem ser acompanhados de uma tradução numa dessas línguas.

59. Tal como utilizado no n.º 2, "as injunções ao abrigo do artigo 7.º e os pedidos ao abrigo do artigo 6.º, bem como qualquer informação que os acompanhe" referem-se a:

- o pedido (n.º 3) nos termos do artigo 6.º; e

- a injunção (n.º 3) e a informação suplementar (n.º 4) nos termos do artigo 7.º.

60. Sempre que uma Parte tenha exigido uma notificação nos termos do artigo 7.º, a Parte requerente deve estar preparada para enviar a injunção e qualquer informação que a acompanhe numa língua aceitável para a Parte que exige a notificação, não obstante a aceitação pelo fornecedor de serviços de outras línguas.

61. Informalmente, o T-CY esforçar-se-á também por recolher informação sobre as línguas nas quais as injunções e os pedidos e a informação que os acompanham serão apresentados aos fornecedores de serviços e entidades que prestam serviços de registo de nomes de domínio nos termos do artigo 4.º, n.º 2, e por informar as Partes no âmbito do inquérito descrito no n.º 54 do relatório explicativo acima.

Capítulo II – Medidas para uma cooperação reforçada

Secção 1 – Princípios gerais aplicáveis ao Capítulo II

Artigo 5.º – Princípios gerais aplicáveis ao Capítulo II

62. O artigo 5.º, n.º 1, deixa claro que, tal como no artigo 23.º e no artigo 25.º, n.º 1, da Convenção, as Partes prestarão, em conformidade com o disposto no Capítulo II, uma cooperação "o mais ampla possível". Este princípio exige que as Partes prestem uma ampla cooperação e minimizem os obstáculos ao fluxo rápido e harmonioso de informação e de provas a nível internacional.

63. Os n.os 2 a 5 organizam as sete medidas de cooperação do presente Protocolo em quatro secções diferentes que se seguem à primeira secção relativa aos princípios gerais. Estas secções dividem-se pelos tipos de cooperação pretendidos: a secção 2 abrange a cooperação direta com entidades privadas; a secção 3 contém formas de cooperação internacional reforçada entre as autoridades para a divulgação dos dados armazenados; a secção 4 prevê a assistência mútua em situações de emergência; e a secção 5 conclui com disposições de cooperação internacional a aplicar na ausência de um tratado ou acordo com base em legislação uniforme ou recíproca entre as Partes em causa. Estas secções estão também organizadas de forma progressiva, das formas de assistência à investigação frequentemente solicitada numa fase inicial de uma investigação – para obter a divulgação de informação sobre o registo de nomes de domínio e os subscritores – até aos pedidos de dados de tráfego e, em seguida, de dados de conteúdo, seguidos de videoconferências e equipas de investigação conjuntas, que são formas de assistência procuradas, com frequência, nas fases posteriores de uma investigação.

64. A presente secção relativa aos princípios gerais esclarece em que grau cada medida é ou não afetada pela existência de um tratado ou acordo de assistência mútua com base em legislação uniforme ou recíproca entre as Partes em causa, ou seja, a Parte requerente e a Parte requerida para a cooperação entre governos, a Parte que solicita a informação e a Parte em cujo território a entidade privada que detém ou controla essa informação está localizada para efeitos de cooperação direta nos termos dos artigos 6.º e 7.º. Um "acordo com base em legislação uniforme ou recíproca" refere-se a acordos "sendo disso exemplo o sistema de cooperação desenvolvido entre os países nórdicos, o qual é igualmente reconhecido pela Convenção Europeia sobre Assistência Mútua em Matéria Penal (artigo 250.º, nº 4), e entre os membros da Commonwealth" (ver o n.º 263 do relatório explicativo à Convenção). As medidas previstas nas secções 2 a 4 do presente capítulo são aplicáveis independentemente de as Partes em causa estarem ou não mutuamente vinculadas por um acordo ou convénio de assistência mútua aplicável com base em legislação uniforme ou recíproca. Salvo disposição em contrário, as disposições em matéria de cooperação internacional constantes da secção 5 só se aplicam na ausência de tais acordos ou convénios.

65. Tal como descrito no n.º 2 do presente artigo, a secção 2 do deste capítulo é constituída pelo artigo 6.º, intitulado "Pedido de informação sobre o registo de nomes de domínio", e pelo artigo 7.º intitulado "Divulgação de informação sobre subscritores". Trata-se dos chamados artigos de "cooperação direta" que permitem às autoridades competentes de uma Parte interagir diretamente com entidades privadas – ou seja, com entidades que prestam serviços de registo de nomes de domínio nos termos do artigo 6.º e com fornecedores de serviços no artigo 7.º –

para efeitos de investigações ou processos penais específicos. A secção 2 aplica-se independentemente de existir ou não um tratado ou acordo de assistência mútua com base na legislação uniforme ou recíproca em vigor entre a Parte que solicita a informação e a Parte em cujo território se encontra a entidade privada que detém ou controla essa informação.

66. Tal como descrito no n.º 3 do presente artigo, a secção 3 deste capítulo é constituída pelo artigo 8.º intitulado "Execução de injunções de outra Parte para a apresentação expedita de informação sobre subscritores e dados de tráfego", e pelo artigo 9.º intitulado "Divulgação expedita de dados informáticos armazenados em caso de emergência". Trata-se de medidas destinadas a "reforçar a cooperação internacional entre autoridades", ou seja, prevê a cooperação entre as autoridades competentes, mas de natureza diferente da cooperação internacional tradicional. A secção 3 aplica-se independentemente de existir ou não um tratado ou acordo de assistência mútua com base em legislação uniforme ou recíproca em vigor entre as Partes requerente e requerida.

67. Tal como descrito no n.º 4 do presente artigo, a secção 4 deste capítulo é constituída pelo artigo 10.º intitulado "Assistência mútua de emergência". Embora a assistência mútua de emergência seja uma prestação de assistência mútua, constitui um instrumento de cooperação importante para situações de emergência que não esteja expressamente previsto em muitos tratados de assistência mútua. Por conseguinte, os redatores decidiram que a presente secção deveria ser aplicável independentemente de existir ou não um acordo ou convénio de assistência mútua aplicável com base na legislação uniforme ou recíproca em vigor entre as Partes em causa. No tocante aos procedimentos que regem a assistência mútua de emergência, existem duas possibilidades. Quando as Partes em causa estiverem mutuamente vinculadas por um acordo ou convénio de assistência mútua aplicável com base em legislação uniforme ou recíproca, a secção 4 é complementada pelas disposições desse acordo, a menos que as Partes em causa decidam mutuamente aplicar determinadas disposições da Convenção em seu lugar (ver artigo 10.º, n.º 8, do presente Protocolo). Quando as Partes em causa não estiverem mutuamente vinculadas por esse acordo ou convénio, aplicam determinados procedimentos previstos nos artigos 27.º e 28.º da Convenção, relativos à assistência mútua na ausência de um tratado (ver artigo 10.º, n.º 7, do presente Protocolo).

68. Tal como descrito no n.º 5 do presente artigo, a secção 5 do presente capítulo é constituída pelo artigo 11.º, intitulado "Videoconferência", e pelo artigo 12.º intitulado "Equipas de investigação conjuntas e investigações conjuntas". Estas disposições são medidas de cooperação internacional que se aplicam apenas em caso de inexistência de quaisquer tratados de assistência mútua ou acordos celebrados com base numa legislação uniforme ou recíproca, entre as Partes requerente e requerida. Estas medidas não são aplicáveis nos casos em que esse tratado ou acordo exista, exceto se o artigo 12.º, n.º 7, for aplicável independentemente da existência ou não desse tratado ou acordo. No entanto, as Partes em causa podem decidir mutuamente aplicar as disposições da secção 5 em vez de um tratado ou acordo existente, a menos que tal seja proibido pelos termos do tratado ou do acordo.

69. O n.º 6 é elaborado com base o artigo 25.º, n.º 5, da Convenção, pelo que o n.º 259 do relatório explicativo da Convenção também é válido neste caso: "Nos casos em que a Parte requerida esteja autorizada a exigir a dupla criminalidade como condição necessária à prestação de assistência... considera-se que existe dupla criminalidade caso a conduta subjacente à infração para a qual é pedida a assistência seja igualmente classificada como infração penal à luz da legislação da Parte requerida, mesmo que tal legislação inclua a dita infração numa categoria diferente de infrações ou que a terminologia utilizada na sua designação não seja a mesma. A necessidade inerente a esta disposição é a de assegurar que as Partes requeridas não se regem por critérios demasiadamente rígidos em se tratando da aplicação da dupla criminalidade. Tendo em conta as diferenças verificadas ao nível dos sistemas jurídicos internos, é inevitável a constatação das variações existentes no plano da terminologia e da categorização das condutas de índole criminosa. Se a conduta em causa constituir uma infração penal ao abrigo de ambos os sistemas jurídicos, as diferenças de ordem técnica não deverão, pois, constituir um impedimento à prestação de assistência. Nos casos aos quais é aplicável o critério da dupla criminalidade, tal deverá ocorrer com alguma flexibilidade a fim de facilitar a concessão de assistência".

70. O n.º 7 estabelece que "as disposições do presente capítulo não restringem a possibilidade de cooperação entre as Partes, ou entre as Partes e os fornecedores de serviços ou outras entidades, através de outros acordos, convénios, práticas ou direito interno aplicáveis". Isto significa que o Protocolo não elimina nem restringe qualquer cooperação entre as Partes ou entre as Partes e entidades privadas que esteja disponível de outra forma – seja através de acordos, convénios, legislação nacional ou mesmo de práticas informais aplicáveis. Os redatores pretenderam alargar, sem restringir, os instrumentos disponíveis no conjunto de instrumentos disponíveis aos profissionais responsáveis pela aplicação da lei para obter informação ou elementos de prova para investigações ou processos penais específicos. Os redatores reconheceram que, em determinadas situações, os mecanismos existentes, como a assistência mútua, podem ser os melhores para um profissional utilizar. No entanto, noutras situações, os instrumentos criados pelo presente Protocolo podem ser mais eficientes ou preferíveis. Por exemplo, se uma autoridade competente necessitar de dados de conteúdo numa base não urgente, poderá optar por utilizar um pedido tradicional de assistência mútua ao abrigo de um tratado bilateral ou do artigo 27.º da Convenção, conforme aplicável, uma vez que o Protocolo não contém disposições para a obtenção de dados de conteúdo numa base não urgente. No entanto, se necessitar de informação sobre subscritores, poderá optar por recorrer ao artigo 7.º do Protocolo para emitir uma injunção diretamente a um fornecedor de serviços.

71. Por último, algumas disposições do Capítulo II e de outras disposições do presente Protocolo permitem a imposição de limitações ou condições de utilização, tais como a confidencialidade. Quando, nos termos das disposições do presente Protocolo, a receção dos elementos de prova ou da informação solicitados estiver sujeita a tal limitação ou condição de utilização, os negociadores reconheceram as exceções e estão implícitas no texto. Em primeiro lugar, enquanto medida de proteção dos direitos humanos e das liberdades em conformidade com o artigo 13.º, ao abrigo dos princípios jurídicos fundamentais de muitos Estados, se o material fornecido à Parte recetora for considerado ilibatório para um arguido, deve ser comunicado à defesa ou a uma autoridade judicial. Este princípio não prejudica o texto do artigo 12.º, n.º 6, alínea b), nem o n.º 215 do relatório explicativo, podendo ser aplicados nos casos em que as Partes tenham criado uma equipa de investigação conjunta. Os redatores entenderam que, nesses casos, a Parte recetora notificará a Parte que procede à transferência antes da divulgação e, se tal lhe fosse solicitado, consultará a Parte que procede à transferência. Em segundo lugar, quando tenha sido imposta uma limitação de utilização relativamente ao material recebido ao abrigo do presente Protocolo que esteja prevista para utilização em julgamento, o julgamento (incluindo as divulgações durante o processo de instrução judicial) é normalmente um processo público. Uma vez tornado público no julgamento, o material passou a ser do domínio público. Em situações como esta, não será possível garantir a confidencialidade da investigação ou da ação penal relativamente à qual o material foi solicitado. Estas exceções são semelhantes às exceções relacionadas com a aplicação do artigo 28.º, n.º 2, da Convenção, tal como explicado no n.º 278 do relatório explicativo da Convenção. Por último, o material pode ser utilizado para outros fins se tiver sido obtido o consentimento prévio de uma Parte que procede à transferência.

Secção 2 – Procedimentos para reforçar a cooperação direta com fornecedores e entidades de outras Partes

Artigo 6 – Pedido de informação sobre o registo de nomes de domínio

72. O artigo 6.º estabelece um procedimento que prevê a cooperação direta entre as autoridades de uma Parte e uma entidade que presta serviços de registo de nomes de domínio no território de outra Parte, a fim de obter informação sobre os registos de nomes de domínio na Internet. À semelhança do artigo 7.º, o procedimento baseia-se nas conclusões do *Cloud Evidence Group* do Comité da Convenção sobre o Cibercrime, que reconhece a importância de um acesso transfronteiras atempado a provas sob a forma eletrónica em investigações ou processos penais específicos, tendo em conta os desafios colocados pelos procedimentos existentes de obtenção de provas sob a forma eletrónica.

73. O procedimento reconhece igualmente o atual modelo de governação da Internet, que assenta no desenvolvimento de políticas que envolvem vários intervenientes baseadas em consensos. Estas políticas fundamentam-se normalmente no direito contratual. O procedimento previsto no presente artigo destina-se a complementar essas políticas para efeitos do presente Protocolo,

ou seja, para efeitos de investigações ou processos penais específicos. A obtenção dos dados relativos ao registo de nomes de domínio é muitas vezes indispensável, como primeiro passo para muitas investigações penais e para determinar para onde dirigir os pedidos de cooperação internacional.

74. Muitas formas de cibercrime são facilitadas pelos infratores que criam e exploram domínios para fins maliciosos e ilícitos. Por exemplo, um nome de domínio pode ser utilizado como plataforma para a propagação de *malware*, *botnets*, *phishing* e atividades semelhantes, fraude, distribuição de materiais de abuso infantil e para outros fins criminosos. O acesso à informação sobre a pessoa singular ou coletiva que registou um domínio (o "registante") é, por conseguinte, fundamental para identificar um suspeito numa investigação ou processo penal específico. Embora os dados relativos ao registo de nomes de domínio estivessem historicamente disponíveis ao público, o acesso a alguma informação é agora limitado, o que afeta as autoridades judiciais e policiais nas suas funções de política pública.

75. A informação relativa ao registo de nomes de domínio é detida por entidades que prestam serviços de registo de nomes de domínio. Estas incluem organizações que vendem nomes de domínio ao público ("agentes de registo"), bem como operadores de registos regionais ou nacionais que mantêm bases de dados fidedignas ("registos") de todos os nomes de domínio registados para um domínio de nível superior e que aceitam pedidos de registo. Em determinados casos, essa informação pode ser considerada dados pessoais e estar protegida ao abrigo da regulamentação em matéria de proteção de dados na Parte onde está localizada a respetiva entidade que presta serviços de registo de nomes de domínio (o agente de registo ou o registo) ou onde está localizada a pessoa a quem os dados dizem respeito.

76. O objetivo do artigo 6.º é proporcionar um quadro eficaz e eficiente para obter informação para identificar ou contactar o registante de um nome de domínio. A forma de aplicação depende das considerações jurídicas e políticas das Partes. Este artigo destina-se a complementar as políticas e práticas atuais e futuras em matéria de governação da Internet.

N.º 1

77. Nos termos do n.º 1, cada Parte deve adotar as medidas necessárias para habilitar as suas autoridades competentes a emitir pedidos diretamente a uma entidade que preste serviços de registo de nomes de domínio no território de outra Parte, ou seja, sem exigir que as autoridades do território em que a entidade está localizada atuem como intermediárias. O n.º 1 confere às Partes flexibilidade quanto ao formato em que os pedidos são apresentados, uma vez que o formato depende das respetivas considerações jurídicas e políticas das Partes. Uma Parte pode utilizar os procedimentos previstos no seu direito interno, incluindo a emissão de uma injunção; no entanto, para efeitos do artigo 6.º, tal injunção é tratada como um pedido não vinculativo. A forma do pedido ou os efeitos que produz nos termos do direito interno da Parte requerente não afetarão, por conseguinte, o caráter voluntário da cooperação internacional ao abrigo do presente artigo e, se a entidade não divulgar a informação solicitada, será aplicável o n.º 5.

78. A redação do artigo 6.º, n.º 1, é suficientemente ampla para reconhecer que esse pedido também pode ser emitido e que a informação pode ser obtida através de uma interface, portal ou outra ferramenta técnica disponibilizada pelas organizações. Por exemplo, uma organização pode dispor de uma interface ou uma ferramenta de transparência para facilitar ou acelerar a divulgação de informação sobre o registo de nomes de domínio na sequência de um pedido. No entanto, em vez de adaptar este artigo a qualquer portal ou interface específico, este artigo utiliza termos tecnologicamente neutros para permitir a adaptação à tecnologia em constante evolução.

79. Tal como previsto no artigo 2.º, um pedido ao abrigo do n.º 1 só pode ser emitido para efeitos de investigações ou processos penais específicos. O termo "autoridade competente" é definido no artigo 3.º, n.º 2, alínea b), e refere-se a "autoridade judicial, administrativa ou outra que zele pela aplicação da lei e que se encontre, ao abrigo do direito interno, investida dos poderes necessários para ordenar, autorizar ou executar as medidas nos termos deste Protocolo". Uma "entidade que preste serviços de registo de nomes de domínio" refere-se atualmente a agentes de registo e registos. Para ter em conta a situação atual e, ao mesmo tempo, permitir a adaptação, uma vez que os modelos de negócios e a arquitetura da Internet podem mudar ao longo do tempo, este artigo utiliza o termo mais genérico de "entidade que preste serviços de

registo de nomes de domínio".

80. Embora a informação para identificar ou contactar o registante de um nome de domínio seja, com frequência, armazenada por entidades que prestam serviços gerais de registo de nomes de domínio a nível mundial, por exemplo, "domínios genéricos de nível superior", as Partes reconheceram que os serviços de registo de nomes de domínio mais específicos relacionados com entidades nacionais ou regionais ("domínios de nível superior com código de país") podem também ser registados por pessoas ou entidades de outros países e também podem ser utilizados por infratores. Por conseguinte, o artigo 6.º não se limita às entidades que fornecem domínios genéricos de nível superior, uma vez que ambos os tipos de serviços de registo de nomes de domínio – ou futuros tipos desses serviços – podem ser utilizados para cometer o cibercrime.

81. A expressão "informação para identificar ou contactar o registante de um nome de domínio" refere-se à informação anteriormente disponibilizada ao público através dos chamados instrumentos de vigilância WHOIS, tais como o nome, o endereço físico, o endereço de e-mail e o número de telefone de um registante. Algumas Partes podem considerar esta informação como um subconjunto de informação de subscritores, tal como definido no artigo 18.º, n.º 3, da Convenção. A informação de registo de nomes de domínio é informação básica que não permite tirar conclusões precisas sobre a vida privada e os hábitos quotidianos das pessoas. A sua divulgação pode, portanto, ser menos intrusiva do que a divulgação de outras categorias de dados.

N.º 2

82. O n.º 2 exige que cada Parte adote medidas para permitir que as entidades no seu território que prestam serviços de registo de nomes de domínio divulguem essa informação em resposta a um pedido apresentado ao abrigo do n.º 1, sob reserva de condições razoáveis estabelecidas no direito interno, que, em algumas Partes, podem incluir condições de proteção de dados. Simultaneamente, o artigo 14.º limita a possibilidade de recusar transferências de dados ao abrigo das regras de proteção de dados relativas às transferências internacionais, tendo sido incluídos os fatores referidos no n.º 83 para facilitar o tratamento ao abrigo das regras de proteção de dados. Estas medidas devem facilitar, tanto quanto possível, a divulgação rápida e eficaz dos dados solicitados.

83. O presente artigo não exige que as Partes adotem legislação que obrigue estas entidades a responder a um pedido de uma autoridade de outra Parte. Assim, a entidade que disponibiliza serviços de registo de nomes de domínio pode ter de determinar se divulga a informação solicitada. O presente Protocolo contribui para esta determinação, prevendo salvaguardas que deverão facilitar a capacidade de as entidades responderem sem dificuldade aos pedidos ao abrigo do presente artigo, tais como:

- o presente Protocolo prevê ou exige que as Partes forneçam uma base jurídica para os pedidos;

- este artigo requer que o pedido emane de uma autoridade competente (artigo 6.º, n.os 1 e 3, alínea a), e n.os 79 e 84 do presente relatório explicativo);

- o Protocolo prevê que seja apresentado um pedido para efeitos de investigações ou processos penais específicos (artigo 2.º);

- este artigo exige que o pedido contenha uma declaração de que a necessidade da informação se deve à sua relevância para uma investigação ou processo penal específico e de que a informação só será utilizada para essa investigação ou processo penal específico (artigo 6.º, n.º 3, alínea c));

- o presente Protocolo prevê salvaguardas para o tratamento de dados pessoais divulgados e transferidos em conformidade com esses pedidos através do artigo 14.º;

- a informação a divulgar é limitada e não permite tirar conclusões precisas sobre a vida privada das pessoas;

- pode esperar-se ou obrigar as entidades a cooperarem ao abrigo de acordos contratuais com a Corporação da Internet para Atribuição de Nomes e Números (ICANN).

N.º 3

84. O n.º 3 do presente artigo especifica a informação que, no mínimo, deve ser prestada por uma autoridade que emita um pedido nos termos do n.º 1 do presente artigo. Esta informação é particularmente relevante para a execução do pedido pela entidade que presta serviços de registo de nomes de domínio. O pedido deverá incluir:

a. a data do pedido e a identidade e os dados de contacto da autoridade competente que emite o pedido (n.º 3, alínea a)) (ver o n.º 79 do relatório explicativo);

b. o nome de domínio sobre o qual é solicitada informação e uma lista pormenorizada da informação solicitada, incluindo os elementos de dados específicos, tais como o nome, o endereço físico, o endereço de e-mail ou o número de telefone de um registante (n.º 3, alínea b));

c. uma declaração de que o pedido foi emitido nos termos do presente Protocolo; ao fazer esta declaração, a Parte indica que o pedido está em conformidade com o disposto no presente Protocolo (n.º 3, alínea c)). A Parte requerente confirma igualmente nesta declaração que a informação é "necessária" devido à sua relevância para uma investigação ou processo penal específico e que a informação só será utilizada para essa investigação ou processo penal específico.

   Para os países europeus, a informação é "necessária" – ou seja, necessária e proporcionada – para uma investigação ou um processo penal deve decorrer dos princípios da Convenção do Conselho da Europa de 1950 para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, da sua jurisprudência aplicável e da legislação e jurisprudência nacionais. Essas fontes determinam que o poder ou o procedimento devem ser proporcionais à natureza e às circunstâncias de uma infração (ver o n.º 146 do relatório explicativo da Convenção sobre o Cibercrime). As outras Partes aplicarão princípios conexos do seu direito, tais como princípios relevantes (ou seja, que os elementos de prova procurados por um pedido devem ser relevantes para a investigação ou a ação penal). As Partes devem evitar pedidos amplos de divulgação de informação sobre o nome de domínio, a menos que seja necessário para a investigação ou o processo penal específico;

d. o prazo e o modo de divulgação da informação e quaisquer outras instruções processuais especiais (n.º 3, alínea d)). As "instruções processuais especiais" destinam-se a incluir qualquer pedido de confidencialidade, incluindo um pedido de não divulgação do pedido ao registante ou a terceiros. Se a confidencialidade for necessária para evitar uma divulgação prematura da questão, tal deve ser indicado no pedido. Em algumas Partes, a confidencialidade do pedido será mantida por força da lei, ao passo que noutras Partes tal não é necessariamente o caso. Por conseguinte, sempre que seja necessária confidencialidade, as Partes são incentivadas a analisar a informação disponível ao público e a procurar orientações junto de outras Partes sobre a legislação aplicável, bem como sobre as políticas das entidades que prestam serviços de registo de nomes de domínio em matéria de informação de subscritores/registantes, antes de apresentarem um pedido nos termos do n.º 1 à entidade. Além disso, as instruções processuais especiais podem incluir a especificação do canal de transmissão mais adaptado às necessidades da autoridade.

85. O n.º 3 não inclui a obrigação de incluir uma declaração dos factos no pedido, tendo em conta que esta informação é confidencial na maioria das investigações criminais e não pode ser divulgada a uma parte privada. No entanto, a entidade que recebe um pedido ao abrigo deste artigo pode necessitar de determinada informação adicional que lhe permita tomar uma decisão positiva relativa ao pedido. Por conseguinte, a entidade pode procurar mais informação se não puder executar o pedido de outra forma.

N.º 4

86. O objetivo do n.º 4 é incentivar a utilização de meios eletrónicos quando tal for aceitável para a entidade que presta serviços de registo de nomes de domínio, uma vez que estes são quase sempre os meios de comunicação mais eficientes e mais rápidos. Por conseguinte, se for aceitável para a entidade que presta serviços de registo de nomes de domínio, uma Parte pode apresentar um pedido à entidade em formato eletrónico, utilizando, por exemplo, o e-mail, portais eletrónicos ou outros meios. Embora se presuma que as entidades preferem receber pedidos nesse formato, não é obrigatório que apenas este formato possa ser utilizado. Tal como previsto noutros artigos do presente Protocolo que permitem injunções ou pedidos em formato eletrónico (como os artigos 7.º, 8.º e outros), podem ser exigidos níveis apropriados de segurança e autenticação. As Partes e as entidades podem decidir elas próprias se existem canais ou meios seguros de transmissão e autenticação ou se podem ser necessárias medidas de proteção especiais de segurança (incluindo a encriptação) num caso particularmente sensível.

N.º 5

87. Embora esta disposição diga respeito a "pedidos" e não a "injunções" obrigatórias para a divulgação de dados de registo de nomes de domínio, espera-se que uma entidade requerida possa divulgar a informação solicitada nos termos desta disposição, quando estiverem reunidas as condições aplicáveis. Se a entidade não divulgar a informação solicitada, poderão, dependendo das circunstâncias, ser considerados outros mecanismos para obter a informação. Por conseguinte, o n.º 5 prevê a realização de consultas entre as Partes envolvidas com vista a obter informação adicional e a determinar os mecanismos disponíveis, por exemplo, para melhorar a cooperação futura. A fim de facilitar as consultas, o n.º 5 prevê igualmente que uma Parte requerente pode solicitar informação complementar a uma entidade. As entidades são incentivadas a explicar as razões para não divulgar os dados solicitados em resposta a esse pedido.

N.º 6

88. O n.º 6 exige que, no momento da assinatura do presente Protocolo ou aquando do depósito do seu instrumento de ratificação, aceitação ou aprovação, ou em qualquer outro momento, as Partes nomeiem uma autoridade para efeitos de consulta nos termos do n.º 5. A disponibilização de um ponto de contacto na Parte onde a entidade está localizada ajudará a Parte requerente a determinar rapidamente quais as medidas disponíveis para obter os dados solicitados, caso a entidade recuse a execução de um pedido direto apresentado ao abrigo do artigo 6.º.

N.º 7

89. O n.º 7 é autoexplicativo e prevê que o Secretário-Geral do Conselho da Europa estabeleça e mantenha um registo das autoridades designadas nos termos do n.º 6 e que cada Parte assegure em permanência a exatidão dos dados fornecidos para o registo.

Artigo 7.º – Divulgação de informação sobre subscritores

90. O artigo 7.º estabelece um procedimento que prevê a cooperação direta entre as autoridades de uma Parte e um fornecedor de serviços no território de outra Parte para obter informação sobre subscritores. O procedimento baseia-se nas conclusões do *Cloud Evidence Group* do T-CY e na nota de orientação sobre o artigo 18.º da Convenção, reconhecendo a importância de um acesso transfronteiras atempado a provas sob a forma eletrónica em investigações ou processos penais específicos, tendo em conta os desafios colocados pelos procedimentos existentes para a obtenção de provas sob a forma eletrónica junto de fornecedores de serviços de outros países.

91. Atualmente, um número crescente de investigações ou processos penais exige o acesso a provas sob a forma eletrónica por parte de fornecedores de serviços de outros países. Mesmo no caso de crimes de natureza exclusivamente nacional – ou seja, quando o crime, a vítima e o autor do crime se encontram todos no mesmo país da autoridade de investigação – as provas sob a forma eletrónica podem ser detidas por um fornecedor de serviços no território de outro

país. Em muitas situações, as autoridades que estão a investigar um crime podem ser obrigadas a recorrer a procedimentos de cooperação internacional, como a assistência mútua, que nem sempre são capazes de prestar assistência de forma rápida ou eficaz para as necessidades da investigação ou do processo devido ao aumento constante do volume de pedidos de obtenção de provas sob a forma eletrónica.

92. A informação de subscritores é a informação mais frequentemente procurada em investigações criminais relacionadas com o cibercrime e outros tipos de criminalidade para os quais são necessárias provas sob a forma eletrónica. Fornece a identidade de um determinado subscritor de um serviço, o seu endereço e informação semelhante identificada no artigo 18.º, n.º 3, da Convenção. Não permite tirar conclusões rigorosas sobre a vida privada e os hábitos diários das pessoas em causa, pelo que a sua divulgação pode ter um menor grau de intrusão por comparação com a divulgação de outras categorias de dados.

93. A informação dos subscritores é definida no artigo 18.º, n.º 3, da Convenção (incorporada no artigo 3.º, n.º 1, do presente Protocolo) como "quaisquer dados, apresentados sob a forma de dados informáticos ou sob qualquer outra forma, que sejam detidos por um fornecedor de serviços e que digam respeito a subscritores dos seus serviços, diferentes dos dados relativos ao tráfego ou ao conteúdo e que permitam determinar: a. o tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço; b. a identidade, a morada postal ou geográfica e o número de telefone do subscritor, e qualquer outro número de acesso, os dados respeitantes à faturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; c. qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços" (ver também os n.ºs 177 a 183 do relatório explicativo da Convenção). A informação necessária para efeitos de identificação de um subscritor de um serviço pode incluir determinada informação sobre o endereço IP (protocolo Internet) – por exemplo, o endereço IP utilizado no momento da criação de uma conta, o endereço IP mais recente ou o endereço IP de início de sessão utilizado num determinado momento. Em algumas Partes, esta informação é tratada como dados de tráfego por várias razões, incluindo o facto de se considerar que dizem respeito à transmissão de uma comunicação. Por conseguinte, o artigo 7.º, n.º 9, alínea b), prevê uma reserva para algumas Partes.

94. Embora o artigo 18.º da Convenção já aborde alguns aspetos da necessidade de um acesso rápido e eficaz às provas sob a forma eletrónica por parte dos fornecedores de serviços, não constitui, por si só, uma solução completa para este desafio, uma vez que este artigo se aplica a um conjunto mais limitado de circunstâncias. Especificamente, o artigo 18.º da Convenção aplica-se quando um fornecedor de serviços se encontra "no território" da Parte emissora (ver artigo 18.º, n.º 1, alínea a), da Convenção) ou "preste serviços" na Parte emissora (ver artigo 18.º, n.º 1, alínea b), da Convenção). Tendo em conta os limites do artigo 18.º e os desafios que se colocam à assistência mútua, considerou-se importante criar um mecanismo complementar que permitisse um acesso transfronteiras mais eficaz à informação necessária a investigações ou processos penais específicos. Igualmente, o âmbito de aplicação do artigo 7.º do presente Protocolo ultrapassa o âmbito de aplicação do artigo 18.º da Convenção ao permitir que uma Parte emita determinadas injunções a fornecedores de serviços no território de outra Parte. As Partes reconheceram que, embora tais injunções diretas das autoridades de uma Parte a fornecedores de serviços estabelecidos noutra Parte sejam desejáveis para um acesso rápido e efetivo à informação, uma Parte não deve ser autorizada a utilizar todos os mecanismos de execução disponíveis ao abrigo do seu direito interno para a execução dessas injunções. Por esse motivo, a execução destas injunções nos casos em que o fornecedor não divulgue a informação especificada sobre os subscritores está limitada da forma prevista no artigo 7.º, n.º 7. Este procedimento prevê salvaguardas para ter em conta os requisitos únicos decorrentes de uma cooperação direta entre as autoridades de uma Parte e os fornecedores de serviços estabelecidos noutra Parte.

95. Tal como refletido no artigo 5.º, n.º 7, o presente artigo não prejudica a capacidade de as Partes executarem injunções emitidas ao abrigo do artigo 18.º ou de outra forma permitidas pela Convenção, nem prejudica a cooperação (incluindo a cooperação espontânea) entre as Partes, ou entre as Partes e os fornecedores de serviços, através de outros acordos, convénios, práticas ou legislação nacional aplicáveis.

N.º 1

96. O n.º 1 exige que as Partes dotem as autoridades competentes dos poderes necessários para emitirem uma injunção a um fornecedor de serviços no território de outra Parte para obter a divulgação de informação sobre subscritores. A injunção só pode ser emitida para informação de subscritores especificada e armazenada.

97. O n.º 1 inclui igualmente o requisito de que as injunções só possam ser emitidas e apresentadas no contexto de "investigações ou processos penais específicos" da Parte emissora, tal como utilizado no artigo 2.º do presente Protocolo. Como outra limitação, as injunções podem também ser emitidas apenas para informação "necessária para" essa investigação ou processo. Para os países europeus, a informação é necessária – ou seja, necessária e proporcionada – para uma investigação ou um processo penal deve decorrer dos princípios da Convenção do Conselho da Europa de 1950 para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, da sua jurisprudência aplicável e da legislação e jurisprudência nacionais. Essas fontes determinam que o poder ou o procedimento devem ser proporcionais à natureza e às circunstâncias de uma infração (ver o n.º 146 do relatório explicativo da Convenção). As outras Partes aplicarão princípios conexos do seu direito, tais como princípios relevantes (ou seja, que os elementos de prova procurados por uma injunção devem ser relevantes para a investigação ou a ação penal) e que evitem injunções demasiado amplas de divulgação de informação de subscritores. Esta restrição reitera o princípio já estabelecido no artigo 2.º do presente Protocolo e no artigo 7.º, n.º 1, que limita a medida a investigações e processos penais específicos, segundo o qual as disposições não podem ser utilizadas para a produção de dados em massa ou em larga escala (ver também o n.º 182 do relatório explicativo da Convenção).

98. Tal como definido no artigo 3.º, n.º 2, alínea b), o termo "autoridade competente" refere-se a uma autoridade judicial, administrativa ou outra que zele pela aplicação da lei e que se encontre, ao abrigo do direito interno, investida dos poderes necessários para ordenar, autorizar ou executar as medidas nos termos deste Protocolo. A mesma abordagem está prevista para efeitos do procedimento de cooperação direta no presente artigo. Por conseguinte, a ordem jurídica interna de uma Parte regerá a autoridade que é considerada autoridade competente para emitir uma injunção. Embora a Parte emissora determine qual das suas autoridades pode emitir a injunção, o artigo 7.º prevê uma salvaguarda no n.º 5, segundo a qual a Parte recetora pode exigir que uma autoridade designada reveja as injunções emitidas ao abrigo do presente artigo e tenha capacidade para pôr termo à cooperação direta, tal como descrito mais abaixo.

99. No artigo 7.º, a expressão "um fornecedor de serviços no território de outra Parte" exige que o fornecedor de serviços esteja fisicamente presente na outra Parte. Nos termos deste artigo, o simples facto de, por exemplo, um fornecedor de serviços ter estabelecido uma relação contratual com uma empresa de uma Parte, mas o próprio fornecedor de serviços não estar fisicamente presente nessa Parte, não constitui um fornecedor de serviços "no território" dessa Parte. O n.º 1 requer, além disso, que os dados estejam na posse ou sob o controlo do fornecedor de serviços.

N.º 2

100. No artigo 7.º, n.º 2, as Partes devem adotar todas as medidas necessárias para que os fornecedores de serviços no seu território respondam a uma injunção emitida por uma autoridade competente de outra Parte nos termos do n.º 1. Considerando as diferenças entre os sistemas jurídicos nacionais, as Partes podem aplicar medidas diferentes para estabelecer um procedimento de cooperação direta com eficácia e eficiência. Tal pode ir da eliminação de obstáculos jurídicos para que os fornecedores de serviços respondam a uma injunção à disponibilização de uma base positiva, que obrigue os fornecedores de serviços a responder a uma injunção de uma autoridade de outra Parte de forma eficaz e eficiente. Cada Parte deve assegurar que os fornecedores de serviços possam cumprir legalmente as injunções previstas no artigo 7.º de um modo que garanta segurança jurídica, para que os fornecedores de serviços não incorram em responsabilidade jurídica pelo simples facto de terem cumprido de boa-fé uma injunção emitida nos termos do n.º 1, que uma Parte declarou (nos termos do artigo 7.º, n.º 3, alínea b)), emitida nos termos do presente Protocolo. Tal não exclui a responsabilidade por outros motivos que não o cumprimento da injunção, por exemplo, o incumprimento de qualquer requisito legal aplicável de que um fornecedor de serviços mantenha níveis apropriados de

segurança da informação armazenada. A forma de aplicação depende das considerações jurídicas e políticas das Partes. Para as Partes que têm requisitos em matéria de proteção de dados, tal incluirá o fornecimento de uma base clara para o tratamento de dados pessoais. Tendo em conta os requisitos adicionais ao abrigo da legislação em matéria de proteção de dados para autorizar eventuais transferências internacionais de informação de subscritores reativas, o presente Protocolo reflete o importante interesse público desta medida de cooperação direta e inclui as salvaguardas exigidas para esse efeito no artigo 14.º.

101. Conforme acima explicado, a ordem jurídica interna de uma Parte regerá a autoridade que é considerada autoridade competente para emitir uma injunção. Algumas Partes consideraram necessário dispor de uma salvaguarda adicional de uma nova avaliação da legalidade da injunção (ver, por exemplo, o n.º 98 acima) à luz do caráter direto da cooperação. Embora a Parte emissora determine qual das suas autoridades pode emitir a injunção, o n.º 2, alínea b), permite que as Partes façam uma declaração indicando que "a injunção a que se refere o artigo 7.º, n.º 1, tem de ser emitida por um procurador ou por outra autoridade judicial, ou sob a sua supervisão, ou ser emitida sob supervisão independente". Uma Parte que utilize a presente declaração tem de aceitar uma injunção emitida por ou sob a supervisão de qualquer uma dessas autoridades enumeradas.

N.º 3

102. O artigo 7.º, n.º 3, especifica a informação que, no mínimo, deve ser disponibilizada por uma autoridade que emita uma injunção nos termos do n.º 1 do presente artigo, embora uma Parte emissora possa optar por incluir informação adicional na própria injunção para auxiliar no tratamento ou porque o seu direito interno exige informação adicional. Nos termos do n.º 5, a informação especificada no n.º 3 é particularmente relevante para a aplicação da injunção pelo fornecedor de serviços, bem como para a eventual participação da autoridade da Parte na qual o fornecedor de serviços está localizado. A injunção deve incluir o nome da autoridade emissora e a data em que a injunção foi emitida, informação que identifique o fornecedor de serviços, a infração que é objeto da investigação ou do processo penal, a autoridade que solicita a informação do subscritor e uma descrição pormenorizada da informação específica solicitada sobre o subscritor. A injunção deve também incluir uma declaração de que a injunção foi emitida nos termos do presente Protocolo. Ao fazer esta declaração, a Parte indica que a injunção está em conformidade com as disposições do presente Protocolo.

103. No que diz respeito à diferença entre o n.º 3., alínea a) (a autoridade emissora) e o n.º 3, alínea e) (a autoridade que solicita a informação sobre o subscritor), em algumas Partes, a autoridade emissora e a autoridade que solicita os dados não são as mesmas. Por exemplo, os investigadores ou procuradores podem ser as autoridades que procuram os dados, ao passo que é um juiz quem emite a injunção. Em tais situações, tanto a autoridade que procura os dados como a autoridade que emite a decisão devem ser identificadas.

104. Não é necessária qualquer declaração dos factos, tendo em conta que esta informação é confidencial na maioria das investigações criminais e não pode ser divulgada a uma parte privada.

N.º 4

105. Embora o n.º 3 estabeleça a informação mínima exigida para as injunções emitidas nos termos do n.º 1, estas injunções só podem, com frequência, ser executadas se o fornecedor de serviços (e, se for caso disso, a autoridade designada da Parte recetora nos termos do n.º 5) receber informação suplementar. Por conseguinte, o artigo 7.º, n.º 4, especifica que a autoridade emissora deve fornecer informação suplementar sobre os fundamentos jurídicos nacionais que habilitam a autoridade a emitir a injunção; uma referência às disposições legais e às sanções aplicáveis à infração investigada ou objeto de ação penal; os dados de contacto da autoridade à qual o fornecedor de serviços deve devolver a informação sobre o subscritor, solicitar informação complementar ou responder de outra forma; o prazo e o modo como a informação sobre o subscritor deve ser devolvida; se já foi solicitada a preservação dos dados, incluindo a data de preservação e qualquer número de referência aplicável; quaisquer instruções processuais especiais (por exemplo, pedidos de confidencialidade ou autenticação); uma

declaração, se aplicável, de que foi efetuada uma notificação simultânea nos termos do n.º 5; e qualquer outra informação que possa ajudar a obter a divulgação da informação sobre o subscritor. Os dados de contacto não têm de identificar a pessoa, mas apenas o serviço. Esta informação suplementar pode ser fornecida separadamente, mas também pode ser incluída na própria injunção, se tal for permitido pela legislação da Parte emissora. Tanto a injunção como a informação suplementar devem ser transmitidas diretamente ao fornecedor de serviços.

106. As instruções processuais especiais abrangem, em especial, qualquer pedido de confidencialidade, incluindo um pedido de não divulgação da injunção ao subscritor ou a outros terceiros, exceto no caso de as instruções processuais especiais não poderem impedir o fornecedor de consultar as autoridades a notificar nos termos do n.º 5, alínea a) ou a consultá-las nos termos do n.º 5, alínea b). Se a confidencialidade for necessária para evitar uma divulgação prematura da questão, tal deve ser indicado no pedido. Em algumas Partes, a confidencialidade da injunção será mantida por força da lei, ao passo que noutras Partes tal não é necessariamente o caso. Por conseguinte, para evitar o risco de divulgação prematura da investigação, as Partes são incentivadas a tomar conhecimento da legislação aplicável e das políticas do fornecedor de serviços em matéria de notificação dos subscritores antes de apresentarem a injunção ao abrigo do n.º 1 ao fornecedor de serviços. Além disso, as instruções processuais especiais podem incluir a especificação do canal de transmissão mais adaptado às necessidades da autoridade. O fornecedor de serviços pode igualmente solicitar informação adicional sobre a conta ou outra informação para o ajudar a dar uma resposta rápida e completa. Um pedido de confidencialidade não deve impedir os fornecedores de serviços de comunicar informação sobre a transparência dos números agregados anonimizados de injunções recebidas ao abrigo do artigo 7.º.

N.º 5

107. Nos termos do n.º 5, alínea a), uma Parte pode notificar o Secretário-Geral do Conselho da Europa de que, quando for emitida uma injunção ao abrigo do n.º 1 a um fornecedor de serviços no seu território, será necessária uma notificação simultânea em todas as circunstâncias (ou seja, para todas as injunções transmitidas aos fornecedores de serviços no seu território) ou em circunstâncias identificadas.

108. Nos termos do n.º 5, alínea b), uma Parte pode igualmente, ao abrigo do seu direito interno, requerer a um fornecedor de serviços que receba uma injunção de outra Parte para o consultar em circunstâncias identificadas. Uma Parte não pode exigir a realização de consultas para todas as injunções, o que acrescentaria um passo adicional suscetível de provocar atrasos significativos, mas apenas em circunstâncias mais limitadas e identificadas. Os requisitos em matéria de consulta devem limitar-se às circunstâncias em que existe um potencial acrescido para a necessidade de impor uma condição ou de invocar um motivo de recusa, ou uma preocupação de potencial prejuízo para as investigações ou processos penais da Parte que procede à transferência.

109. Os procedimentos de notificação e consulta são totalmente discricionários. Uma Parte não é obrigada a exigir nenhum dos procedimentos.

110. As partes notificadas nos termos do n.º 5, alínea a) ou consultadas nos termos do n.º 5, alínea b), podem dar instruções a um fornecedor de serviços para que não divulgue informação pelos motivos previstos no n.º 5, alínea c), que são descritos de forma mais pormenorizada no n.º 141 do relatório explicativo sobre o artigo 8.º. Por conseguinte, a possibilidade de uma Parte ser notificada ou consultada constitui uma salvaguarda adicional. Posto isto, a cooperação deve, em princípio, ser extensa e os seus obstáculos estritamente limitados. Consequentemente, tal como explicado nos n.os 242 e 253 do relatório explicativo da Convenção, a determinação pela Parte notificada ou consultada sobre as condições e recusas aplicáveis nos termos do artigo 25.º, n.º 4, e do artigo 27.º, n.º 4, da Convenção deverá também ser limitada, em consonância com os objetivos do artigo 7.º do Protocolo, de eliminar os obstáculos e prever procedimentos mais eficientes e acelerados para o acesso transfronteiras a provas sob a forma eletrónica para investigações criminais.

111. Nos termos do n.º 5, alínea d), as Partes que façam uma declaração nos termos do n.º 5, alínea a), ou que exijam consultas nos termos do n.º 5, alínea b), podem contactar e solicitar informação

adicional à autoridade designada nos termos do n.º 4, alínea c) para determinar se existe uma base nos termos do n.º 5, alínea c), para dar instruções ao fornecedor de serviços no sentido de não dar cumprimento à injunção. Pretende-se que o processo seja tão rápido quanto as circunstâncias o permitam. A Parte notificada ou consultada deve recolher a informação necessária e proceder à sua determinação nos termos do n.º 5, alínea c), "sem demora indevida". Se necessário, para permitir a cooperação, o procedimento previsto no n.º 5.º, alínea d) pode também proporcionar a oportunidade de clarificar aspetos da confidencialidade da informação solicitada, bem como qualquer limitação da utilização prevista pela autoridade que solicita os dados.

Essa Parte deve também notificar prontamente a autoridade da Parte emissora caso decida dar instruções ao fornecedor de serviços para que não o cumpra, bem como indicar as razões para tal.

112. Uma Parte que exija notificação ou consulta pode decidir impor ao fornecedor um período de espera antes de o fornecedor disponibilizar a informação sobre o subscritor em resposta à injunção, de modo a permitir a notificação ou a consulta e qualquer pedido de informação complementar apresentado pela Parte.

113. Nos termos do n.º 5, alínea e), uma Parte que exija notificação ou consulta deve nomear uma única autoridade e, quando a notificação for exigida nos termos do n.º 5, alínea a), deve fornecer ao Secretário-Geral do Conselho da Europa as informação de contacto adequadas.

114. Uma Parte pode alterar a sua notificação ou o seu requisito de consulta a qualquer momento, em função da sua determinação de quaisquer fatores que lhe digam respeito, tais como, por exemplo, se pretende passar de um regime de notificação para um regime de consulta ou se desenvolveu um nível de confiança suficiente com a cooperação direta para poder rever ou suprimir um requisito anterior de notificação ou consulta. Pode igualmente decidir que, em resultado da experiência adquirida com o mecanismo de cooperação direta, pretende instituir um regime de notificação ou de consulta.

115. Nos termos do n.º 5, alínea f), o Secretário-Geral do Conselho da Europa deverá criar e manter atualizado um registo dos requisitos de notificação das Partes nos termos dos n.os 5, alínea a) e 5, alínea e). É fundamental ter um registo atualizado disponível ao público para garantir que as autoridades e os fornecedores de serviços da Parte emissora tenham conhecimento dos requisitos de notificação de cada Parte, que, tal como acima referido, pode ser alterado a qualquer momento. Uma vez que cada Parte pode proceder a essa alteração ao seu critério, cada Parte que introduza qualquer alteração ou constate qualquer inexatidão no que se refere aos seus dados no registo deve notificar imediatamente o Secretário-Geral, a fim de assegurar que outras Partes têm conhecimento dos requisitos em vigor e os podem aplicar corretamente.

N.º 6

116. O n.º 6 esclarece que é admissível notificar a outra Parte e fornecer informação adicional através de meios eletrónicos, incluindo a utilização de e-mail e portais eletrónicos. Se o fornecedor de serviços o aceitar, uma Parte pode apresentar uma injunção nos termos do n.º 1 e informação suplementar nos termos do n.º 4 em formato eletrónico. O objetivo é incentivar a utilização de meios eletrónicos se tal for aceitável para o fornecedor de serviços, uma vez que estes são quase sempre os meios de comunicação mais eficientes e mais rápidos. Os métodos de autenticação podem incluir uma variedade de meios ou uma combinação dos mesmos que permita uma identificação segura da autoridade requerente. Esses meios podem incluir, por exemplo, a obtenção de confirmação da autenticidade através de uma autoridade conhecida da Parte emissora (por exemplo, do remetente ou de uma autoridade central ou designada), comunicações subsequentes entre a autoridade emissora e a Parte recetora, a utilização de um endereço de e-mail oficial ou de futuros métodos de verificação tecnológica que possam ser facilmente utilizados pelas autoridades responsáveis pela transmissão. O artigo 10.º, n.º 2, contém um texto semelhante e o n.º 174 do relatório explicativo fornece mais orientações no que diz respeito ao requisito de segurança. O artigo 6.º, n.º 4, e o artigo 8.º, n.º 5, do Protocolo contêm igualmente um texto semelhante.

N.º 7

117. O n.º 7 estabelece que, se um fornecedor de serviços não cumprir uma injunção emitida nos termos do artigo 7.º, a Parte emissora só pode requerer a execução nos termos do artigo 8.º ou de outra forma de assistência mútua. As Partes que procedam nos termos do presente artigo não podem requerer a execução unilateral.

118. Para a execução da injunção através do artigo 8.º, o presente Protocolo prevê um procedimento simplificado de conversão de uma injunção ao abrigo do presente artigo numa injunção ao abrigo do artigo 8.º, com vista a facilitar a capacidade da Parte emissora para obter informação sobre os subscritores.

119. A fim de evitar a duplicação de esforços, a Parte emissora deve conceder ao fornecedor de serviços 30 dias ou o prazo estipulado no n.º 4, alínea d), consoante o que for mais longo, para que o processo de notificação e consulta ocorra e para que o fornecedor de serviços divulgue a informação ou indique uma recusa para o fazer. Uma Parte emissora só pode requerer a execução nos termos do artigo 8.º ou outras formas de assistência mútua após o termo desse prazo, ou se o fornecedor tiver indicado a sua recusa em cumprir antes do final desse prazo. Para permitir que as autoridades avaliem se pretendem aplicar a lei nos termos do n.º 7, os fornecedores de serviços são incentivados a explicar as razões para não fornecerem os dados solicitados. Por exemplo, um fornecedor de serviços pode explicar que os dados deixaram de estar disponíveis.

120. Se uma autoridade notificada nos termos do n.º 5, alínea a) ou consultada nos termos do n.º 5, alínea b), tiver informado a Parte emissora de que o fornecedor de serviços recebeu instruções no sentido de não divulgar a informação solicitada, a Parte emissora pode, no entanto, solicitar a execução da injunção através do artigo 8.º ou de outra forma de assistência mútua. No entanto, existe o risco de esse novo pedido ser igualmente indeferido. Aconselha-se a Parte emissora a consultar previamente uma autoridade designada nos termos dos n.ºs 5, alínea a) ou b), no sentido de corrigir eventuais deficiências da injunção inicial e evitar a apresentação de injunções ao abrigo do artigo 8.º ou através de qualquer outro mecanismo de assistência mútua que possa ser rejeitado.

N.º 8

121. Nos termos do n.º 8, uma Parte pode declarar que outra Parte deve solicitar ao fornecedor de serviços a divulgação de informação sobre subscritores antes de a solicitar ao abrigo do artigo 8.º, a menos que a Parte emissora apresente uma explicação razoável para não o ter feito. Por exemplo, uma Parte pode apresentar essa declaração por considerar que os procedimentos previstos no presente artigo devem permitir que as outras Partes obtenham os dados dos subscritores mais rapidamente do que nos termos do artigo 8.º, podendo, por conseguinte, reduzir o número de situações em que o artigo 8.º tem de ser invocado. Os procedimentos previstos no artigo 8.º só serão utilizados quando os esforços para obter a divulgação de informação de subscritores diretamente junto do fornecedor de serviços não forem bem-sucedidos, quando a Parte emissora tiver uma explicação razoável para não utilizar primeiro este artigo ou quando a Parte emissora se tiver reservado o direito de não aplicar o presente artigo. Por exemplo, uma Parte emissora pode demonstrar este facto quando um fornecedor de serviços não fornecer, habitualmente, informação sobre subscritores em resposta a injunções recebidas diretamente dessa Parte. Ou, como outro exemplo, se uma Parte emissora, através de uma única injunção, procurar obter informação sobre subscritores e dados de tráfego de outra Parte que aplique o artigo 8.º a ambas as categorias de dados, a Parte emissora não terá de procurar primeiro, em separado, a informação do subscritor.

N.º 9

122. Nos termos do n.º 9, alínea a), uma Parte que formule uma reserva ao presente artigo não é obrigada a tomar medidas ao abrigo do n.º 2 para que os fornecedores de serviços no seu território divulguem informação sobre subscritores em resposta a injunções emitidas por outras Partes. Uma Parte que formule uma reserva ao presente artigo não está autorizada a emitir

injunções ao abrigo do n.º 1 a fornecedores de serviços nos territórios de outras Partes.

123. O n.º 9, alínea b), prevê que – pelas razões explicadas no n.º 93 supra – se a divulgação de determinados tipos de números de acesso nos termos do presente artigo for incompatível com os princípios fundamentais do seu sistema jurídico interno, uma Parte pode reservar-se o direito de não aplicar o presente artigo a esses números. Uma Parte que formule tal reserva não está autorizada a emitir injunções para esses números ao abrigo do n.º 1 a fornecedores de serviços nos territórios de outras Partes.

Secção 3 – Procedimentos para reforçar a cooperação internacional entre autoridades para a divulgação de dados informáticos armazenados

Artigo 8.º – Execução de injunções de outra Parte para a apresentação expedita de informação sobre subscritores e dados de tráfego

124. O objetivo do artigo 8.º é permitir à Parte requerente emitir uma injunção a apresentar como parte de um pedido a outra Parte e à Parte requerida ter a possibilidade de dar cumprimento a essa injunção obrigando um fornecedor de serviços no seu território a fornecer informação sobre subscritores ou dados de tráfego na sua posse ou sob o seu controlo.

125. Este artigo estabelece um mecanismo que complementa as disposições da Convenção relativas à assistência mútua. Foi concebido para ser mais simplificado do que é a assistência mútua atualmente, na medida em que a informação que a Parte requerente deve fornecer é mais limitada e o processo de obtenção dos dados mais rápido. O presente artigo complementa e, por conseguinte, não prejudica outros processos de assistência mútua ao abrigo da Convenção ou de outros acordos multilaterais ou bilaterais, que uma Parte pode invocar. Com efeito, nas situações em que uma Parte requerente pretenda solicitar dados de tráfego a uma Parte que se tenha formulado uma reserva a esse aspeto do artigo 8.º, a Parte requerente pode recorrer a outro procedimento de assistência mútua. Quando, como acontece frequentemente, são procuradas simultaneamente informação sobre subscritores, dados de tráfego e dados de conteúdo armazenados, pode ser mais eficiente solicitar os três tipos de dados para a mesma conta através de um único pedido tradicional de assistência mútua do que solicitar, separadamente, alguns tipos de dados através do método previsto no presente artigo e outros através de um pedido de assistência mútua.

N.º 1

126. O n.º 1 exige que a Parte requerente possa emitir uma injunção para obter informação sobre subscritores ou dados de tráfego junto de um fornecedor de serviços no território da outra Parte. A "injunção" referida no artigo 8.º é qualquer processo jurídico destinado a obrigar um fornecedor de serviços a disponibilizar informação sobre os subscritores ou dados de tráfego. Por exemplo, pode ser executada através de uma ordem de produção, de uma citação ou de outro mecanismo legalmente autorizado e que pode ser emitido com o objetivo de obrigar à apresentação de informação sobre subscritores ou dados de tráfego.

127. Tal como definido no artigo 3.º, n.º 2, alínea b), "autoridade competente" no n.º 1 do presente artigo refere-se a "autoridade judicial, administrativa ou outra que zele pela aplicação da lei e que se encontre, ao abrigo do direito interno, investida dos poderes necessários para ordenar, autorizar ou executar as medidas nos termos deste Protocolo, cujo objeto seja a recolha ou a produção de provas relativamente a investigações ou processos penais específicos". Note-se que as autoridades competentes para emitir uma injunção nos termos do n.º 1 podem não ser necessariamente as mesmas que as autoridades designadas para apresentar a injunção a aplicar em conformidade com o artigo 8.º, n.º 10, alínea a), conforme descrito mais pormenorizadamente a seguir.

128. No artigo 8.º, a expressão "um fornecedor de serviços no território de outra Parte" exige que o fornecedor de serviços esteja fisicamente presente na outra Parte. Nos termos deste artigo, o simples facto de, por exemplo, um fornecedor de serviços ter estabelecido uma relação contratual com uma empresa de uma Parte, mas o próprio fornecedor de serviços não estar fisicamente presente nessa Parte, não constitui um fornecedor de serviços "no território" dessa

Parte. O n.º 1 requer, além disso, que os dados estejam na posse ou sob o controlo do fornecedor de serviços.

N.º 2

129. O n.º 2 exige que a Parte requerida adote as medidas necessárias para dar execução, no seu território, a uma injunção emitida nos termos do n.º 1, sob reserva das salvaguardas a seguir descritas. "Dar execução" significa que a Parte requerida obrigará o fornecedor de serviços a disponibilizar a informação sobre os subscritores e os dados de tráfego utilizando o mecanismo da escolha da Parte requerida, desde que o mecanismo torne a injunção executória nos termos da legislação interna da Parte requerida e cumpra os requisitos do presente artigo. Por exemplo, uma Parte requerida pode dar cumprimento a uma injunção de uma Parte requerente aceitando-a como equivalente às injunções internas, aprovando-a para a executar como uma injunção interna ou emitindo a sua própria ordem de produção. Qualquer mecanismo deste tipo estará sujeito aos termos da legislação da Parte requerida, uma vez que serão controlados pelos procedimentos da Parte requerida. Por conseguinte, a Parte requerida pode assegurar o cumprimento da sua própria legislação, incluindo os requisitos constitucionais e em matéria de direitos humanos, em especial no que se refere a quaisquer salvaguardas adicionais, incluindo as necessárias para a produção de dados de tráfego.

130. Embora o presente artigo possa ser cumprido de várias formas, uma Parte pode desejar conceber os seus próprios processos internos com flexibilidade para tratar os pedidos das diversas autoridades competentes. O n.º 3, alínea b), foi negociado para assegurar a disponibilização de informação suficiente à Parte requerida para que, se necessário, se possa proceder a um reavaliação completa, uma vez que algumas Partes indicaram que emitiriam a sua própria injunção como forma de dar cumprimento à injunção da Parte requerente.

N.º 3

131. Para dar início ao processo da Parte requerida para dar cumprimento à injunção, a Parte requerente transmite-a, bem como a informação de apoio. O n.º 3 descreve o que a Parte requerente deve fornecer à Parte requerida para que esta execute a injunção e exija a produção por um fornecedor de serviços no território dessa Parte. O n.º 3, alínea a) descreve a informação a incluir na própria injunção e inclui informação fundamental para a sua execução. A informação referida no n.º 3, alínea b), que se destina exclusivamente a ser utilizada pela Parte requerida e que não deve ser partilhada com o fornecedor de serviços, exceto com o consentimento da Parte requerente, constitui informação de apoio que estabelece os fundamentos jurídicos internos e a base internacional no presente Protocolo para a injunção, e fornece informação para que a Parte requerida avalie potenciais motivos para condições ou recusas ao abrigo do n.º 8. No momento em que apresentam um pedido nos termos do artigo 8.º, as partes devem indicar se existe informação ao abrigo do n.º 3, alínea b), que possa ser partilhada com o fornecedor de serviços. Nos termos do n.º 3, alínea c), o pedido deve também incluir todas as instruções especiais, incluindo, por exemplo, os pedidos de certificação ou de confidencialidade do pedido (à semelhança do artigo 27.º, n.º 8, da Convenção), no momento da transmissão, a fim de assegurar o tratamento adequado do pedido.

132. A injunção de informação sobre os subscritores ou os dados de tráfego descritos no n.º 3, alínea a), devem especificar: i) a autoridade que emitiu a injunção e a data em que a mesma foi emitida, ii) uma declaração de que está a ser emitida nos termos do presente Protocolo, iii) o nome e o endereço do(s) fornecedor(es) de serviços a notificar, iv) a(s) infração(ões) que é(são) objeto da investigação ou do processo penal, v) a autoridade que solicita os dados, se não for a autoridade emissora, e vi) uma descrição pormenorizada dos dados específicos solicitados (ou seja, a identidade do subscritor, o endereço postal ou geográfico, o número de telefone ou outro número de contacto e a informação sobre faturação e pagamento disponível com base no acordo ou disposição de serviço (ver artigo 3.º do presente Protocolo que incorpora o artigo 18.º, n.º 3, da Convenção e o n.º 93 do relatório explicativo acima); e em relação aos dados de tráfego, dados informáticos relativos a uma comunicação por meio de um sistema informático, gerados por um sistema informático que fazia parte da cadeia de comunicação, indicando a origem, o destino, o trajeto, a hora, a data, a dimensão, a duração ou o tipo de serviço subjacente à comunicação (ver artigo 3.º, n.º 1, do presente Protocolo que incorpora o artigo 1.º, alínea d), da Convenção). No que diz respeito ao n.º 3, alínea a), ponto v, se a autoridade emissora e a autoridade que

solicita os dados não forem as mesmas, a disposição exige que ambos sejam identificados. Por exemplo, uma autoridade responsável pela investigação ou ação penal pode estar a procurar os dados, enquanto um juiz emite a injunção. Esta informação demonstra a legitimidade da injunção e fornece instruções claras para a sua execução.

133. A informação de apoio descrita no n.º 3, alínea b), destina-se a fornecer à Parte requerida a informação necessária para dar cumprimento à injunção da Parte requerente. Tal poderá também ser facilitado por um modelo de preenchimento fácil, o que poderá aumentar ainda mais a eficiência do processo. Estão incluídos na lista de informação de apoio os seguintes elementos:

- O n.º 3, alínea b), ponto i, remete para a base jurídica que confere à autoridade emissora o poder de emitir a ordem de produção. Por outras palavras, é esta a lei pertinente que habilita uma autoridade competente a emitir a injunção descrita no n.º 1.

- O n.º 3, alínea b), ponto ii, refere-se à disposição jurídica relativa à infração referida na injunção no n.º 3,, alínea a), ponto iv, e ao conjunto de penas que lhe está associado. A inclusão destes dois elementos é importante para que a Parte requerida avalie se o pedido se enquadra ou não no âmbito das suas obrigações.

- O n.º 3, alínea b), ponto iii, refere-se a qualquer informação que a Parte requerente possa fornecer que a levou a concluir que o(s) fornecedor(es) de serviços objeto da injunção se encontra(m) na posse ou no controlo da informação ou dos dados solicitados. Esta informação é essencial para dar início ao processo na Parte requerida. A identificação do fornecedor de serviços nacional e a convicção de que possui ou controla a informação ou os dados solicitados é muitas vezes uma condição prévia para iniciar pedidos de ordens de produção.

- O n.º 3, alínea b), ponto iv, refere-se a uma síntese dos factos relacionados com a investigação ou o processo. Esta informação é também um fator fundamental para a Parte requerida determinar se uma injunção ao abrigo do presente artigo deve ou não ser executada no seu território.

- O n.º 3, alínea b), ponto v, refere-se a uma declaração relativa à pertinência da informação ou dos dados para a investigação ou processo. A presente declaração destina-se a ajudar a Parte requerida a decidir se foram ou não cumpridos os requisitos do n.º 1 do presente artigo, ou seja, que a informação ou os dados são “necessários para as investigações ou processos penais específicos da Parte”.

- O n.º 3, alínea b), ponto vi, refere-se aos dados de contacto de uma autoridade ou autoridades caso a autoridade competente da Parte requerida exija informação adicional para dar cumprimento à injunção.

- O n.º 3, alínea b), ponto vii, refere-se à informação sobre se a preservação da informação ou dos dados já foi solicitada. Trata-se de informação importante para a Parte requerida, especialmente em relação aos dados de tráfego, devendo incluir, por exemplo, os números de referência e a data de preservação, uma vez que essa informação pode permitir à Parte requerida estabelecer a correspondência entre o pedido atual e um pedido de preservação anterior e, por conseguinte, facilitar a divulgação da informação ou dos dados inicialmente preservados. Para reduzir o risco de a informação ou de os dados serem suprimidos, as Partes são incentivadas a procurar a preservação da informação ou dos dados solicitados o mais rapidamente possível e antes de dar início a um pedido ao abrigo do presente artigo, bem como a solicitar, atempadamente, a prorrogação das medidas de preservação.

- O n.º 3, alínea b), ponto viii, refere-se à informação sobre se os dados já foram solicitados por outros meios e, em caso afirmativo, de que forma. Esta disposição diz principalmente respeito ao facto de a Parte requerente já ter procurado informação sobre subscritores ou dados de tráfego diretamente junto do fornecedor de serviços.

134. A informação a fornecer nos termos do n.º 3, alínea b), não pode ser divulgada ao fornecedor de serviços sem o consentimento da Parte requerente. Em especial, o resumo dos factos e a declaração relativa à pertinência da informação ou dos dados para a investigação ou processo é fornecido à Parte requerida para determinar se existe um motivo para impor termos ou condições ou para recusar, mas está frequentemente sujeito ao sigilo da investigação.

135. Nos termos do n.º 3, alínea c), a Parte requerente pode solicitar instruções processuais especiais, incluindo pedidos de não divulgação da injunção ao subscritor ou formulários de autenticação a preencher para obter os elementos de prova. Esta informação terá de ser conhecida no início, uma vez que instruções especiais podem exigir procedimentos adicionais na Parte requerida.

136. Para executar a injunção e facilitar ainda mais a produção da informação ou dos dados, a Parte requerida pode disponibilizar ao fornecedor de serviços informação adicional, como o método de produção, e a quem os dados devem ser apresentados na Parte requerida.

N.º 4

137. Nos termos do n.º 4, pode ser necessário fornecer informação adicional à Parte requerida para que esta possa dar cumprimento à injunção. Por exemplo, ao abrigo da legislação interna de algumas Partes, a produção de dados de tráfego pode exigir mais informação, uma vez que a respetiva legislação prevê requisitos adicionais para a obtenção desses dados. Além disso, a Parte requerida pode solicitar esclarecimentos sobre a informação prestada nos termos do n.º 3, alínea b). Como outro exemplo, algumas Partes podem solicitar informação adicional se a injunção não tiver sido emitida ou revista por um procurador ou outra autoridade judicial ou administrativa independente da Parte requerente. Ao fazer essa declaração, as Partes deverão ser tão específicas quanto possível no que diz respeito ao tipo de informação complementar requerida.

N.º 5

138. O n.º 5 requer que a Parte requerida aceite os pedidos em formato eletrónico. podendo exigir a utilização de meios de comunicações eletrónicos seguros e autenticáveis para facilitar a transmissão de informação ou dados e documentos, incluindo a transmissão de injunções e informação de apoio. Os artigos 6.º a 11.º preveem igualmente esses meios de comunicação.

N.º 6

139. Nos termos do n.º 6, a Parte requerida deve tomar medidas razoáveis para dar rapidamente seguimento ao pedido. Envidará todos os esforços razoáveis para tratar os pedidos e solicitará a notificação do fornecedor de serviços no prazo de 45 dias a contar da receção pela Parte requerida de todos os documentos e informação necessários. A Parte requerida deve ordenar ao fornecedor de serviços que apresente a informação sobre os subscritores no prazo de 20 dias e os dados de tráfego no prazo de 45 dias. Embora a Parte requerida deva procurar obrigar a produção o mais rapidamente possível, existem muitos fatores que podem atrasar a produção, tais como fornecedores de serviços que levantem objeções, não respondam a pedidos ou não cumpram a data de retorno da produção, bem como o volume de pedidos que uma Parte requerida pode ser chamada a tratar. Por conseguinte, foi decidido exigir que as Partes requeridas envidassem esforços razoáveis para concluir apenas os processos sob o seu controlo.

N.º 7

140. As Partes reconheceram que algumas instruções processuais especiais da Parte requerente podem igualmente causar atrasos no tratamento das instruções, se as instruções exigirem procedimentos internos adicionais para dar cumprimento às instruções processuais especiais. A Parte requerida pode igualmente solicitar informação adicional à Parte requerente para apoiar quaisquer pedidos de injunções suplementares, tais como ordens de confidencialidade (ordens de não divulgação). Algumas instruções processuais podem não estar disponíveis ao abrigo da legislação da Parte requerida, caso em que o n.º 7 prevê que esta informe imediatamente a

Parte requerente e especifique as condições em que poderá cumprir, dando à Parte requerente a possibilidade de determinar se deseja ou não dar seguimento ao pedido.

N.º 8

141. Nos termos do n.º 8, a Parte requerida pode recusar a execução de um pedido se existirem os motivos de recusa previstos no artigo 27.º, n.º 4, ou do artigo 25.º, n.º 4, da Convenção. Por exemplo, em conformidade com o n.º 257 do relatório explicativo da Convenção, este prevê que esta disposição está sujeita aos motivos de recusa previstos nos tratados de assistência mútua e na legislação nacional aplicáveis e prevê "salvaguardas relativamente aos direitos de pessoas que se encontrem no território da Parte requerida" e, em conformidade com o n.º 268 do referido relatório explicativo, a assistência pode ser recusada com base "no prejuízo causado à soberania do Estado, à segurança, à *ordre public* ou a outros interesses essenciais". Pode igualmente impor condições necessárias para permitir a execução do pedido, tais como a confidencialidade. Além disso, a Parte requerida pode adiar a execução do pedido nos termos do artigo 27.º, n.º 5, da Convenção. A Parte requerida notifica a Parte requerente da sua decisão de recusar, condicionar ou adiar o pedido. Além disso, as Partes podem aplicar limites de utilização em conformidade com o disposto no artigo 28.º, n.º 2, alínea b), da Convenção.

142. Para promover o princípio de proporcionar uma cooperação tão ampla quanto possível (ver o artigo 5.º, n.º 1), os motivos de recusa estabelecidos por uma Parte requerida devem ser restritos e exercidos com contenção. De recordar que o n.º 253 do relatório explicativo da Convenção prevê que "a assistência mútua deverá, por princípio, ser alargada e as barreiras à mesma serem estritamente limitadas". Por conseguinte, as condições e recusas devem também ser limitadas, em consonância com os objetivos do presente artigo, de eliminar os obstáculos à partilha transfronteiras de informação sobre subscritores e de dados de tráfego e de proporcionar procedimentos mais eficientes e acelerados do que a assistência mútua tradicional.

N.º 9

143. Nos termos do n.º 9, alínea i) "se uma Parte requerente não puder cumprir uma condição imposta pela Parte requerida nos termos do n.º 8, informará imediatamente a Parte requerida desse facto. A Parte requerida determinará então se a informação ou o material deve, ainda assim, ser disponibilizado. …Se a Parte requerente aceitar esta condição, ficará vinculada pela mesma. A Parte requerida que fornece informação ou material sujeito a essa condição poderá exigir à Parte requerente que lhe forneça esclarecimentos relativos a essa condição, quanto à utilização dessa informação ou desse material".

N.º 10

144. O objetivo do n.º 10 é assegurar que as Partes, no momento da assinatura ou aquando do depósito dos seus instrumentos de ratificação, aceitação ou aprovação, identifiquem as autoridades que devem apresentar e receber instruções nos termos do artigo 8.º. As Partes não precisam de indicar o nome e o endereço de uma pessoa específica, mas podem identificar um escritório ou unidade que tenha sido considerado competente para enviar e receber injunções ao abrigo do presente artigo.

N.º 11

145. O n.º 11 permite que uma Parte declare que exige que as injunções que lhe sejam apresentadas ao abrigo do presente artigo sejam transmitidas pela autoridade central da Parte requerente ou por outra autoridade, se as Partes o determinarem mutuamente. As Partes são incentivadas a proporcionar a maior flexibilidade possível para a apresentação de pedidos.

N.º 12

146. O n.º 12 exige que o Secretário-Geral do Conselho da Europa crie e mantenha atualizado um registo das autoridades designadas pelas Partes nos termos do n.º 10 e que cada Parte assegure a exatidão dos seus dados constantes do registo. Essa informação ajudará as Partes requeridas a verificar a autenticidade dos pedidos.

N.º 13

147. Nos termos do n.º 13, uma Parte que se reserve o direito de não aplicar o presente artigo aos dados de tráfego não é obrigada a dar seguimento a injunções de dados de tráfego provenientes de outra Parte. Uma Parte que formule uma reserva para efeitos do presente artigo não está autorizada a apresentar injunções para dados de tráfego a outras Partes ao abrigo do n.º 1.

Artigo 9.º – Divulgação expedita de dados informáticos armazenados em caso de emergência

148. Para além das outras formas de cooperação rápida previstas no presente Protocolo, os redatores estavam conscientes da necessidade de facilitar às Partes, em caso de emergência, a possibilidade de obterem rapidamente dados informáticos específicos armazenados na posse ou sob o controlo de um fornecedor de serviços no território de outra Parte para serem utilizados em investigações ou processos penais específicos. Tal como referido nos pontos 42 e 172 do presente relatório explicativo, a necessidade de uma cooperação tão rápida quanto possível pode surgir numa série de situações de emergência, tais como no rescaldo imediato de um ataque terrorista, um ataque de *ransomware* que pode afetar um sistema hospitalar ou quando investigam contas de e-mail utilizadas por raptores para emitir pedidos de resgate e comunicar com a família da vítima.

149. Nos termos da Convenção, em caso de emergência, as Partes apresentam pedidos de assistência mútua para a obtenção de dados e, nos termos do artigo 35.º, n.º 1, alínea c), da Convenção, a rede 24/7 está disponível para facilitar a execução desses pedidos. Além disso, os sistemas jurídicos de alguns países permitem que as autoridades competentes de outros países procurem a divulgação de dados de emergência através da rede 24/7 sem enviar um pedido de assistência mútua.

150. Tal como refletido no artigo 5.º, n.º 7, o presente artigo não prejudica a cooperação (incluindo a cooperação espontânea) entre as Partes, ou entre as Partes e os fornecedores de serviços, através de outros acordos, convénios, práticas ou legislação nacional aplicáveis. Por conseguinte, ao abrigo do presente Protocolo, todos os mecanismos acima referidos continuam à disposição das autoridades competentes que procuram dados em situações de emergência. A inovação do presente Protocolo consiste na elaboração de dois artigos que obrigam todas as Partes a proporcionar, no mínimo, canais específicos para uma cooperação rápida em situações de emergência: artigo 9.º e artigo 10.º.

151. Este artigo permite que as Partes cooperem na obtenção de dados informáticos em situações de emergência, utilizando como canal a rede 24/7, criada pelo artigo 35.º da Convenção. A rede 24/7 é particularmente adequada para tratar os pedidos sensíveis ao fator tempo e de elevada prioridade previstos neste artigo. A rede 24/7 dispõe de pontos de contacto que, na prática, comunicam rapidamente e sem necessidade de traduções escritas e estão em condições de dar resposta a pedidos recebidos de outras Partes, quer se dirijam diretamente a fornecedores no seu território, solicitando assistência a outras autoridades competentes ou recorrendo a autoridades judiciais, caso tal seja exigido pela legislação interna da Parte. Estes pontos de contacto podem igualmente aconselhar as Partes requerentes sobre questões que possam ter em relação aos fornecedores e à recolha de provas sob a forma eletrónica, por exemplo, explicando o direito interno que deve ser satisfeito para obter os elementos de prova. Essa comunicação retroativa reforça a compreensão, por parte da Parte requerente, do direito interno da Parte requerida e facilita a obtenção mais fácil dos elementos de prova necessários.

152. A utilização do canal estabelecido no presente artigo pode ter vantagens em relação ao canal de assistência mútua de emergência previsto no artigo 10.º. Por exemplo, este canal tem a vantagem de não ser necessário preparar previamente qualquer pedido de assistência mútua. Poderá ser necessário algum tempo para preparar um pedido prévio de assistência mútua, para o traduzir e transmitir através dos canais nacionais à autoridade central da Parte requerente para efeitos de assistência mútua, o que não seria exigido nos termos do artigo 9.º. Além disso, uma vez recebido o pedido, se a Parte requerida tiver de obter informação suplementar antes de poder conceder assistência, o tempo adicional que pode ser necessário para um pedido de

assistência mútua é mais suscetível de atrasar a execução do pedido. No contexto da assistência mútua, as Partes requeridas exigem frequentemente que a informação suplementar seja fornecida por escrito e de forma mais pormenorizada, ao passo que o canal da rede 24/7 funciona através do intercâmbio de informação em tempo real. Por outro lado, o canal de assistência mútua de emergência oferece vantagens em determinadas situações. Por exemplo: i) a utilização deste canal envolve uma perda de tempo diminuta ou nenhuma se existirem relações de trabalho particularmente estreitas entre as autoridades centrais em causa, ii) a assistência mútua de emergência pode ser utilizada para obter formas de cooperação adicionais para além dos dados informáticos na posse dos fornecedores, e iii) pode ser mais fácil autenticar as provas obtidas através da assistência mútua. Cabe às Partes, com base na sua experiência acumulada e nas circunstâncias jurídicas e factuais específicas em questão, decidir qual é a melhor via a utilizar num caso específico.

N.º 1

153. Nos termos do n.º 1, alínea a), cada Parte deve adotar as medidas necessárias para assegurar que o seu ponto de contacto para a rede 24/7 possa transmitir pedidos de emergência ao ponto de contacto de outra Parte, solicitando assistência imediata para obter a divulgação expedita de dados informáticos especificados e armazenados na posse de fornecedores no território dessa Parte e receber pedidos de pontos de contacto de outras Partes relativos a esses dados na posse de fornecedores no seu território. Tal como previsto no artigo 2.º, o pedido deve ser apresentado no âmbito de uma investigação ou processo penal específico.

154. Os pontos de contacto da rede 24/7 devem ter a possibilidade de transmitir e receber esses pedidos em caso de urgência, sem que seja necessário preparar e transmitir previamente um pedido de assistência mútua, tal como descrito no n.º 152 do relatório explicativo supra, sob reserva da possibilidade de declaração nos termos do artigo 9.º, n.º 5. O termo "emergência" é definido no artigo 3.º. Nos termos do artigo 9.º, a Parte requerida deve determinar se existe uma "emergência" em relação a um pedido utilizando a informação prevista no n.º 3.

155. Contrariamente a outros artigos do presente Protocolo, como o artigo 7.º, que só podem ser utilizados para obter "informação específica e armazenada sobre subscritores", este artigo utiliza o termo mais abrangente "dados informáticos especificados e armazenados". O âmbito de aplicação deste termo é amplo, mas não indiscriminado: abrange quaisquer dados informáticos "especificados", tal como definida no artigo 1.º, alínea b), da Convenção, que está incorporada no artigo 3.º do presente Protocolo. A utilização deste termo mais amplo reconhece a importância de obter conteúdos armazenados e dados de tráfego, e não apenas informação sobre subscritores, em situações de emergência, sem exigir a apresentação de um pedido de assistência mútua como condição prévia. Trata-se, pois, de dados existentes ou dados armazenados, não incluindo assim os dados ainda não existentes tais como os dados de tráfego ou de conteúdo relacionados com comunicações futuras (ver o n.º 170 do relatório explicativo da Convenção).

156. Esta disposição proporciona flexibilidade à Parte requerente para determinar qual das suas autoridades deve dar início ao pedido, tal como as suas autoridades competentes que estão a conduzir a investigação ou o seu ponto de contacto da rede 24/7, em conformidade com o direito interno. O ponto de contacto da rede 24/7 na Parte requerente funciona então como canal para transmitir o pedido ao ponto de contacto da rede 24/7 na outra Parte.

157. Nos termos do n.º 1, alínea b), uma Parte pode declarar que não executará um pedido ao abrigo do artigo 9.º apenas relativo a informação sobre subscritores, tal como definido no artigo 18.º, n.º 3, da Convenção, incorporado no artigo 3.º, n.º 1, do presente Protocolo. Para algumas Partes, a receção de pedidos ao abrigo do presente artigo apenas relativo a informação de subscritores correria o risco de sobrecarregar os pontos de contacto da rede 24/7 ao desviar recursos e energia dos pedidos de dados de conteúdo ou de tráfego. Nesses casos, as Partes que solicitem apenas informação sobre subscritores podem, em vez disso, utilizar os artigos 7.º ou 8.º, que facilitam a rapidez da divulgação de tal informação. Essa declaração não proíbe as outras Partes de incluírem um pedido de informação sobre subscritores quando também emitem um pedido ao abrigo do presente artigo para dados de conteúdo e/ou de tráfego.

N.º 2

158. O n.º 2 exige que cada Parte adote as medidas necessárias para assegurar que as suas autoridades possam, ao abrigo do seu direito interno, procurar e obter os dados solicitados nos termos do n.º 1 junto de fornecedores de serviços no seu território e responder a esses pedidos sem que a Parte requerente tenha de apresentar um pedido de assistência mútua, sob reserva da possibilidade de apresentar uma declaração em conformidade com o n.º 5.

159. Dada a diferença entre as legislações internas, o n.º 2 destina-se a proporcionar flexibilidade às Partes na conceção dos seus sistemas de resposta aos pedidos ao abrigo do n.º 1. No entanto, as Partes são incentivadas a desenvolver mecanismos para dar cumprimento a este artigo que coloquem a tónica na rapidez e eficiência, que sejam adaptados às necessidades de uma situação de emergência e que proporcionem uma ampla base jurídica para a divulgação de dados a outras Partes em situações de emergência.

160. Cabe à Parte requerida determinar: i) se os requisitos para a utilização do presente artigo foram cumpridos, ii) se outro mecanismo é adequado para efeitos de assistência à Parte requerente, iii) a autoridade competente para executar um pedido recebido pelo ponto de contacto da rede 24/7. Embora o ponto de contacto da rede 24/7 em algumas Partes possa já dispor da autoridade necessária para executar ele próprio o pedido, outras Partes podem exigir que o seu ponto de contacto transmita o pedido a outra autoridade ou autoridades para solicitar a divulgação dos dados junto do fornecedor. Em algumas Partes, tal pode requerer a obtenção de uma ordem judicial para solicitar a divulgação de dados. A Parte requerida também pode determinar o canal de transmissão dos dados de resposta à Parte requerente – quer através do ponto de contacto da rede 24/7, quer através de outra autoridade.

N.º 3

161. O n.º 3 especifica a informação a fornecer num pedido apresentado nos termos do n.º 1. A informação especificada no n.º 3 deve facilitar a avaliação e, se for caso disso, a execução do pedido pela autoridade competente da Parte requerida.

162. No que diz respeito ao n.º 3, alínea a), a Parte requerente deve especificar a autoridade competente em nome da qual os dados são solicitados.

163. No que diz respeito ao n.º 3, alínea b), a Parte requerente deve declarar que o pedido é emitido nos termos do presente Protocolo. Deste modo, garante-se que o pedido é apresentado em conformidade com o presente Protocolo e que quaisquer dados recebidos em consequência serão tratados em conformidade com os requisitos do presente Protocolo. Tal fará também uma distinção entre o pedido e outros pedidos de divulgação de emergência que o ponto de contacto da rede 24/7 possa receber.

164. Nos termos do n.º 3, alínea e), a Parte requerente deve fornecer factos suficientes que demonstrem a existência de uma emergência, tal como definida no artigo 3.º, e a forma como os dados solicitados se relacionam com essa emergência. Se a Parte requerida solicitar esclarecimentos sobre o pedido ou requerer informação adicional para dar seguimento ao pedido, deve consultar o ponto de contacto da rede 24/7 da Parte requerente.

165. Nos termos do n.º 3, alínea g), o pedido deve especificar quaisquer instruções processuais especiais. Estas incluem, em especial, pedidos de não divulgação do pedido a subscritores e outros terceiros ou formulários de autenticação a preencher para os dados solicitados. Nos termos do presente número, estas instruções processuais são fornecidas no início, uma vez que instruções especiais podem exigir procedimentos adicionais na Parte requerida. Em algumas Partes, a confidencialidade poderá ser mantida por força da lei, ao passo que noutras Partes tal não é necessariamente o caso. Por conseguinte, para evitar o risco de divulgação prematura da investigação, as Partes são incentivadas a comunicar a necessidade e quaisquer dificuldades que possam surgir para manter a confidencialidade, incluindo a legislação aplicável, bem como as políticas do fornecedor de serviços em matéria de notificação. Uma vez que os pedidos de autenticação dos dados de resposta podem, com frequência, atrasar o objetivo fundamental de uma rápida divulgação dos dados solicitados, as autoridades da Parte requerida devem, em

consulta com as autoridades da Parte requerente, determinar quando e de que forma deve ser fornecida a confirmação da autenticidade.

166. Além disso, a Parte ou o fornecedor de serviços pode solicitar informação adicional para localizar e divulgar os dados informáticos armazenados solicitados pela Parte requerente.

N.º 4

167. O n.º 4 requer que a Parte requerida aceite os pedidos em formato eletrónico. As partes são incentivadas a utilizar meios de comunicação rápidos para facilitar a transmissão de informação, dados e documentos, incluindo a transmissão de pedidos. Este número baseia-se no artigo 8.º, n.º 5, mas foi alterado para acrescentar que uma Parte pode aceitar pedidos oralmente, um método de comunicação frequentemente utilizado pela rede 24/7.

N.º 5

168. O n.º 5 permite que uma Parte faça uma declaração em como exige que as outras Partes que lhe solicitem dados nos termos do presente artigo forneçam, na sequência da execução do pedido e da transmissão dos dados, o pedido e qualquer informação suplementar transmitida em seu apoio, num formato específico e através de um canal específico. Por exemplo, uma Parte pode declarar que, em circunstâncias específicas, exigirá que uma Parte requerente apresente um pedido subsequente de assistência mútua para documentar formalmente o pedido de emergência e a decisão prévia de fornecer dados em resposta a esse pedido. No caso de algumas Partes, tal procedimento será exigido pelo seu direito interno, ao passo que outras Partes indicaram que não dispõem de tais requisitos e não necessitam de recorrer a esta possibilidade de declaração.

N.º 6

169. Este artigo refere-se a "pedidos" e não exige que as Partes requeridas forneçam os dados solicitados às Partes requerentes. Por conseguinte, os redatores reconhecem que haverá situações em que as Partes requeridas não fornecerão os dados solicitados a uma Parte requerente ao abrigo do presente artigo. A Parte requerida pode determinar que, num caso específico, a assistência mútua de emergência ao abrigo do artigo 10.º ou outros meios de cooperação serão os mais apropriados. Consequentemente, o n.º 6 prevê que, sempre que uma Parte requerida determine que não fornecerá os dados solicitados a uma Parte que tenha apresentado um pedido nos termos do n.º 1 do presente artigo, a Parte requerida informa a Parte requerente da sua decisão numa base expedita e, se for caso disso, especifica as condições em que fornece os dados e explica quaisquer outras formas de cooperação que possam estar disponíveis, a fim de alcançar o objetivo mútuo das Partes de acelerar a divulgação de dados em situações de emergência.

N.º 7

170. O n.º 7 descreve os procedimentos aplicáveis quando o Estado requerido tiver especificado condições para a concessão da cooperação ao abrigo do n.º 6. Nos termos do n.º 7, alínea a), se a Parte requerente não puder cumprir determinadas condições, deve comunicar imediatamente esse facto à Parte requerida e a Parte requerida deve então determinar se a assistência ainda pode ser concedida. Em contrapartida, quando a Parte requerente aceitar uma condição específica, ficará vinculada pela mesma. Nos termos do n.º 7, alínea b), uma Parte requerida que tenha fornecido informação ou materiais sujeitos a uma das condições previstas no n.º 6 pode, a fim de verificar se essa condição foi cumprida, exigir que a Parte requerente explique a utilização que fez da informação ou materiais fornecidos, mas foi entendido que a Parte requerente não pode exigir uma prestação de contas demasiado onerosa (ver n.os 279 e 280 do relatório explicativo da Convenção).

Secção 4 – Procedimentos relativos à assistência mútua de emergência

Artigo 10.º – Assistência mútua de emergência

171. O artigo 10.º do presente Protocolo destina-se a prever um procedimento o mais expedito possível para os pedidos de assistência mútua apresentados em situações de emergência. Uma emergência é definida no artigo 3.º, n.º 2, alínea c), e explicada nos n.os 41 e 42 do presente relatório explicativo.

172. Uma vez que o artigo 10.º do presente Protocolo se limita às situações de emergência que justificam uma ação expedita, é distinto do artigo 25.º, n.º 3, da Convenção, no qual os pedidos de assistência mútua podem ser apresentados por meios de comunicação expeditos em circunstâncias urgentes que não atinjam o nível de emergência definido. Por outras palavras, o artigo 25.º, n.º 3, tem um âmbito de aplicação mais amplo do que o artigo 10.º do presente Protocolo, na medida em que abrange situações não abrangidas pelo artigo 10.º, tais como os riscos atuais mas não iminentes para a vida ou a segurança das pessoas, a potencial destruição de provas que possam resultar de atrasos, uma aproximação rápida da data do julgamento ou de outros tipos de emergências. Embora o mecanismo previsto no artigo 25.º, n.º 3, preveja um método mais rápido de transmissão e resposta a um pedido, as obrigações em caso de emergência nos termos do artigo 10.º do presente Protocolo são significativamente superiores; ou seja, quando existe um risco significativo e iminente para a vida ou a segurança de uma pessoa singular, o processo deve ser ainda mais acelerado (ver o n.º 42 do presente relatório explicativo para exemplos de situações de emergência).

N.º 1

173. Nos termos do n.º 1, ao apresentar um pedido de emergência, a Parte requerente deve concluir pela existência de uma situação de emergência na aceção do artigo 3.º, n.º 2, alínea c), e incluir no seu pedido uma descrição dos factos que o demonstrem, explicando a forma como a assistência solicitada é necessária para dar resposta à emergência, para além de outra informação que deve constar do pedido nos termos do tratado ou da legislação interna aplicável da Parte requerida. A este respeito, importa recordar que, nos termos do artigo 25.º, n.º 4, da Convenção, a execução dos pedidos de assistência mútua "será sujeita às condições fixadas pelo direito interno da Parte requerida ou pelos tratados de auxílio mútuo aplicáveis, incluindo os fundamentos com base nos quais a Parte requerida pode recusar a cooperação". Os redatores entenderam que tal se aplica também aos pedidos de assistência mútua de emergência ao abrigo do presente Protocolo.

N.º 2

174. O n.º 2 exige que a Parte requerida aceite o pedido de assistência mútua em formato eletrónico. Antes de aceitar o pedido, a Parte requerida pode subordinar a aceitação do pedido ao cumprimento, pela Parte requerente, dos níveis apropriados de segurança e autenticação. No que diz respeito ao requisito de segurança citado no presente número, as Partes poderão decidir, entre si, a necessidade de proteções especiais de segurança (incluindo a encriptação) relativamente a casos particularmente delicados.

N.º 3

175. Sempre que a Parte requerida solicitar informação adicional para concluir que existe uma situação de emergência na aceção do artigo 3.º, n.º 2, alínea c), e/ou que os outros requisitos de assistência mútua foram cumpridos, é obrigada, nos termos do n.º 3, a solicitar essa informação adicional de forma expedita. Do mesmo modo, o n.º 3 exige que a Parte requerente forneça a informação suplementar de forma igualmente expedita. Por conseguinte, ambas as Partes devem envidar todos os esforços para evitar perdas de tempo que possam contribuir inadvertidamente para um resultado trágico.

N.º 4

176. Nos termos do n.º 4, logo que tenha sido fornecida a informação necessária que permita a execução do pedido, a Parte requerida deve responder ao pedido com a mesma celeridade. Tal significa, em geral, acelerar rapidamente a obtenção de injunções judiciais que obriguem um fornecedor a apresentar dados que constituam prova da infração e a notificação igualmente rápida da decisão ao fornecedor. No entanto, os atrasos ocasionados pelos prazos de resposta do fornecedor a tais injunções não devem ser atribuídos às autoridades da Parte requerida.

N.º 5

177. Nos termos do n.º 5, todas as Partes asseguram que os membros da sua autoridade central ou outras autoridades responsáveis pela resposta aos pedidos de assistência mútua estejam disponíveis vinte e quatro horas por dia, sete dias por semana, caso os pedidos de assistência mútua de emergência tenham de ser apresentados fora das horas normais de expediente. A este respeito importa recordar que, nos termos do artigo 35.º da Convenção, a rede 24/7 está disponível para coordenação com as autoridades responsáveis pela assistência mútua. A obrigação prevista no presente número não exige que a autoridade central ou outras autoridades responsáveis pela resposta aos pedidos de assistência mútua estejam sempre dotadas de pessoal e operacionais. Pelo contrário, essa autoridade deve implementar procedimentos para assegurar que o pessoal possa ser contactado a fim de analisar os pedidos de emergência fora das horas normais de expediente. O T-CY esforçar-se-á informalmente por manter um diretório dessas autoridades.

N.º 6

178. O n.º 6 constitui uma base para as autoridades centrais ou outras autoridades responsáveis pela assistência mútua determinarem mutuamente um canal alternativo para a transmissão da informação ou dos elementos de prova de resposta, seja o modo de transmissão ou as autoridades entre as quais são transmitidos. Assim, em vez de a informação ou elementos de prova de resposta serem devolvidos através do canal da autoridade central habitualmente utilizado para transmitir informação ou elementos de prova fornecidos na execução do pedido da Parte requerente, podem decidir mutuamente utilizar um canal diferente para acelerar a transmissão, manter a integridade dos elementos de prova ou por qualquer outro motivo. Por exemplo, numa situação de emergência, as autoridades podem decidir transmitir os elementos de prova diretamente a uma autoridade responsável pela investigação ou ação penal na Parte requerente que os utilizará e não através da cadeia de autoridades através das quais esses elementos de prova normalmente seriam transmitidos. As autoridades podem igualmente decidir, por exemplo, sobre o tratamento especial das provas físicas para poderem excluir a possibilidade de as provas terem sido alteradas ou contaminadas em processos judiciais subsequentes, ou podem decidir mutuamente o tratamento especial da transmissão de provas sensíveis.

N.º 7

179. No que diz respeito aos procedimentos que regem este artigo, existem duas possibilidades, tal como descrito nos n.os 7 e 8. O artigo 10.º, n.º 7, prevê que, quando as Partes em causa não estiverem mutuamente vinculadas por um acordo ou convénio de assistência mútua aplicável com base numa legislação uniforme ou recíproca, as Partes aplicam determinados procedimentos previstos nos artigos 27.º e 28.º da Convenção (que regem a assistência mútua na ausência de um tratado).

N.º 8

180. O n.º 8 prevê que, quando as Partes em causa estiverem mutuamente vinculadas por esse acordo ou convénio, o artigo 10.º é complementado pelas disposições desse acordo ou convénio, salvo se as Partes em causa decidirem mutuamente aplicar, em vez delas, uma ou todas as disposições da Convenção referida no n.º 7.

N.º 9

181. Por último, o n.º 9 prevê a possibilidade de uma declaração através da qual as Partes no presente Protocolo possam prever a apresentação de pedidos diretamente entre procuradores ou outras autoridades judiciais. Em algumas Partes, essa autoridade judicial direta para os canais das autoridades judiciais está bem estabelecida e pode constituir um meio eficaz para acelerar ainda mais a apresentação e a execução dos pedidos. A transmissão do pedido de emergência através do ponto de contacto da rede 24/7 da Parte ou através da Organização Internacional de Polícia Criminal (INTERPOL) é útil não só para reduzir qualquer atraso, mas também para aumentar as normas de segurança e autenticação. No entanto, em algumas Partes, o envio de um pedido diretamente a uma autoridade judicial da Parte requerida sem o envolvimento e a aprovação da sua autoridade central pode ser contraproducente, na medida em que, sem orientação e/ou aprovação da sua autoridade central, a autoridade recetora pode não estar habilitada a agir de forma independente ou pode não estar familiarizada com o procedimento adequado. Por conseguinte, uma Parte deve declarar que os pedidos podem ser enviados através destes canais da autoridade não central.

Secção 5.º – Procedimentos relativos aos pedidos de assistência mútua na ausência de acordos internacionais aplicáveis

182. Tal como estabelecido no artigo 5.º, n.º 5, a presente secção, relativa aos artigos 11.º e 12.º, aplica-se "em caso de inexistência de quaisquer tratados de assistência mútua ou acordos celebrados com base numa legislação uniforme ou recíproca, entre as Partes requerente e requerida. As disposições da secção 5 não serão aplicáveis caso exista tal tratado ou acordo, exceto nos casos previstos no artigo 12.º, n.º 7. No entanto, as Partes em questão podem decidir mutuamente aplicar, em sua substituição, as disposições da secção 5, se o tratado ou o acordo não o proibir". Isto segue a abordagem do artigo 27.º da Convenção.

183. Entre algumas Partes no presente Protocolo, as matérias abrangidas pelos artigos 11.º e 12.º já são reguladas pelos termos dos tratados de assistência mútua (por exemplo, o Segundo Protocolo Adicional à Convenção Europeia sobre Assistência Mútua em Matéria Penal (STCE n.º 182) ou o Acordo entre a União Europeia e os Estados Unidos da América sobre Assistência Jurídica Mútua). Os tratados de assistência mútua, como o STCE n.º 182, podem também fornecer mais pormenores sobre as circunstâncias, as condições e os procedimentos em que essa cooperação se pode verificar.

184. Embora os redatores tenham considerado estes tratados, os artigos 11.º e 12.º do presente Protocolo contêm termos que diferem de disposições análogas de outros tratados de assistência mútua.

185. Embora os termos do STCE n.º 182 continuem a ser aplicados entre as Partes, considerou-se adequado regulamentar estes dois artigos do presente Protocolo de uma forma que difere em alguns aspetos pelas seguintes razões:

- A adesão ao STCE n.º 182 é diferente da Convenção sobre o Cibercrime, pelo que as suas disposições não estão disponíveis para cooperação entre todas as Partes na Convenção sobre o Cibercrime. O STCE n.º 182 foi negociado para satisfazer as necessidades dos Estados-Membros do Conselho da Europa e não os requisitos, sistemas e necessidades legais de todas as Partes na Convenção sobre o Cibercrime, embora, em princípio, a Convenção Europeia sobre Assistência Mútua em Matéria Penal (STCE n.º 30) e os seus protocolos estejam abertos à adesão de Estados não membros do Conselho da Europa, na sequência de um convite do Comité de Ministros.

- As disposições do presente Protocolo relativas à assistência mútua têm um âmbito de aplicação material específico, na medida em que se aplicam a "investigações ou processos penais específicos relativos a infrações penais relacionadas com sistemas e dados informáticos e com a recolha de provas sob a forma eletrónica de uma infração penal" (artigo 2.º) Tendo em conta os problemas específicos deste tipo de investigação ou processo – como a volatilidade dos dados, questões relacionadas com a territorialidade e a jurisdição, bem como com o volume de pedidos – as disposições análogas do STCE n.º 182 podem nem

sempre ser aplicáveis da mesma forma.

- Os redatores reconheceram que "dado que a Convenção se aplica a Partes que apresentam um vasto leque de culturas e sistemas jurídicos diversos, não é possível especificar detalhadamente as condições e salvaguardas aplicáveis a cada poder ou procedimento" (ver o n.º 145 do relatório explicativo da Convenção). Em vez disso, as Partes devem assegurar a "proteção adequada dos direitos humanos e das liberdades" e aplicar "normas comuns [e] salvaguardas mínimas, às quais as Partes... deverão aderir", incluindo "salvaguardas decorrentes das obrigações assumidas por uma Parte ao abrigo dos instrumentos internacionais aplicáveis, relativos aos direitos do Homem" (ver o n.º 145 do relatório explicativo da Convenção). Ver o artigo 13.º do presente Protocolo (que incorpora o artigo 15.º da Convenção). Por conseguinte, contrariamente às disposições do STCE n.º 182 – por exemplo, o artigo 9.º relativo à "audição por videoconferência" – que estabelece procedimentos e salvaguardas específicos a seguir pelas Partes no STCE n.º 182, as disposições correspondentes do presente Protocolo permitem uma maior flexibilidade na aplicação pelas Partes. Por exemplo, os procedimentos e as condições que regem o funcionamento das equipas de investigação conjuntas são os acordados entre as autoridades competentes das Partes (ver artigo 12.º, n.º 2) e, no que diz respeito a videoconferência, uma Parte requerida pode exigir condições e salvaguardas especiais ao permitir a audição de um suspeito ou acusado por videoconferência (ver artigo 11.º, n.º 8). Na medida prevista nesses artigos, as Partes podem igualmente decidir não cooperar se os seus requisitos em termos de condições e salvaguardas não forem cumpridos.

186. Os artigos 11.º e 12.º do presente Protocolo só são aplicáveis na ausência de outros tratados ou acordos de assistência mútua com base em legislação uniforme ou recíproca – salvo se as Partes em causa decidirem mutuamente aplicar uma ou todas as suas disposições em seu lugar, se o tratado ou o acordo o não proibir. No entanto, o artigo 12.º, n.º 7, aplica-se independentemente de existir ou não um tratado ou acordo de assistência mútua com base em legislação uniforme ou recíproca em vigor entre as Partes interessadas.

Artigo 11.º – Videoconferência

187. O artigo 11.º aborda principalmente a utilização de tecnologias de videoconferência para recolher testemunhos ou depoimentos. Esta forma de cooperação pode ser prevista nos atuais tratados bilaterais e multilaterais de assistência mútua, como, por exemplo, o STCE n.º 182. A fim de não se sobrepor a disposições especificamente destinadas a cumprir as exigências das Partes nesses tratados ou convenções, e tal como estabelecido nos princípios gerais aplicáveis à presente secção (artigo 5.º, n.º 5), o artigo 11.º, tal como o artigo 12.º do presente Protocolo, "é aplicável quando não exista um tratado ou acordo de assistência mútua com base em legislação uniforme ou recíproca em vigor entre as Partes requerente e requerida. As disposições da secção 5 não serão aplicáveis caso exista tal tratado ou acordo, exceto nos casos previstos no artigo 12.º, n.º 7. No entanto, as Partes em questão podem decidir mutuamente aplicar, em sua substituição, as disposições da secção 5, se o tratado ou o acordo não o proibir".

N.º 1

188. O n.º 1 autoriza a recolha de depoimentos e declarações de testemunhas ou de peritos por videoconferência. O presente número confere à Parte requerida o poder discricionário de aceitar ou não o pedido de assistência mútua ou de estabelecer condições para a prestação de assistência. Por exemplo, uma Parte pode recusar ou adiar a assistência pelos motivos previstos no artigo 27.º, n.ºs 4 a 5, da Convenção. Em alternativa, se for mais eficaz que a assistência seja prestada de forma diferente, por exemplo através de um formulário escrito que autentique os registos oficiais ou comerciais, a Parte requerida pode optar por prestar assistência dessa forma.

189. Ao mesmo tempo, espera-se que as Partes no presente Protocolo disponham da capacidade técnica de base para prestar assistência através de videoconferência.

190. A realização de uma videoconferência para recolher o depoimento ou uma declaração pode suscitar muitas questões, que podem incluir problemas jurídicos, logísticos e técnicos. Para que a videoconferência funcione sem problemas, é essencial uma coordenação prévia. Poderá ser

necessária uma coordenação adicional quando a Parte requerida estabelecer condições como pré-requisitos para a realização da videoconferência. Por conseguinte, o n.º 1 exige igualmente que as Partes requerentes e requeridas se consultem sempre que seja necessário para facilitar a resolução de quaisquer questões que surjam. Por exemplo, conforme explicado mais abaixo, a videoconferência pode ter de seguir um determinado procedimento para que o resultado seja admissível como elemento de prova na Parte requerente. Em contrapartida, a Parte requerida pode ter de aplicar os seus próprios requisitos legais em determinados aspetos (por exemplo, a prestação de juramento pela testemunha ou a prestação de aconselhamento sobre os seus direitos). Além disso, a Parte requerida pode exigir que o(s) seu(s) funcionário(s) esteja(m) presente(s) na videoconferência em algumas ou em todas as situações, quer para presidir ao processo, quer para assegurar o respeito dos direitos da pessoa cujo depoimento ou declaração é obtido. A este respeito, as consultas podem revelar que algumas Partes requerentes exigem que o seu funcionário participante possa intervir, interromper ou parar a audição em caso de dúvidas quanto à conformidade com a sua legislação, ao passo que outras Partes podem permitir a realização de uma videoconferência sem a participação dos seus funcionários em determinadas circunstâncias. A título de exemplo, as Partes requeridas podem procurar obter garantias especiais no que diz respeito às testemunhas cuja segurança esteja em risco, às testemunhas menores e similares. Estas questões devem ser previamente discutidas e decididas. Em alguns casos, o desejo da Parte requerida de um procedimento pode entrar em conflito com a legislação da Parte requerente no sentido de facilitar a utilização do depoimento ou da declaração no julgamento. Nesses casos, as Partes devem envidar todos os esforços para tentar encontrar soluções criativas que respondam às necessidades de ambas as Partes. Além disso, as Partes consultam-se previamente para facilitar a resolução de questões, tais como a forma de tratar objeções ou alegações de privilégio ou imunidade levantadas pela pessoa ou pelo seu consultor jurídico, ou a utilização de provas documentais ou outras, durante a videoconferência. Ademais, podem ser necessários procedimentos especiais devido às condições impostas para a realização de uma videoconferência.

As questões logísticas, como a questão de saber se a Parte requerente deve assegurar a interpretação e a gravação do depoimento ou da declaração da sua parte da videoconferência ou da Parte requerida, devem também ser debatidas, bem como a coordenação técnica para iniciar e manter a transmissão e dispor de canais de comunicação alternativos em caso de interrupção da transmissão.

N.º 2

191. O n.º 2 aborda uma série de mecanismos processuais e conexos que regem esta forma de cooperação (para além de outros procedimentos e requisitos aplicáveis estabelecidos nos restantes números do presente artigo), que foram retirados ou adaptados da Convenção. O n.º 2 está dividido em duas alíneas.

192. Uma vez que a videoconferência é uma forma de assistência mútua, o n.º 2, alínea a), prevê que as autoridades centrais das Partes requerida e requerente devem comunicar diretamente entre si para efeitos da aplicação do presente artigo. Uma vez que o presente artigo só se aplica na ausência de um acordo ou convénio de assistência mútua com base em legislação uniforme ou recíproca, entende-se aqui por "autoridade central" a autoridade ou autoridades designadas nos termos do artigo 27.º, n.º 2, alínea a), da Convenção (ver artigo 3.º, n.º 2, alínea a), do presente Protocolo e o n.º 38 do relatório explicativo).

193. O n.º 2, alínea a), do presente artigo prevê igualmente que uma Parte requerida pode aceitar um pedido de videoconferência em formato eletrónico, podendo exigir níveis apropriados de segurança e autenticação antes de aceitar o pedido.

194. O n.º 2, alínea b), exige (à semelhança do artigo 27.º, n.º 7, da Convenção) que a Parte requerida informe a Parte requerente dos motivos que a levaram a não executar um pedido ou a atrasar a execução do pedido. Tal como referido no n.º 192 supra, essas comunicações devem ser efetuadas através dos canais da autoridade central. Por último, o n.º 2, alínea b), prevê que o artigo 27.º, n.º 8 (que trata da confidencialidade de um pedido de assistência mútua na ausência de um tratado), e o artigo 28.º, n.ºs 2 a 4 (que trata da confidencialidade da resposta e das limitações de utilização na ausência de um tratado), da Convenção se aplicam ao artigo relativo à videoconferência.

N.º 3

195. Uma vez que uma videoconferência pode exigir que os funcionários judiciais e auxiliares de uma Parte requerente estejam disponíveis para participar na recolha do depoimento ou declaração na Parte requerida, com muitos fusos horários de diferença, é fundamental que a pessoa a ouvir compareça na hora e no local previstos. Nos termos do n.º 3, quando a Parte requerida presta assistência ao abrigo do presente artigo envidará esforços para obter a presença da pessoa cujo depoimento ou declaração é solicitado. A melhor forma de o fazer pode depender das circunstâncias do caso, do direito interno da Parte requerida e da existência, por exemplo, da confiança de que a pessoa comparecerá voluntariamente à hora programada. Em contrapartida, para assegurar a comparência da pessoa, pode ser aconselhável que a Parte requerida emita uma ordem ou citação que a obrigue a comparecer, e o presente número a autoriza a fazer, em conformidade com as salvaguardas previstas no seu direito interno.

N.º 4

196. O procedimento relativo à realização de videoconferências é descrito no n.º 4. O principal objetivo é fornecer o depoimento ou declaração à Parte requerente de uma forma que permita a sua utilização como elemento de prova na sua investigação e processo. Por esse motivo, são aplicados os procedimentos solicitados pela Parte requerente, salvo se tal for incompatível com a legislação da Parte requerida, incluindo os princípios jurídicos aplicáveis da Parte requerida não codificados na sua legislação. Por exemplo, durante a videoconferência, o procedimento preferido será que a Parte requerida permita às autoridades da Parte requerente interrogar diretamente a pessoa à qual são solicitados depoimentos ou declarações. Será o procurador, juiz de instrução ou investigador da Parte requerente que conhece mais profundamente a investigação ou ação penal e, por conseguinte, conhece melhor as questões mais úteis para a investigação ou ação penal, bem como a melhor forma de as formular em conformidade com a legislação da Parte requerente. Nesse caso, a autoridade da Parte requerida que participa na audição só intervirá se necessário porque a autoridade da Parte requerente procedeu de forma incompatível com a legislação da Parte requerida. Nesse caso, a Parte requerida pode recusar as perguntas, assumir o interrogatório ou tomar outras medidas que se afigurem apropriadas nos termos da sua legislação e das circunstâncias da videoconferência. A expressão "incompatível com a legislação da Parte requerida" não abrange as situações em que o procedimento é meramente diferente do da Parte requerida, o que será, com frequência, o caso. Pelo contrário, destina-se a resolver situações em que o procedimento é contrário ou impraticável ao abrigo da legislação da Parte requerida. Em tais casos, ou se a Parte requerente não solicitar um procedimento específico, o procedimento por defeito será o procedimento aplicável ao abrigo da legislação da Parte requerida. Se a aplicação da legislação da Parte requerida causar um problema à Parte requerente, por exemplo em termos de admissibilidade do depoimento ou da declaração no julgamento, a Parte requerente e a Parte requerida podem procurar chegar a acordo sobre um procedimento diferente que permita à Parte requerente evitar o problema ao abrigo da legislação da Parte requerida.

N.º 5

197. O n.º 5, relativo à pena ou sanção por falsas declarações, recusa de resposta e outras faltas graves, tem por objetivo proteger a integridade do processo de prestação de depoimento ou declaração quando a testemunha estiver fisicamente situada num país diferente daquele em que decorre o processo penal. Na medida em que a Parte requerida tenha imposto à pessoa a obrigação de depor ou de testemunhar de forma fidedigna, ou tenha proibido a pessoa de praticar determinado comportamento (por exemplo, interromper o processo), a testemunha ficará sujeita a consequências na jurisdição em que se encontra a testemunha. Nesses casos, a Parte requerida deve poder aplicar a sanção que aplicaria se tal comportamento tivesse ocorrido no decurso dos seus próprios procedimentos internos. O presente é aplicável sem prejuízo de qualquer jurisdição da Parte requerente. Este requisito constitui um incentivo adicional para que a testemunha testemunhe, o faça de forma fidedigna e não participe em comportamentos proibidos. Se não existir uma sanção aplicável no processo interno da Parte requerida (por exemplo, em caso de falsas declarações por parte de um arguido), esta não é obrigada a estabelecer qualquer sanção para esse tipo de conduta cometida durante uma videoconferência. Esta disposição será particularmente útil para garantir a ação penal contra uma testemunha que

preste falso testemunho, mas não possa ser extraditada para ser alvo de ação penal na Parte requerente devido, por exemplo, à proibição de extradição de nacionais por parte de uma Parte requerida.

N.º 6

198. O n.º 6 estabelece regras relativas à alocação dos custos decorrentes de videoconferências. Regra geral, todos os custos decorrentes de uma videoconferência são suportados pela Parte requerida, com exceção de: i) honorários de testemunhos de peritos, ii) custos de tradução, interpretação e transcrição, e iii) custos tão significativos que sejam de natureza extraordinária. Na maioria dos casos, as despesas de deslocação e as despesas de alojamento na Parte requerida não são substanciais, pelo que tais custos, se existirem, são geralmente assumidos pela Parte requerida. No entanto, as regras relativas aos custos podem ser alteradas por acordo entre a Parte requerente e a Parte requerida. Por exemplo, se a Parte requerente assegurar a presença de um intérprete que é necessário ou de serviços de transcrição no final da videoconferência, poderá não ser necessário pagar à Parte requerida pela prestação desses serviços. Quando a Parte requerida prevê custos extraordinários para a prestação de assistência, em conformidade com o n.º 6, alínea b), a Parte requerente e a Parte requerida consultam-se antes da execução do pedido, a fim de determinar se a Parte requerente pode suportar esses custos e, em caso negativo, como podem ser evitados.

N.º 7

199. Embora o n.º 1 autorize expressamente a utilização de tecnologia de videoconferência para a obtenção de depoimentos ou declarações, o n.º 7, alínea a), prevê que as disposições do artigo 11.º podem ser aplicadas para efeitos de realização de audioconferências, se tal for mutuamente acordado. Além disso, o n.º 7, alínea b), prevê que, quando acordado pelas Partes requerente e requerida, a tecnologia pode ser utilizada para outros "fins, ou para audiências, [...] inclusive para efeitos de identificação de pessoas ou objetos". Assim, se mutuamente acordado, as Partes requerente e requerida podem ponderar a utilização de tecnologia de videoconferência para ouvir ou levar a cabo um processo relativo a um suspeito ou arguido (note-se que algumas Partes podem considerar que um suspeito ou acusado é uma "testemunha", de modo a que a recolha do depoimento ou da declaração dessa pessoa já esteja abrangida pelo n.º 1 do presente artigo). Nos casos em que o n.º 1 não seja aplicável, o n.º 7 confere poderes legais para permitir a utilização da tecnologia.

N.º 8

200. O n.º 8 aborda a situação em que a Parte requerida opta por permitir a audição de um suspeito ou acusado, nomeadamente para efeitos de prestação de depoimentos ou declarações, ou para notificações ou outras medidas processuais. Da mesma forma que a Parte requerida tem poder discricionário para autorizar uma videoconferência de uma testemunha ou perito comum, tem poder discricionário no que diz respeito a um suspeito ou acusado. Além disso, para além de qualquer outra condição ou limitação que uma Parte requerida possa impor para permitir a realização de uma videoconferência, a legislação interna de uma Parte pode exigir condições especiais no que diz respeito à audição de suspeitos ou arguidos. Por exemplo, a legislação de uma Parte pode exigir o consentimento do suspeito ou acusado para prestar depoimento ou declarações, ou a legislação de uma Parte pode proibir ou limitar a utilização de videoconferência para notificações ou outras medidas processuais. Assim, o n.º 8 visa sublinhar o facto de os procedimentos aplicados a um suspeito ou arguido poderem dar origem à necessidade de condições ou salvaguardas complementares às que, de outro modo, poderiam surgir.

Artigo 12.º – Equipas de investigação conjuntas e investigações conjuntas

201. Dada a natureza transnacional do cibercrime e das provas sob a forma eletrónica, as investigações e ações penais relacionadas com o cibercrime e as provas sob a forma eletrónica têm, com frequência, ligações a outros Estados. As equipas de investigação conjuntas podem constituir um meio eficaz de cooperação operacional ou de coordenação entre dois ou mais Estados. O artigo 12.º fornece uma base para essas formas de cooperação.

202. A experiência demonstrou que, quando um Estado está a investigar uma infração com dimensão transfronteiras relacionada com o cibercrime ou para a qual é necessário obter provas sob a forma eletrónica, a investigação pode beneficiar da participação das autoridades de outros Estados que também estão a investigar a mesma conduta ou conduta conexa ou quando a coordenação é de outro modo útil.

203. Tal como indicado no artigo 5.º, n.os 182 a 186, do presente Protocolo e do relatório explicativo, o disposto no artigo 12.º não é aplicável nos casos em que exista um tratado ou acordo de assistência mútua com base na legislação uniforme ou recíproca em vigor entre as Partes requerente e requerida, a menos que as Partes em causa decidam mutuamente aplicar uma parte ou a totalidade do resto do presente artigo em seu lugar, se o tratado ou acordo não o proibir. Tal como explicado abaixo, o n.º 7 aplica-se independentemente de existir ou não um tratado ou acordo de assistência mútua com base em legislação uniforme ou recíproca em vigor entre as Partes interessadas.

N.º 1

204. O n.º 1 estabelece que as autoridades competentes de duas ou mais Partes podem acordar em criar uma equipa de investigação conjunta sempre que o considerem de especial utilidade. Uma equipa de investigação conjunta é estabelecida de comum acordo. Os termos "comum acordo", "acordo" e "acordar" – tal como utilizados no artigo 12.º – não devem ser entendidos como exigindo um acordo vinculativo ao abrigo do direito internacional.

205. Este artigo utiliza dois termos conexos: "autoridades competentes" e "autoridades participantes". Cada Parte determina quais as autoridades que têm competência – ou seja, as "autoridades competentes" – para celebrar um acordo de equipas de investigação conjuntas. Algumas Partes podem autorizar uma série de funcionários, tais como procuradores, juízes de instrução ou outros altos funcionários responsáveis pela aplicação da lei que dirigem investigações ou processos penais, a celebrar esse acordo; outras podem exigir que a autoridade central – o serviço normalmente responsável pelas questões de assistência mútua – o faça. A decisão sobre quais as autoridades que participam efetivamente numa equipa de investigação conjunta – as "autoridades participantes" – será igualmente determinada pelas respetivas Partes.

N.º 2

206. O n.º 2 prevê que os procedimentos e condições que regem o funcionamento das equipas de investigação conjuntas, tais como os seus objetivos específicos, a sua composição, as suas atribuições, a sua duração e eventuais prorrogações, a sua localização, a sua organização, as condições de recolha, transmissão e utilização de informação ou dos elementos de prova, as condições de confidencialidade, e as condições de participação das autoridades de uma Parte nas atividades de investigação que tenham lugar no território de outra Parte serão os acordados entre essas autoridades competentes. Em especial, ao preparar o acordo, as Partes em causa podem desejar discutir as condições de recusa ou restrição da utilização de informação ou elementos de prova, incluindo, por exemplo, pelos motivos estabelecidos no artigo 27.º, n.os 4 ou 5, da Convenção, e o procedimento a seguir se a informação ou prova for necessária para fins diferentes daqueles para os quais o acordo foi celebrado (incluindo a utilização da informação ou do elemento de prova pela ação penal ou pela defesa noutro caso ou quando tal seja necessário para evitar uma emergência, tal como definida no artigo 3.º, n.º 2, alínea c), ou seja, uma situação em que exista um risco significativo e iminente para a vida ou a segurança de uma pessoa singular). As Partes são incentivadas a especificar no acordo os limites dos poderes dos funcionários participantes de uma Parte que se encontrem fisicamente presentes no território de outra Parte. As Partes são igualmente instadas a, no acordo, autorizar a transmissão eletrónica da informação ou elementos de prova recolhidos.

207. Prevê-se que, de um modo geral, as Partes determinem mutuamente esses procedimentos e condições por escrito. Em qualquer acordo, deve ser tido em conta o nível de pormenor exigido. Um texto simplificado pode proporcionar o nível de rigor necessário para circunstâncias previsíveis, com a possibilidade de acrescentar disposições suplementares caso circunstâncias futuras requeiram um maior rigor. As Partes devem considerar o âmbito geográfico e a duração

do acordo relativo à equipa de investigação conjunta, bem como o facto de o acordo poder ter de ser alterado ou alargado à medida que estiverem disponíveis novos dados.

208. A informação ou elementos de prova utilizados como parte da equipa de investigação conjunta podem incluir dados pessoais sob a forma de informação sobre subscritores, dados de tráfego ou dados de conteúdo. Tal como no caso de outras medidas de cooperação ao abrigo do presente Protocolo, o artigo 14.º aplica-se à transferência de dados pessoais no âmbito das equipas de investigação conjuntas.

209. Como é geralmente o caso no que diz respeito a toda a informação ou elementos de prova recebidos por uma Parte nos termos do presente Protocolo, as regras aplicáveis dessa Parte em matéria de prova reger-se-ão pela admissibilidade da informação ou dos elementos de prova em processos judiciais.

N.º 3

210. O n.º 3 autoriza uma Parte a declarar, no momento da assinatura do presente Protocolo ou aquando do depósito do seu instrumento de ratificação, aceitação ou aprovação, que a sua autoridade central deverá ser signatária ou consubstanciada no acordo que institui a equipa. Esta disposição foi inserida por várias razões. Em primeiro lugar, algumas Partes consideram que as equipas de investigação conjuntas constituem uma forma de assistência mútua e, em várias outras Partes, as autoridades centrais de assistência mútua podem desempenhar um papel importante para garantir o cumprimento dos requisitos jurídicos internos aplicáveis quando as autoridades competentes (que podem ser procuradores ou a polícia com uma experiência de cooperação internacional relativamente limitada) estão a preparar um acordo de equipa de investigação conjunta ao abrigo do presente artigo. A experiência de uma autoridade central com acordos internacionais que regem a assistência mútua e outras formas de cooperação internacional (incluindo o presente Protocolo) pode também ajudá-la a desempenhar um papel valioso na garantia do cumprimento dos requisitos do Protocolo. Por último, se uma Parte tiver realizado a declaração prevista no presente número, as autoridades das outras Partes que pretendam participar numa equipa de investigação conjunta com a Parte declarante são notificadas de que a autoridade central da Parte declarante deve assinar ou aceitar de outra forma o acordo relativo à equipa de investigação conjunta para que este seja válido ao abrigo do Protocolo. Tal assegura proteção contra a celebração de um acordo de equipa de investigação conjunta que não tenha exigido autorização ou não cumpra os requisitos legais aplicáveis da Parte declarante.

N.º 4

211. Nos termos do n.º 4, as autoridades competentes determinadas pelas Partes nos termos do n.º 1 e as autoridades participantes descritas no n.º 2 devem normalmente comunicar diretamente entre si para garantir a eficiência e a eficácia. No entanto, sempre que circunstâncias excecionais possam exigir uma coordenação mais centralizada – tais como casos com ramificações particularmente graves ou situações que suscitem problemas específicos de coordenação – poderão ser acordados outros canais apropriados. Por exemplo, as autoridades centrais de assistência mútua podem estar disponíveis para prestar assistência na coordenação dessas questões.

N.º 5

212. O n.º 5 prevê que, sempre que seja necessário tomar medidas de investigação no território de uma das Partes participantes, as autoridades participantes dessa Parte podem apresentar um pedido às suas próprias autoridades para que apliquem tais medidas. Essas autoridades determinam se podem tomar a medida de investigação com base no seu direito interno. Caso o possam fazer, poderá não ser necessário outras Partes participantes apresentarem um pedido de assistência mútua. Trata-se de um dos aspetos mais inovadores das equipas de investigação conjuntas. No entanto, em algumas situações, essas autoridades podem não ter autoridade interna suficiente para tomar uma determinada medida de investigação em nome de outra Parte sem um pedido de assistência mútua.

N.º 6

213. O n.º 6 aborda a utilização de informação ou elementos de prova obtidos pelas autoridades participantes de uma Parte junto das autoridades participantes de outra Parte. A utilização pode ser recusada ou limitada nos termos de um acordo descrito nos n.os 1 e 2; no entanto, se esse acordo não previr condições para recusar ou restringir a utilização, a informação ou elementos de prova podem ser utilizados da forma prevista no n.º 6, alíneas a) a c). As circunstâncias previstas no n.º 6 não prejudicam os requisitos estabelecidos no artigo 14.º para a transferência ulterior de informação ou elementos de prova para outro Estado.

14. Note-se que, quando o n.º 6, alíneas a) a c), forem aplicáveis, as autoridades participantes poderão, no entanto, decidir de comum acordo limitar ainda mais a utilização de determinada informação ou elementos de prova, com vista a evitar consequências negativas para uma das suas investigações, antes ou particularmente depois de a informação ou os elementos de prova terem sido fornecidos. Por exemplo, mesmo que a utilização de elementos de prova se destine a uma finalidade para a qual a equipa de investigação conjunta foi criada pela Parte que os recebeu, poderá ter um impacto negativo na investigação da Parte que fornece a informação ou elementos de prova (por exemplo, revelando a existência da investigação a um grupo criminoso, podendo assim levar os criminosos a fugir, destruir provas ou intimidar testemunhas). Nesse caso, a Parte que forneceu a informação ou os elementos de prova podem solicitar à outra Parte que não as torne públicas até que esse risco deixe de existir.

215. No n.º 6, alínea b), os redatores pretendiam que, na ausência de um acordo que estipulasse as condições de recusa ou restrição da utilização, não seria necessário o consentimento das autoridades que forneceram a informação ou os elementos de prova quando, de acordo com os princípios jurídicos fundamentais da Parte cujas autoridades participantes os receberam, a informação ou os elementos de prova importantes para conduzir uma defesa eficaz no processo relativo a essas outras infrações devam ser comunicados à defesa ou a uma autoridade judicial. Mesmo que, neste caso, não seja necessário o consentimento, a notificação da divulgação da informação ou dos elementos de prova para este efeito deve ser efetuada sem demora indevida. Se possível, essa notificação deve ser efetuada antes da divulgação, para que a Parte que forneceu a informação ou os elementos de prova possa preparar-se para a divulgação e permitir que as Partes se consultem, se for caso disso.

216. Os redatores entenderam que o n.º 6, alínea c), se refere a circunstâncias excecionais em que as autoridades da Parte recetora podem utilizar diretamente a informação ou os elementos de prova para evitar uma emergência, tal como definida no artigo 3.º, n.º 2, alínea c), do presente Protocolo. A segurança de uma pessoa singular significa danos corporais graves. O conceito de "risco significativo e iminente para a vida ou a segurança de qualquer pessoa singular" é explicado de forma mais pormenorizada no n.º 42 do relatório explicativo, que também fornece exemplos de tais situações. Os redatores consideraram que os casos em que uma ameaça significativa e iminente a bens ou redes envolva a vida ou a segurança de uma pessoa singular seriam incluídos nesse conceito. Nos casos em que seja utilizada informação ou elementos de prova nos termos do n.º 6, alínea c), as autoridades participantes da Parte que a forneceu devem ser notificadas sem demora indevida dessa utilização, salvo determinação em contrário. Por exemplo, as autoridades participantes podem determinar que a autoridade central deve ser notificada.

N.º 7

217. Por último, importa recordar que, de um modo geral, há uma longa história de esforços de cooperação internacional entre parceiros responsáveis pela aplicação da lei numa base *ad hoc*, na qual uma equipa de procuradores e/ou investigadores de um país cooperou com homólogos estrangeiros numa determinada investigação, numa base que não as equipas de investigação conjuntas. O n.º 7 prevê estes esforços de cooperação internacional e estabelece uma base consagrada no Tratado para a realização de uma investigação conjunta na ausência de um acordo descrito nos n.os 1 e 2, caso uma Parte exija essa base jurídica. O presente número aplica-se independentemente de existir ou não um tratado ou acordo de assistência mútua com base em legislação uniforme ou recíproca em vigor entre as Partes interessadas. Tal como com todas as medidas ao abrigo do presente Protocolo, as investigações conjuntas ao abrigo do n.º 7 estão sujeitas às condições e salvaguardas previstas no Capítulo III.

Capítulo III – Condições e salvaguardas

Artigo 13.º – Condições e salvaguardas

218. Com base no artigo 15.º da Convenção, o artigo 13.º dispõe que o "cada Parte assegurará que o estabelecimento, a execução e a aplicação dos poderes e procedimentos previstos no presente Protocolo estejam sujeitos às condições e salvaguardas previstas no seu direito interno, que devem assegurar a proteção adequada dos direitos humanos e das liberdades". Uma vez que este artigo se baseia no artigo 15.º da Convenção, a explicação desse artigo nos n.os 145 a 148 do relatório explicativo da Convenção é igualmente válida para o artigo 13.º do presente Protocolo, incluindo que o princípio da proporcionalidade "deverá ser implementado por cada uma das Partes, em conformidade com os princípios relevantes da sua legislação nacional" (ver o n.º 146 do relatório explicativo da Convenção).

219. Note-se que, para além deste artigo, outros artigos contêm salvaguardas importantes. Por exemplo, as medidas do presente Protocolo têm um âmbito de aplicação limitado, ou seja, "a investigações ou processos penais específicos relativos a infrações penais relacionadas com sistemas e dados informáticos e com a recolha de provas sob a forma eletrónica de uma infração penal" (ver artigo 2.º). Além disso, os artigos específicos estabelecem a informação a incluir nos pedidos, injunções e informação de acompanhamento que podem ajudar a aplicar as salvaguardas nacionais (ver artigo 6.º, n.º 3; artigo 7.º, n.os 3 e 4; artigo 8.º, n.º 3; artigo 9.º, n.º 3). Além disso, os tipos de dados a divulgar são especificados em cada artigo, como, por exemplo, no artigo 7.º, que se limita à informação dos subscritores. Igualmente, as Partes podem formular reservas e fazer declarações, por exemplo para limitar o tipo de informação a fornecer, tal como previsto nos artigos 7.º e 8.º. Por último, quando os dados pessoais são transferidos nos termos do presente Protocolo, aplicam-se as salvaguardas em matéria de proteção de dados previstas no artigo 14.º.

Artigo 14.º – Proteção de dados pessoais

N.º 1 – Âmbito

220. As medidas previstas no Capítulo II do presente Protocolo implicam, com frequência, a transferência de dados pessoais. Dado que muitas Partes no presente Protocolo podem ser obrigadas, com vista a cumprir as suas obrigações constitucionais ou internacionais, a assegurar a proteção dos dados pessoais, o artigo 14.º prevê salvaguardas em matéria de proteção de dados para permitir que as Partes cumpram esses requisitos e, assim, permitam o tratamento de dados pessoais para efeitos do presente Protocolo.

221. Nos termos do n.º 1, alínea a), cada Parte procede ao tratamento dos dados pessoais que receba ao abrigo do presente Protocolo, em conformidade com as garantias específicas estabelecidas nos n.os 2 a 15. Tal inclui os dados pessoais transferidos no âmbito de uma injunção ou de um pedido nos termos do presente Protocolo. No entanto, os n.os 2 a 15 não se aplicam se forem aplicáveis os termos das exceções enunciadas nos n.º 1, alínea b) ou alínea c).

222. A primeira exceção é estabelecida no n.º 1, alínea b), que prevê que "se, no momento da receção dos dados pessoais ao abrigo do presente Protocolo, tanto a Parte que procede à transferência como a Parte recetora estiverem mutuamente vinculadas por um acordo internacional que estabeleça um quadro abrangente entre essas Partes para a proteção de dados pessoais, aplicável à transferência de dados pessoais para efeitos de prevenção, deteção, investigação e repressão de infrações penais, e que preveja que o tratamento de dados pessoais ao abrigo desse acordo está em conformidade com os requisitos da legislação em matéria de proteção de dados das Partes interessadas, os termos desse acordo serão aplicáveis no caso das medidas abrangidas pelo âmbito desse acordo, aos dados pessoais recebidos ao abrigo do Protocolo em substituição dos n.os 2 a 15, exceto quando o contrário for mutuamente acordado pelas Partes interessadas". Neste contexto, um quadro seria, de um modo geral, considerado "abrangente" quando incluísse de forma abrangente os aspetos das transferências de dados relativos à proteção de dados. Dois exemplos de acordos ao abrigo do n.º 1, alínea b), são a Convenção para a Proteção das Pessoas no que diz respeito ao Tratamento Automatizado de Dados

Pessoais (STCE n.º 108), com a redação que lhe foi dada pelo Protocolo STCE n.º 223, e o Acordo entre os Estados Unidos da América e a União Europeia sobre a Proteção de Informação Pessoal em matéria de Prevenção, Investigação, Deteção e Repressão de Infrações Penais. Os termos desses acordos são aplicáveis, em vez dos n.os 2 a 15, às medidas abrangidas pelo âmbito de aplicação desses acordos. No que diz respeito às Partes na Convenção STCE n.º 108, com a redação que lhe foi dada pelo Protocolo STCE n.º 223, tal significa que é aplicável o artigo 14.º, n.º 1, desse tratado, tal como explicado nos n.os 105 a 107 do seu relatório explicativo. Em termos de calendário, os n.os 2 a 15 do presente artigo só serão substituídos se as Partes estiverem mutuamente vinculadas pelo acordo no momento da receção dos dados pessoais ao abrigo do presente Protocolo. Tal aplica-se enquanto o acordo previr que os dados transferidos ao abrigo do mesmo continuam a ser tratados nos termos desse acordo.

223. A segunda exceção é estabelecida no n.º 1, alínea c), que prevê que mesmo que a Parte que procede à transferência e a Parte recetora não estiverem mutuamente vinculadas ao abrigo de um acordo do tipo descrito no n.º 1, alínea b), poderão, contudo, determinar mutuamente que a transferência de dados pessoais ao abrigo do presente Protocolo pode ter lugar com base noutros acordos ou convénios entre elas em substituição dos n.º 2 a 15 de aplicação deste artigo. Tal garante que as Partes mantêm flexibilidade na determinação das salvaguardas em matéria de proteção de dados aplicáveis às transferências entre si ao abrigo do Protocolo. No sentido de proporcionar segurança jurídica e transparência às pessoas singulares e aos fornecedores e entidades envolvidos nas transferências de dados nos termos das medidas previstas no Capítulo II, secção 2, do presente Protocolo, as Partes são incentivadas a comunicar claramente ao público a sua determinação mútua de que tal acordo ou convénio reja os aspetos de proteção de dados das transferências de dados pessoais entre si.

224. Os redatores consideraram que, através das salvaguardas em matéria de proteção de dados previstas nos n.os 2 a 15 do presente artigo, o presente Protocolo assegura uma proteção apropriada para as transferências de dados ao abrigo do presente Protocolo. Para o efeito, nos termos do n.º 1, alínea d), considera-se que as transferências de dados ao abrigo do n.º 1, alínea a), satisfazem os requisitos do quadro jurídico em matéria de proteção de dados para as transferências internacionais de dados pessoais de cada Parte, não sendo necessária qualquer outra autorização para tais transferências ao abrigo desses quadros jurídicos.

Além disso, na medida em que os acordos descritos no n.º 1, alínea b), prevejam nos seus termos que o tratamento de dados pessoais ao abrigo desses acordos cumpre os requisitos da legislação em matéria de proteção de dados das Partes em causa, o n.º 1, alínea d), alarga esta aprovação às transferências ao abrigo do presente Protocolo. O presente número proporciona, assim, segurança jurídica às transferências internacionais de dados pessoais em conformidade com o n.º 1, alínea a) ou alínea b) em resposta a injunções e pedidos ao abrigo do presente Protocolo para assegurar um intercâmbio de dados eficaz e previsível. Uma vez que os acordos ou convénios descritos no n.º 1, alínea c), nem sempre podem fazer referência ao cumprimento do quadro jurídico das Partes em matéria de proteção de dados para as transferências internacionais – por exemplo, no caso de tratados bilaterais de assistência mútua – não recebem a mesma aprovação ao abrigo do presente Protocolo que para o n.º 1, alínea a) ou alínea b). No entanto, as Partes em causa podem prever essa aprovação por determinação mútua.

225. Além disso, o n.º 1, alínea d), prevê que uma Parte só poderá recusar ou impedir transferências de dados pessoais para outra Parte ao abrigo do presente Protocolo por razões de proteção de dados: i) nas condições estabelecidas no n.º 15 relativas à consulta e suspensão quando for aplicável o n.º 1, alínea a), ou ii) nos termos de acordos ou convénios específicos referidos no n.º 1, alíneas b) ou c), quando for aplicável um desses números.

226. Por último, o artigo 14.º tem por objetivo estabelecer salvaguardas apropriadas que permitam a transferência de dados pessoais entre as Partes ao abrigo do presente Protocolo. O artigo 14.º não exige a harmonização dos quadros jurídicos nacionais para o tratamento de dados pessoais em geral, nem do quadro para o tratamento de dados pessoais especificamente para efeitos de aplicação do direito penal. O n.º 1, alínea e), prevê que as Partes não estão impedidas de aplicar salvaguardas de proteção de dados mais rigorosas do que as previstas nos n.os 2 a 15 ao tratamento, pelas suas próprias autoridades, de dados pessoais que essas autoridades recebam ao abrigo do presente Protocolo. Inversamente, o n.º 1, alínea e), não se destina a permitir que as Partes imponham requisitos adicionais em matéria de proteção de dados para

as transferências de dados ao abrigo do presente Protocolo para além dos especificamente autorizados no presente artigo.

N.º 2 – Finalidade e utilização

227. O n.º 2 aborda as finalidades e a utilização para as quais as Partes podem tratar dados pessoais ao abrigo do presente Protocolo. O n.º 2, alínea a), prevê que "a Parte que tenha recebido dados pessoais procederá ao seu tratamento para os fins descritos no artigo 2.º", ou seja, para efeitos de "investigações ou processos penais específicos relativos a infrações penais relacionadas com sistemas e dados informáticos e com dados" e para a "recolha de provas sob a forma eletrónica de uma infração penal", e entre as Partes no Primeiro Protocolo, para efeitos de "investigações ou processos penais específicos relativos a infrações penais estabelecidas nos termos do Primeiro Protocolo". Por outras palavras, as autoridades devem investigar ou processar uma atividade criminosa específica, que é a finalidade legítima para a qual podem ser procurados e tratados elementos de prova ou informação que contenham dados pessoais.

228. Embora, em primeiro lugar, o presente Protocolo só possa ser invocado para obter informação ou elementos de prova no âmbito de uma investigação ou processo penal específico, e não para outros fins, o n.º 2, alínea a), prevê igualmente que uma Parte "não procederá ao tratamento adicional dos dados pessoais para uma finalidade incompatível, nem procederá ao tratamento posterior dos dados quando tal não for permitido pelo seu quadro jurídico interno". Ao determinar se a finalidade do tratamento posterior não é incompatível com a finalidade inicial, a autoridade competente é incentivada a proceder a uma avaliação global das circunstâncias específicas, tais como: i) a relação entre a finalidade inicial e a finalidade posterior (por exemplo, qualquer ligação objetiva), ii) as consequências (potenciais) da utilização posterior prevista para as pessoas em causa, tendo em conta a natureza dos dados pessoais (por exemplo, a sua sensibilidade), iii) as expectativas razoáveis das pessoas em causa quanto à finalidade de uma utilização posterior e às entidades que podem tratar os dados, e iv) a forma como os dados serão tratados e protegidos contra uma utilização indevida. O quadro jurídico de uma Parte pode ainda estabelecer limitações específicas relativamente a outros fins para os quais os dados podem ser utilizados.

229. O tratamento para uma finalidade não incompatível inclui normalmente a utilização dos dados para fins de cooperação internacional, nos termos do direito interno e de acordos ou convénios internacionais (por exemplo, assistência mútua) no domínio do direito penal. Poderá também incluir, entre outros aspetos, utilizações para determinadas funções públicas, como a comunicação de informação aos organismos de supervisão, inquéritos conexos sobre violações do direito penal, civil ou administrativo (incluindo inquéritos de outras componentes governamentais) e respetiva decisão, divulgações exigidas por decisões judiciais nacionais, divulgação a litigantes particulares, divulgação de determinada informação ao advogado de um arguido, e a divulgação direta ao público ou aos meios de comunicação social (incluindo no contexto dos pedidos de acesso a documentos e de processos judiciais públicos). Do mesmo modo, o tratamento posterior de dados pessoais para fins de arquivo de interesse público, de investigação científica ou histórica ou para fins estatísticos pode ser considerado compatível.

230. O n.º 2, alínea a) permite ainda que as Partes imponham condições e limitações adicionais à utilização de dados pessoais em casos individuais, na medida prevista no Capítulo II do presente Protocolo. No entanto, essas condições não devem incluir condições genéricas de proteção de dados – ou seja, as que não são específicas de casos – para além das previstas no artigo 14.º. A título de exemplo, são aceites diferentes sistemas de supervisão ao abrigo do n.º 14 e uma Parte não pode subordinar a transferência, num caso concreto, ao facto de a Parte requerente ter o equivalente a uma autoridade especializada em matéria de proteção de dados.

231. Por último, o n.º 2, alínea b), exige que, ao procurar e utilizar dados pessoais ao abrigo do presente Protocolo, "a Parte recetora assegurará, ao abrigo do seu quadro jurídico interno, que os dados pessoais solicitados e tratados são pertinentes e não excessivos em relação às finalidades desse tratamento". Este requisito pode ser aplicado, por exemplo, através de regras em matéria de prova e de limitações à extensão das injunções obrigatórias, dos princípios da necessidade e da proporcionalidade, dos princípios da razoabilidade e das orientações e políticas internas que limitam a recolha ou utilização de dados. As Partes são igualmente

incentivadas a considerar, no âmbito dos seus quadros jurídicos nacionais, situações que envolvam pessoas vulneráveis, como, por exemplo, vítimas ou menores.

N.º 3 – Qualidade e integridade

232. O n.º 3 exige que as Parte "adotem as medidas razoáveis para assegurar que os dados pessoais sejam conservados com a exatidão e integridade necessárias e estejam atualizados na medida do necessário e apropriado para o tratamento legítimo dos dados pessoais, tendo em conta as finalidades para que são tratados". O contexto é importante, para que este princípio possa ser aplicado de forma diferente consoante as circunstâncias. Por exemplo, o princípio será aplicado de forma distinta em processos penais da para outros fins.

233. No que diz respeito às investigações e processos penais, o n.º 3 não deve ser considerado como exigindo que as autoridades responsáveis pela aplicação da lei penal alterem informação – mesmo que essa informação seja inexata ou incompleta – que possa constituir elementos de prova num processo penal, uma vez que a inexatidão dos dados pode ser fundamental para o crime (por exemplo, em casos de fraude), e também prejudicaria o objetivo de equidade para o arguido se as autoridades alterassem um elemento de prova recolhido através do presente Protocolo.

234. Em muitas situações, quando existem dúvidas quanto à fiabilidade dos dados pessoais, tal deve ser claramente indicado. Por exemplo, na medida em que a informação ou provas recebidas através do presente Protocolo sejam utilizadas para rastrear a conduta criminosa passada, os procedimentos aplicáveis devem proporcionar meios para corrigir ou memorizar erros na informação (por exemplo, alterando ou completando a informação original), bem como para atualizar, alterar ou completar dados não fiáveis ou desatualizados, a fim de minimizar o risco de as autoridades tomarem medidas de aplicação da lei inapropriadas e potencialmente adversas com base na má qualidade dos dados (por exemplo, deter a pessoa errada ou deter uma pessoa com base numa compreensão incorreta da sua conduta). As Partes são incentivadas a tomar medidas razoáveis para garantir que, sempre que os dados fornecidos a outra autoridade ou por ela recebidos sejam considerados incorretos ou desatualizados, a outra autoridade seja informada o mais rapidamente possível, por forma a efetuar as correções necessárias e apropriadas tendo em conta as finalidades do tratamento.

N.º 4 – Dados sensíveis

235. O n.º 4 diz respeito às medidas a tomar ao abrigo do presente Protocolo pelas Partes no tratamento de determinados tipos de dados que possam ser necessários, nomeadamente como elementos de prova no âmbito de uma investigação ou processo penal, mas que sejam, simultaneamente, de natureza tal que se verifique a necessidade de salvaguardas apropriadas para prevenir o risco de efeitos prejudiciais injustificados para a pessoa em causa decorrentes da utilização desses dados, em especial contra a discriminação ilegal.

236. O n.º 4 prevê que os dados sensíveis incluem "dados pessoais que revelem a origem racial ou étnica, as opiniões políticas ou crenças religiosas ou outras, ou a filiação sindical, dados genéticos, dados biométricos considerados sensíveis tendo em conta os riscos envolvidos, ou dados pessoais relativos à saúde ou à vida sexual", que abrangerão tanto a orientação sexual como as práticas sexuais. Os dados de saúde podem incluir dados relacionados com a saúde física ou mental de uma pessoa que revelem informação sobre o seu estado de saúde passado, presente ou futuro (por exemplo, informação sobre uma doença, deficiência, risco de doença, historial clínico ou tratamento de uma pessoa, ou o estado fisiológico ou biomédico da pessoa). Os dados genéticos podem incluir, por exemplo, dados resultantes de análises cromossómicas, ADN ou ARN e relacionados com as características genéticas hereditárias ou adquiridas de uma pessoa que contenham informação única sobre a sua fisiologia, saúde ou filiação.

237. O conceito de dados biométricos abrange uma série de identificadores únicos resultantes de características físicas ou fisiológicas mensuráveis, utilizadas para identificar ou verificar a alegada identidade de uma pessoa (por exemplo, impressões digitais, íris ou padrões das veias da mão, padrões vocais, fotografias ou imagens de vídeo). Algumas Partes consideram igualmente que os identificadores únicos resultantes de características biológicas ou

comportamentais constituem dados biométricos. Embora certas formas de dados biométricos possam ser consideradas sensíveis tendo em conta os riscos envolvidos, outras podem não o ser. Por exemplo, algumas Partes consideram sensíveis os dados biométricos que são calculados ou extraídos de uma amostra ou imagem biométrica (tais como modelos biométricos). Inversamente, determinadas fotografias ou imagens de vídeo, mesmo que revelem características físicas ou anatómicas como cicatrizes, marcas na pele e tatuagens, não serão, em geral, consideradas como sendo abrangidas pela categoria de dados biométricos sensíveis. Dado que o nível de sensibilidade dos dados biométricos pode variar, o n.º 4 proporciona flexibilidade às Partes para regulamentar este domínio, indicando que os dados sensíveis incluem "dados biométricos considerados sensíveis tendo em conta os riscos envolvidos". Esta linguagem reconhece que a biometria é um domínio em evolução e que dados considerados "sensíveis" nos termos do presente número terão de ser avaliados ao longo do tempo em conjunto com os desenvolvimentos tecnológicos, de investigação e outros, bem como os riscos para o indivíduo envolvido. No que diz respeito às Partes na Convenção para a Proteção das Pessoas no que diz respeito ao Tratamento Automatizado de Dados Pessoais (STCE n.º 108), com a redação que lhe foi dada pelo Protocolo STCE n.º 223, a interpretação do que constitui dados biométricos "sensíveis" deve orientar-se pelo artigo 6.º, n.º 1, desse tratado, tal como especificado nos n.os 58 e 59 do seu relatório explicativo.

238. A utilização abusiva e o tratamento inadequado de dados sensíveis apresentam potenciais riscos de prejuízo injustificado para as pessoas, incluindo riscos de discriminação ilegal. O sistema de justiça penal deve ser configurado de modo a prevenir os efeitos prejudiciais injustificados e a discriminação ilegal com base, por exemplo, na utilização de provas que revelem a raça, a religião ou a vida sexual. Como outro exemplo, este número reconhece também a importância de proteção contra o risco de danos causados pela divulgação indevida ou ilícita, por exemplo, uma pessoa que seja ostracizada com base em informação que revele a orientação sexual ou a identidade de género. A este respeito, o n.º 4 exige que as Partes prevejam "salvaguardas apropriadas" para prevenir tais riscos.

239. A adequação das salvaguardas deve ser avaliada em função da sensibilidade dos dados e do âmbito, contexto, finalidade e natureza do tratamento (por exemplo, no caso da tomada de decisões automatizadas), bem como da probabilidade e gravidade dos riscos. Estas salvaguardas podem variar entre os sistemas jurídicos nacionais e dependem destes fatores. Uma lista não exaustiva de salvaguardas pode incluir a restrição do tratamento (por exemplo, permitindo o tratamento apenas para determinadas finalidades ou caso a caso), a limitação da divulgação, a restrição do acesso (por exemplo, a limitação do acesso apenas a determinado pessoal através de uma autorização especial ou procedimentos de autenticação que exijam formação especializada desse pessoal), medidas de segurança organizacionais ou técnicas adicionais (por exemplo, ocultação, pseudonimização ou separação do armazenamento de dados biométricos das informação biográficas conectadas) ou períodos de conservação mais curtos). Em determinados casos, pode ser útil realizar uma avaliação do impacto para ajudar a identificar e a gerir os riscos.

N.º 5 – Períodos de conservação

240. A primeira frase do n.º 5 prevê que "cada Parte conservará os dados pessoais apenas durante o tempo necessário e apropriado, tendo em conta as finalidades do tratamento dos dados nos termos do n.º 2". A este respeito, o princípio da limitação da finalidade previsto no n.º 2 estabelece que uma Parte que tenha recebido dados pessoais deve tratá-los para fins específicos, em conformidade com o artigo 2.º, e não proceder ao seu tratamento posterior para uma finalidade incompatível. Em conformidade com esse princípio, o período de conservação de dados está associado à(s) finalidade(s) específica(s) para a(s) qual(ais) os dados são tratados.

241. Uma vez que, ao abrigo do artigo 2.º, os dados pessoais recebidos por uma Parte nos termos do presente Protocolo se destinam a investigações ou processos penais específicos, os dados pessoais podem ser conservados enquanto for necessário: i) ao longo da duração da investigação e do processo subsequente, incluindo eventuais recursos ou períodos durante os quais um processo pode ser reaberto ao abrigo do direito interno, e ii) após o cumprimento da finalidade da recolha inicial, a continuação do tratamento para uma finalidade "não incompatível" com a finalidade original. Por exemplo, uma Parte pode prever que a informação ou os elementos

de prova sejam conservados para fins de arquivo ou de investigação histórica, ou para outros fins compatíveis, em conformidade com o artigo 14.º, n.º 2, tal como explicado nos números correspondentes do presente relatório explicativo.

242. A segunda frase do n.º 5 confere às Partes duas opções para cumprir a obrigação de conservação de dados pessoais apenas durante o tempo necessário e apropriado, tendo em conta as finalidades do tratamento dos dados nos termos da aplicação do n.º 2 do presente artigo. Em primeiro lugar, uma Parte pode prever períodos de conservação específicos no seu quadro jurídico interno. Em alternativa, as Partes podem prever, no seu quadro jurídico interno, a revisão da necessidade de uma conservação mais prolongada a intervalos previstos. As Partes dispõem de uma margem de apreciação para decidir qual a abordagem, no contexto do seu quadro jurídico interno, que melhor se adequa ao conjunto específico de dados. As Partes podem também combinar um período de conservação específico com um sistema de revisão periódica a intervalos mais curtos. Devem assegurar, no seu quadro jurídico, que as autoridades competentes elaboram regras e/ou procedimentos internos para a aplicação dos períodos de conservação específicos e/ou a revisão periódica da necessidade de uma conservação mais prolongada. Se o período de conservação tiver expirado ou se a Parte tiver determinado, através de revisão periódica, que não é necessário conservar os dados, estes devem ser apagados ou tornados anónimos.

N.º 6 – Decisões automatizadas

243. O n.º 6 diz respeito à proteção das pessoas singulares quando as decisões que produzam um efeito adverso significativo sobre os seus interesses pertinentes se baseiem exclusivamente no tratamento automatizado dos seus dados pessoais. Não se prevê que, quando uma Parte recebe dados pessoais de outra Parte ao abrigo do presente Protocolo, a tomada de decisões automatizadas esteja frequentemente envolvida, uma vez que os elementos de prova ou a informação serão recolhidos por investigadores ou autoridades judiciais para efeitos de uma investigação ou processo penal específico. No entanto, se a decisão automatizada, que produz um efeito adverso significativo sobre os interesses pertinentes da pessoa a quem os dados pessoais dizem respeito, ocorrer na investigação para a qual os dados foram solicitados, as autoridades devem seguir esta disposição. As autoridades devem também observar esta disposição se a utilização subsequente dos dados for efetuada para efeitos de prevenção, deteção, investigação ou repressão de outros crimes (por exemplo, detenção com base no tratamento exclusivamente automatizado de perfis criminosos, condenação, liberdade condicional), ou para uma finalidade compatível (por exemplo, no contexto de verificações de antecedentes), se os dados estiverem sujeitos a instrumentos de análise automatizados para efeitos de tomada de decisões.

244. Por conseguinte, o n.º 6 proíbe uma decisão baseada apenas no tratamento automatizado de dados pessoais quando produza um efeito adverso significativo sobre os interesses relevantes de uma pessoa, incluindo efeitos jurídicos adversos (que afetem o estatuto jurídico ou os direitos da pessoa singular), como a emissão de um mandado de detenção ou a recusa de liberdade condicional, a menos que tal tomada de decisão seja autorizada pelo direito interno e sujeita a salvaguardas apropriadas.

245. É essencial dispor de salvaguardas apropriadas para reduzir o potencial impacto sobre os interesses relevantes da pessoa a quem os dados pessoais dizem respeito. Essas salvaguardas devem abranger a possibilidade de a pessoa em causa obter intervenção humana para avaliar a decisão. As Partes são igualmente incentivadas a tomar medidas razoáveis para garantir a qualidade e a representatividade dos dados utilizados para desenvolver algoritmos e a exatidão das conclusões estatísticas utilizadas, tendo em conta as circunstâncias e o contexto específicos do tratamento, incluindo o contexto da aplicação do direito penal.

N.º 7 – Segurança dos dados e incidentes de segurança

246. Nos termos do n.º 7, alínea a), "cada Parte assegurará que dispõe de medidas tecnológicas, físicas e organizativas apropriadas para a proteção dos dados pessoais". Por exemplo, as medidas tecnológicas podem incluir software que proteja contra programas de *malware* informático, a encriptação de dados e *firewalls*. As medidas físicas podem incluir o armazenamento de servidores e ficheiros informáticos em locais seguros e as medidas

organizativas podem incluir regras, práticas, políticas e procedimentos, incluindo os que limitam os direitos de acesso.

247. O n.º 7, alínea a), prevê ainda que as medidas devem proteger, em especial, contra a perda (por exemplo, procedimentos normalizados de arquivo e tratamento de dados), o acesso acidental ou não autorizado (por exemplo, proteção contra intrusões informáticas, requisitos de autorização ou autenticação para aceder a ficheiros em papel ou ficheiros informáticos), a divulgação acidental ou não autorizada (por exemplo, medidas tecnológicas para detetar e prevenir divulgações acidentais ou não autorizadas e medidas organizativas para descrever as consequências dessas divulgações) e a alteração ou destruição acidental ou não autorizada dos dados (por exemplo, a restrição da introdução ou alteração de dados eletrónicos ou ficheiros em papel a pessoal autorizado, a utilização de sistemas de registo, a visualização de períodos de conservação, a instalação de sistemas de cópia de segurança em formato digital ou em papel).

248. A forma rigorosa de cumprir estes requisitos, de um modo apropriado às circunstâncias específicas, é deixada ao critério da Parte em causa. As Partes são incentivadas, por exemplo, a conceber e aplicar medidas de segurança que tenham em conta fatores como a natureza dos dados pessoais (incluindo a sua sensibilidade), os riscos identificados e quaisquer potenciais consequências adversas para a pessoa em causa em caso de incidente de segurança. Ao mesmo tempo, as Partes podem ter em conta as questões relativas aos recursos envolvidos na conceção e aplicação das medidas de segurança dos dados. As Partes são incentivadas a submeter essas medidas a revisões periódicas e a atualizá-las sempre que apropriado, tendo em conta o desenvolvimento da tecnologia e o caráter evolutivo dos riscos.

249. O n.º 7, alínea b), estabelece os requisitos em caso de "incidente de segurança" (tal como definido no n.º 7, alínea a), e acima descrito) no que diz respeito aos dados pessoais recebidos ao abrigo do presente Protocolo que criem um "risco significativo de danos físicos ou não físicos" para as pessoas singulares ou para a Parte de onde provêm os dados. Os danos relevantes para uma pessoa podem incluir, por exemplo, danos corporais ou reputacionais, sofrimento emocional (por exemplo, através de humilhação ou violação da confidencialidade), discriminação ou danos financeiros (por exemplo, perda de emprego ou de oportunidades profissionais, notação de crédito negativa, roubo de identidade ou potencial de chantagem). No que diz respeito à outra Parte, os danos relevantes podem incluir, em especial, o potencial impacto negativo numa investigação paralela (por exemplo, fuga do suspeito, destruição de elementos de prova). Se existir um "risco significativo" de tais danos, a Parte recetora tem a obrigação de "avaliar prontamente a probabilidade e a magnitude" dos danos e de "adotar prontamente as medidas apropriadas para mitigar esses danos". Os fatores relacionados com a probabilidade e a magnitude dos danos a considerar podem incluir, *inter alia*, o tipo de incidente, tal como, se conhecido, se foi malicioso, as pessoas que têm ou podem obter a informação, a natureza e a sensibilidade dos dados afetados, o volume de dados potencialmente comprometido e o número de pessoas potencialmente afetadas, a facilidade de identificação da(s) pessoa(s) em causa, a probabilidade de acesso e utilização dos dados, por exemplo, se os dados foram encriptados ou tornados de outro modo inacessíveis, e eventuais consequências que possam ocorrer em resultado do incidente.

250. Em conformidade com as medidas descritas no n.º 7, alínea a), e para assegurar uma resposta adequada nos termos do n.º 7, da alínea b), as Partes devem dispor de processos internos que lhes permitam detetar incidentes de segurança. Devem também dispor de um processo para avaliar rapidamente a probabilidade e a magnitude dos potenciais danos e para tomar rapidamente medidas apropriadas para mitigar os danos (por exemplo, recuperando ou solicitando a supressão de informação que tenha sido acidentalmente transmitida a um destinatário não autorizado). A aplicação efetiva destes requisitos pode beneficiar dos procedimentos internos de comunicação de informação e da manutenção de registos de qualquer incidente de segurança.

251. O n.º 7, alínea b), estabelece igualmente as circunstâncias em que a outra Parte e a(s) pessoa(s) afetada(s) devem ser notificadas do incidente, sob reserva de exceções e limitações.

252. No caso de um incidente de segurança em que exista um risco significativo de danos físicos ou não físicos para indivíduos ou para a outra Parte, a notificação deve ser enviada à autoridade que procede à transferência ou, para efeitos do Capítulo II, secção 2, à autoridade ou

autoridades designadas nos termos do n.º 7, alínea c). No entanto, a notificação pode incluir restrições apropriadas quanto à transmissão posterior da notificação, poderá ser adiada ou omitida quando essa notificação puder colocar em perigo a segurança nacional ou adiada quando essa notificação puder colocar em risco as medidas de proteção da segurança pública (incluindo quando a notificação possa pôr em perigo a investigação de infrações penais decorrentes do incidente de segurança). Ao decidir se uma notificação deve ser adiada ou omitida em circunstâncias em que a notificação possa pôr em perigo a segurança nacional, uma Parte deverá ponderar se será razoável, nas circunstâncias, omitir a notificação ou se, pelo contrário, será mais apropriada uma notificação diferida.

253. Em caso de um incidente de segurança em que exista um risco significativo de danos físicos ou não físicos para as pessoas singulares, deve ser igualmente enviada notificação à(s) pessoa(s) afetada(s) pelo incidente de modo a permitir-lhes protegerem os seus interesses, embora tal esteja sujeito a exceções. Em primeiro lugar, o n.º 7, alínea b), estabelece que não é necessário efetuar a notificação se a Parte tiver tomado medidas apropriadas para deixar de existir um risco significativo de danos. Por exemplo, não será necessária qualquer notificação se um e-mail com informação pessoal sensível for acidentalmente enviado ao destinatário errado e criar um risco significativo de danos sem medidas de mitigação, mas for rápida e permanentemente apagado pelo destinatário mediante pedido antes de ser novamente partilhado. Em segundo lugar, a notificação à pessoa singular pode ser adiada ou omitida nas condições estabelecidas no n.º 12, alínea a), ponto i) – ou seja, a notificação "pode estar sujeita à aplicação de restrições proporcionadas permitidas pelo seu quadro jurídico interno, necessárias... para proteger os direitos e as liberdades de terceiros ou objetivos importantes de interesse público geral e que tenham devidamente em conta os interesses legítimos da pessoa afetada".

254. Em geral, as Partes são incentivadas a incluir numa notificação nos termos do n.º 7, alínea b), se for caso disso, informação sobre o tipo de incidente de segurança, o tipo e o volume de informação que possa ter sido comprometido, os eventuais riscos e as medidas previstas para mitigar eventuais danos, incluindo medidas para conter o incidente. Tendo em conta a sua função de supervisão, e com vista a beneficiar de aconselhamento especializado sobre o tratamento do incidente, pode também ser adequado que a Parte notificante informe as autoridades de supervisão descritas no n.º 14 do incidente e de quaisquer medidas de mitigação.

255. Para permitir uma resposta coordenada e a apoiar nos seus próprios esforços de redução dos riscos, a Parte notificada poderá solicitar consultas e informação adicional sobre o incidente e a resposta ao mesmo.

256. O n.º 7, alínea c), prevê os procedimentos necessários para que as Partes designem a autoridade ou autoridades a notificar nos termos do n.º 7, alínea b), para efeitos do Capítulo II, secção 2.

N.º 8 – Manutenção de registos

257. O n.º 8 exige que as Partes "mantenham registos ou disponham de outros meios apropriados para demonstrar a forma como os dados pessoais de uma pessoa são acedidos, utilizados e divulgados num caso específico". O objetivo é que cada Parte disponha de meios eficazes para demonstrar a forma como os dados de uma pessoa específica foram acedidos, utilizados e divulgados num caso específico, em conformidade com este artigo. A demonstração do cumprimento é importante, em especial para efeitos de supervisão e, como tal, contribui para a responsabilização. Embora os meios precisos para demonstrar a forma como os dados são tratados sejam deixados ao critério de cada Parte, as Partes são incentivadas a adaptar os seus métodos às circunstâncias, tendo em conta os riscos para as pessoas em causa e a natureza, o âmbito, as finalidades e o contexto geral do tratamento.

258. Por exemplo, algumas Partes podem decidir utilizar o registo automático de atividades (registo) ou outras alternativas (como registos manuscritos no caso de ficheiros em papel). Tal como acima referido, o objetivo é facilitar a responsabilização, mas permitir um certo grau de flexibilidade quanto à forma como uma Parte o faz, em consonância com outras obrigações aplicáveis nos termos do artigo 14.º. Por exemplo, as Partes devem manter registos ou outra documentação sobre o acesso, a utilização ou a divulgação de informação de uma forma que

facilite o trabalho das autoridades de supervisão.

N.º 9 – Partilha ulterior no seio de uma Parte

259. O n.º 9 estabelece que "quando uma autoridade de uma Parte disponibilizar dados pessoais recebidos inicialmente ao abrigo do presente Protocolo a outra autoridade dessa Parte, essa outra autoridade procederá ao seu tratamento em conformidade com o presente artigo, sem prejuízo do disposto no n.º 9, alínea b)". Por outras palavras, sempre que os dados pessoais recebidos ao abrigo do presente Protocolo sejam posteriormente fornecidos a outra autoridade da mesma Parte – incluindo a uma autoridade de um Estado constituinte ou de outra entidade territorial similar – esses dados devem ser tratados em conformidade com o presente artigo, salvo se for aplicável a exceção prevista no n.º 9, alínea b). O n.º 9 é igualmente aplicável em caso de múltiplos casos de partilha ulterior.

260. O n.º 9, alínea b), prevê uma exceção ao n.º 9, alínea a), quando uma Parte que é um Estado federal tiver formulado uma reserva às obrigações decorrentes do presente Protocolo nos termos do artigo 17.º, em linha com as condições nele estabelecidas. Em conformidade com o n.º 297 do presente relatório explicativo, esta exceção tem em conta "as dificuldades que os Estados federais poderão enfrentar, em resultado da sua típica divisão de poderes entre as autoridades federais e regionais". Ver também o n.º 316 do relatório explicativo da Convenção. Por conseguinte, o n.º 9, alínea b), estabelece que, sempre que uma Parte tenha formulado uma reserva ao abrigo do artigo 17.º, pode ainda fornecer dados pessoais inicialmente recebidos ao abrigo do presente Protocolo aos seus Estados constituintes ou a outras entidades territoriais similares, desde que a Parte tenha adotado medidas para que as autoridades recetoras continuem a proteger eficazmente os dados, proporcionando um nível de proteção dos dados comparável ao previsto pelo presente artigo. O facto de uma Parte não ter "adotado medidas para que as autoridades recetoras continuem a proteger eficazmente os dados, proporcionando um nível de proteção dos dados comparável ao previsto pelo presente artigo" pode, em função da gravidade, dos motivos e das circunstâncias do incumprimento deste requisito, constituir uma violação substancial ou sistemática nos termos do artigo 14.º, n.º 15.

261. O n.º 9, alínea c), prevê que, em caso de indícios de aplicação incorreta do presente número por outra Parte, a Parte que transfere pode solicitar consultas com essa outra Parte e informação pertinente sobre essas indicações com vista a clarificar a situação.

N.º 10 – Transferência ulterior para outro Estado ou organização internacional

262. Nos termos do n.º 10, alínea a), uma Parte só poderá transferir dados pessoais recebidos ao abrigo do Protocolo "para outro Estado ou organização internacional mediante a autorização prévia da autoridade transmissora ou, para efeitos do Capítulo II, secção 2, da autoridade ou autoridades designadas no n.º 10, alínea b)". Este tipo de medida de proteção é uma condição comum para as transferências destinadas a prestar assistência a parceiros estrangeiros no contexto da aplicação da lei penal (por exemplo, ao abrigo de tratados de assistência mútua ou de cooperação policial), e esta abordagem é transposta para este número também como forma de proteger os dados pessoais transferidos ao abrigo do presente Protocolo.

263. O n.º 10, alínea b), prevê que cada Parte deverá, no momento da assinatura do presente Protocolo ou aquando do depósito do seu instrumento de ratificação, aceitação ou aprovação, comunicar ao Secretário-Geral do Conselho da Europa a autoridade ou autoridades designadas para conceder autorização nos termos do n.º 10, alínea a) para efeitos das transferências ao abrigo do Capítulo II, secção 2, que pode ser posteriormente alterada.

264. A obtenção de uma autorização para uma transferência ulterior pode implicar o envio de um pedido individualizado das autoridades da Parte recetora às autoridades da Parte que procede à transferência de dados pessoais especificamente identificados para um determinado país terceiro ou organização internacional. No entanto, o n.º 10, alínea a), não impede as Partes de preverem regras para transferências ulteriores (por exemplo, através de acordos escritos ou de outros convénios). O n.º 10, alínea a), também não prejudica a possibilidade de uma Parte impor outras condições à utilização dos dados pelo destinatário (por exemplo, a imposição de limitações quanto à medida em que a Parte recetora pode utilizar ou divulgar os dados pessoais

a fim de evitar prejudicar a investigação da Parte que os transfere), em conformidade com as disposições específicas do Capítulo II.

265. Ao determinar se concede autorização a uma transferência nos termos do n.º 10, a autoridade transmissora ou designada é incentivada a ter devidamente em conta todos os fatores pertinentes, incluindo a gravidade da infração penal, a finalidade para a qual os dados foram inicialmente transferidos, quaisquer condições aplicáveis à transferência original e se o país terceiro ou a organização internacional assegura um nível apropriado de proteção dos dados pessoais.

N.º 11 – Transparência e notificação

266. O n.º 11, alínea a), impõe determinados requisitos de transparência e de notificação às Partes no que diz respeito aos elementos especificados no n.º 11, alínea a), pontos i a iv). Estes requisitos de transparência e de notificação ajudam as pessoas a compreender a forma como as Partes podem tratar os seus dados. Estes requisitos também informam as pessoas sobre o acesso, a retificação e o recurso disponíveis.

267. Cada Parte tem flexibilidade quanto à questão de saber se essa notificação e transparência são asseguradas através da publicação de notificações gerais ao público – por exemplo, num sítio web governamental – ou através de uma notificação pessoal à pessoa cujos dados pessoais a Parte recebeu. As notificações devem ser acessíveis sem dificuldade e de compreensão fácil. Independentemente de ser fornecida uma notificação geral ou pessoal, deve ser incluída a seguinte informação: i) o fundamento jurídico do tratamento e a(s) finalidade(s) do tratamento, incluindo as finalidades das divulgações previstas ou habituais, ii) períodos de conservação ou de revisão nos termos do n.º 5 do presente artigo, conforme aplicável; iii) os destinatários ou categorias de destinatários a quem os dados são comunicados, e iv) acesso, retificação e vias de recurso judiciais e extrajudiciais disponíveis.

268. Nos termos do n.º 11, alínea b), quando a pessoa singular cujos dados a Parte recebeu é notificada, a notificação e o requisito de transparência previstos no n.º 11, alínea a), podem ser sujeitos a restrições razoáveis, de acordo com as condições estabelecidas no n.º 12, alínea a), ponto i) do presente artigo. Por exemplo, no contexto da justiça penal, podem existir circunstâncias legítimas em que a notificação pode ser adiada ou omitida. Estas circunstâncias são referidas no n.º 12, alínea a), ponto i) e descritas no n.º 272 do presente relatório explicativo. Podem também surgir situações em que o grau de pormenor indicado na notificação geral pode ser limitado, em função da sensibilidade da informação.

269. O n.º 11, alínea c), proporciona às Partes uma base para equilibrar o interesse da transparência com a necessidade de confidencialidade em matéria de justiça penal. Prevê que, sempre que o quadro jurídico interno da Parte que procede à transferência exigir a notificação pessoal da pessoa cujos dados foram disponibilizados a outra Parte ao abrigo do presente Protocolo, a Parte que procede à transferência adotará medidas para que a Parte recetora seja informada no momento da transferência sobre este requisito e os dados de contacto apropriados. A Parte que procede à transferência não notifica a pessoa singular se a Parte recetora tiver solicitado, caso sejam aplicáveis as condições de restrição previstas no n.º 12, alínea a), ponto i), que o fornecimento dos dados seja mantido confidencial. Logo que essas condições de restrições deixem de ser aplicáveis e a notificação pessoal possa ser realizada, a Parte recetora adotará medidas para que a Parte que procede à transferência seja informada de que a notificação se pode verificar. Tal pode incluir uma revisão periódica da necessidade de tais restrições. Se ainda não tiver sido informada, a Parte que procede à transferência tem o direito de apresentar pedidos à Parte recetora, que informará a Parte que procede à transferência da eventual manutenção da restrição.

N.º 12 – Acesso e retificação

270. O n.º 12, alínea a), exige que cada Parte assegure que qualquer pessoa cujos dados pessoais tenham sido recebidos ao abrigo do presente Protocolo tenha o direito de solicitar e obter, em conformidade com os procedimentos estabelecidos no seu quadro jurídico interno e sem demora indevida, o acesso a esses dados (sob reserva de eventuais restrições) e, caso esses dados

sejam inexatos ou tenham sido indevidamente tratados, a retificação. A expressão "em conformidade com os procedimentos estabelecidos no seu quadro jurídico interno" confere às Partes flexibilidade quanto ao modo como o acesso e a retificação podem ser solicitados e obtidos, e destina-se a remeter para os processos estabelecidos, por exemplo, nas leis, regulamentos, regras (como as regras de jurisdição) e políticas aplicáveis, bem como nas regras aplicáveis em matéria de provas. Em alguns sistemas jurídicos, um indivíduo terá de recorrer administrativamente ao acesso e à retificação antes de interpor recurso judicial.

271. O n.º 12, alínea a), ponto i) prevê que, no caso de um pedido de acesso, uma pessoa singular tem o direito de obter uma cópia escrita ou em formato eletrónico da documentação que contém os dados pessoais e a informação disponível, indicando o fundamento jurídico e a(s) finalidade(s) do tratamento, conservação e destinatários ou categorias de destinatários dos dados ("acesso"), bem como informação sobre as vias de recurso disponíveis nos termos do n.º 13. Tal pode igualmente permitir à pessoa em causa confirmar se os seus dados pessoais foram ou não recebidos ao abrigo do presente Protocolo e se foram ou estão a ser tratados. A apresentação de documentação que contenha a informação disponível que indique a base jurídica e a(s) finalidade(s) do tratamento ajudará a pessoa singular a avaliar se os dados pessoais estão a ser tratados em conformidade com a legislação aplicável. Muitas Partes podem já proporcionar um quadro para esse acesso através da sua privacidade, liberdade de informação ou acesso à legislação governamental em matéria de registos.

272. A possibilidade de obter esse acesso num caso específico pode estar sujeita a restrições proporcionadas, autorizadas ao abrigo do quadro jurídico interno de uma Parte, "necessárias, no momento da decisão, para proteger os direitos e as liberdades de terceiros ou objetivos importantes de interesse público geral e que tenham devidamente em conta os interesses legítimos da pessoa afetada". Os direitos e liberdades de terceiros podem, por exemplo, incluir a privacidade de outras pessoas cujos dados pessoais sejam revelados caso o acesso seja concedido. Os objetivos importantes de interesse público geral podem abranger, por exemplo, a proteção da segurança nacional e da segurança pública (por exemplo, informação sobre potenciais ameaças terroristas ou riscos graves para os funcionários responsáveis pela aplicação da lei), prevenção, deteção, investigação ou repressão de infrações penais, e evitar prejudicar os inquéritos, investigações e processos oficiais. À semelhança da descrição da proporcionalidade no n.º 146 do relatório explicativo da Convenção, cada Parte deverá aplicar "restrições proporcionadas" neste contexto, em conformidade com os princípios pertinentes do seu quadro jurídico interno. Para as Partes na Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (STCE n.º 5) ou no Protocolo STCE n.º 223 que altera a Convenção para a Proteção das Pessoas no que diz respeito ao Tratamento Automatizado de Dados Pessoais, a proporcionalidade decorrerá dos requisitos dessas convenções. As outras Partes aplicarão princípios conexos do seu quadro jurídico interno que limitem razoavelmente a capacidade de obter acesso para proteger outros interesses legítimos. Tal como acima referido, as restrições proporcionadas devem proteger os direitos e liberdades de terceiros ou proteger objetivos importantes de interesse público geral e ter devidamente em conta os "interesses legítimos da pessoa afetada". A expressão " interesses legítimos da pessoa afetada" foi considerada pelos redatores como incluindo os direitos e liberdades individuais. Caso sejam invocados esses motivos de restrição, a autoridade requerida é incentivada a documentar essa decisão para efeitos do n.º 14. As Partes devem também ponderar se pode ser concedido acesso parcial quando os motivos para qualquer restrição (por exemplo, para proteger informação comercial classificada ou confidencial) se aplicam apenas a determinadas partes da informação.

273. Sempre que outras disposições do presente artigo permitam restrições nas condições estabelecidas no n.º 12, alínea a), ponto i), "no momento da decisão" deve referir-se, no caso do n.º 7, ao momento da notificação de um incidente de segurança; no caso referido no n.º 11, alínea b), ao momento da notificação pessoal; e, no caso do n.º 11, alínea c), ao momento em que uma Parte solicita confidencialidade.

274. Nos termos do n.º 12, alínea a), ponto ii), cada Parte assegurará que qualquer pessoa, cujos dados tenham sido recebidos ao abrigo do presente Protocolo tem o direito de solicitar e obter, em conformidade com os procedimentos estabelecidos no seu quadro jurídico interno e sem demora indevida, a retificação dos seus dados pessoais quando esses dados forem inexatos ou tiverem sido indevidamente tratados. A retificação deverá incluir – conforme apropriado e razoável tendo em conta os motivos da retificação e o contexto específico do tratamento – a

correção, o complemento (por exemplo, através de uma referência ou do fornecimento de informação adicional ou corretiva), a supressão ou anonimização, a limitação do tratamento ou o bloqueio. A este respeito, os redatores consideraram que a supressão ou a anonimização são as medidas apropriadas e razoáveis se os dados forem tratados em violação do n.º 5. Em caso de violação do disposto no n.º 2, pode também ser apropriado que a Parte restrinja o tratamento; no entanto, tal dependerá, em última análise, do contexto específico (por exemplo, a necessidade de manter dados pessoais para efeitos de prova). Quando os dados são tornados anónimos, as Partes devem ter em conta o risco de reidentificação não autorizada e aplicar medidas apropriadas para minimizar esse risco. As Partes são incentivadas, sempre que possível, a notificar a Parte da qual os dados foram recebidos e outras entidades com as quais os dados tenham sido partilhados de quaisquer medidas corretivas tomadas.

275. De acordo com o n.º 12, alínea b), se o acesso ou a retificação for negado ou restringido nos termos do n.º 12, alínea a), a Parte fornecerá à pessoa em causa, por escrito que poderá ser por meios eletrónicos, sem demora indevida, uma resposta que a informe sobre a recusa ou a restrição. Embora a autoridade deva fundamentar essa recusa ou restrição, uma comunicação pode ser de caráter geral (ou seja, sem confirmar ou negar a existência de qualquer registo relevante), se tal for necessário para não comprometer um objetivo nos termos do n.º 12, alínea a), ponto i). No entanto, as Partes devem assegurar que a comunicação inclui informação sobre as vias de recurso disponíveis.

276. As Partes podem cobrar uma taxa pela obtenção de acesso (por exemplo, os custos administrativos da compilação e análise dos documentos aos quais foi solicitado acesso). No entanto, a fim de não dissuadir ou desencorajar o acesso, qualquer encargo deve limitar-se ao que é razoável e não excessivo, tendo em conta os recursos envolvidos. Para facilitar o exercício dos direitos previstos no n.º 12, alínea a), as Partes são incentivadas a autorizar as pessoas singulares a solicitarem a um representante que lhes preste assistência na procura e na obtenção das medidas nele descritas, ou a apresentarem um pedido e/ou uma denúncia em seu nome. Nessas circunstâncias, a comunicação nos termos do n.º 11, alínea a), bem como a informação obtida em resposta a um pedido de acesso nos termos do n.º 12, alínea a), ponto i), podem fazer referência a esta possibilidade. No entanto, essa representação deve estar em conformidade com os requisitos legais internos aplicáveis da Parte em que tais medidas são solicitadas ou o pedido e/ou a denúncia forem apresentados como acima descrito, incluindo as regras que regem as condições em que pessoas ou entidades podem representar os interesses jurídicos de outras pessoas ou entidades (por exemplo, em alguns ordenamentos jurídicos nacionais, as regras que regem a procuração).

N.º 13 – Recursos judiciais e extrajudiciais

277. O n.º 13 prevê que "cada Parte deverá dispor de vias de recurso judiciais e extrajudiciais eficazes para proporcionar reparação pelas violações do presente artigo". Cabe a cada Parte determinar o tipo de vias de recurso em caso de violação das disposições do presente artigo, não sendo necessário que cada tipo de medida corretiva esteja disponível para cada violação do presente artigo. As vias de recurso previstas devem ser eficazes para fazer face às violações do presente artigo. As Partes podem incluir uma indemnização como reparação, quando apropriado, por danos físicos ou não físicos que o requerente tenha demonstrado terem resultado da violação.

N.º 14 – Supervisão

278. O n.º 14 exige que as Partes disponham de "uma ou mais autoridades públicas que exerçam, individual ou cumulativamente, funções e poderes de supervisão independentes e eficazes no que diz respeito às medidas estabelecidas no presente artigo". A disposição deixa às Partes flexibilidade na forma de aplicar este requisito. Algumas Partes podem criar autoridades especializadas em matéria de proteção de dados, ao passo que outras podem optar por exercer a supervisão cumulativamente através de mais de uma autoridade, cujas funções podem sobrepor-se. Tal reflete as diferenças nas estruturas constitucionais, organizacionais e administrativas das Partes. Em algumas Partes, estas autoridades de supervisão podem existir inseridas em entidades governamentais cujas atividades supervisionam, podendo os respetivos orçamentos fazer parte do orçamento global da entidade. Nesse caso, estas autoridades devem usufruir de independência para desempenharem eficazmente as suas responsabilidades de supervisão.

279. Os redatores consideraram que vários elementos contribuem para funções e poderes de supervisão independentes e eficazes. As autoridades devem desempenhar as suas funções e exercer os seus poderes com imparcialidade, devem dispor de capacidade para agir sem influências externas que possam interferir com o exercício independente dos seus poderes e funções, em especial, essas autoridades não devem estar sujeitas a instruções, especificamente quanto ao exercício dos seus poderes de investigação e/ou à adoção de medidas corretivas, e por último, é importante que as autoridades disponham das competências, dos conhecimentos e das qualificações necessárias para desempenharem as suas funções e recebam os recursos financeiros, técnicos e humanos apropriados para o desempenho eficaz das suas funções.

280. As funções e poderes dessas autoridades incluem "poderes de investigação, o poder de dar seguimento a reclamações e a capacidade de tomar medidas corretivas". Os redatores consideraram que os poderes de investigação devem incluir o poder de obter a informação necessária para o desempenho das suas funções, incluindo, sob reserva de condições apropriadas, o acesso aos registos conservados nos termos do n.º 8. As medidas corretivas podem incluir a emissão de advertências por incumprimento ou instruções sobre a forma de tornar as operações de tratamento de dados conformes (por exemplo, exigindo a aplicação de medidas de segurança adicionais para limitar o acesso aos dados ou a retificação de dados pessoais), exigindo a suspensão (temporária) de determinadas operações de tratamento ou remetendo a questão para outras autoridades (por exemplo, inspetores gerais, procuradores do Ministério Público, juízes de instrução ou órgãos legislativos). Essas medidas corretivas podem ser tomadas por iniciativa própria das autoridades ou na sequência de reclamações apresentadas por pessoas singulares relativamente ao tratamento dos seus dados pessoais.

281. As Partes são incentivadas a promover a cooperação entre as respetivas autoridades de supervisão. Sempre que apropriado, podem realizar-se consultas entre as respetivas autoridades das Partes no exercício das suas funções de supervisão ao abrigo do presente artigo. Tal pode incluir o intercâmbio de informação e de boas práticas.

N.º 15 – Consulta e suspensão

282. O n.º 15 rege as situações em que, nos termos do artigo 14.º, uma Parte pode suspender a transferência de dados pessoais ao abrigo do presente Protocolo para outra Parte, quando as Partes estiverem a proceder nos termos do artigo 14.º, n.º 1, alínea a). O n.º 15 esclarece que, tendo em conta os importantes objetivos de aplicação da lei do presente Protocolo, tais suspensões só deverão ocorrer em condições estritas e de acordo com os procedimentos específicos nele descritos. O objetivo das disposições em matéria de proteção de dados do presente artigo é proporcionar salvaguardas apropriadas para a proteção de dados pessoais, incluindo em caso de partilha ulterior no seio de uma Parte e de transferências ulteriores. Os redatores consideraram que as salvaguardas deste artigo e a sua aplicação efetiva são fundamentais, pelo que consideraram importante prever a suspensão das transferências de dados pessoais em determinadas situações. Por conseguinte, uma Parte pode suspender a transferência de dados pessoais ao abrigo do presente Protocolo para outra Parte se dispuser de provas substanciais de violação sistemática ou material dos termos do presente artigo, ou de que está iminente uma violação material. Embora o requisito de "provas substanciais" não obrigue uma Parte a demonstrar de forma inequívoca uma violação sistemática ou material, também não pode suspender as transferências com base numa mera suspeita ou conjetura. Pelo contrário, a determinação da Parte deve ter um apoio substancial em elementos de prova factuais credíveis. Entende-se por "violação material" uma violação significativa de uma obrigação material nos termos do presente artigo. Tal pode incluir a ausência de uma salvaguarda necessária do presente artigo no quadro jurídico interno de uma Parte. Os redatores reconheceram que a suspensão também está disponível com base em violações sistemáticas – por exemplo, violações frequentes e recorrentes das salvaguardas deste artigo. Os redatores reconheceram ainda que a não aplicação de determinadas salvaguardas em relação ao tratamento de dados pessoais num caso concreto não constituirá, na ausência de uma violação material, um motivo suficiente para invocar esta disposição, uma vez que a pessoa em causa deve poder resolver tais violações através de vias de recurso extrajudiciais e judiciais, nos termos do artigo 14.º, n.º 13.

283. O n.º 15 prevê ainda que uma parte "não deverá suspender as transferências sem um pré-aviso razoável e apenas depois de as Partes interessadas terem iniciado um período razoável de consultas sem chegar a uma resolução". Este requisito de consulta reconhece que a suspensão das transferências críticas para efeitos de aplicação da lei só deve ser efetuada depois de ter dado à outra Parte uma oportunidade razoável para esclarecer a situação ou para dar resposta às preocupações manifestadas. No início dessa consulta, a Parte que invoca o n.º 15 pode solicitar à outra Parte que forneça a informação pertinente. No entanto, tal como reconhecido no n.º 15, a Parte que invoca o presente número deve dispor previamente de provas substanciais de uma violação material ou sistemática ou de uma violação material iminente; por conseguinte, o mecanismo de consulta não deve ser utilizado para recolher elementos de prova adicionais em caso de mera suspeita de violação. As transferências de dados ao abrigo do presente Protocolo só podem ser suspensas após um pré-aviso razoável e um período razoável de consulta sem que seja possível chegar a uma resolução. No entanto, uma Parte pode suspender provisoriamente as transferências em caso de violação sistemática ou material que constitua um risco significativo e iminente para a vida ou a segurança de uma pessoa singular, ou um risco significativo e iminente de danos substanciais para a sua reputação ou situação económica. Tal inclui um risco significativo e iminente de danos corporais ou para a saúde de uma pessoa singular. Nesses casos, a Parte notifica e inicia consultas com a outra Parte imediatamente após a suspensão provisória das transferências. Os redatores consideraram que a suspensão provisória deve, de um modo geral, limitar-se às transferências diretamente relacionadas com a necessidade que justifica a suspensão provisória.

284. Se a Parte que suspende satisfizer as condições estabelecidas no n.º 15, poderá suspender as transferências e a outra Parte não pode recorrer a reciprocidade. No entanto, se a outra Parte dispuser de provas substanciais de que a suspensão pela Parte que suspende era contrária ao disposto no n.º 15, pode, reciprocamente, suspender as transferências de dados para a Parte que suspende. Neste contexto, a expressão "provas substanciais" tem o mesmo significado que no que diz respeito à suspensão inicial pela Parte que suspende. A suspensão pela Parte que suspende será contrária ao disposto no n.º 15, por exemplo, se a Parte que suspende não dispuser de "provas substanciais", a violação não for "sistemática" nem "material" ou a Parte que suspende não satisfizer os requisitos processuais para a suspensão, em especial os relacionados com as consultas.

285. Por último, o n.º 15 prevê que "a Parte que suspende deverá levantar a suspensão logo que a infração que justifica a suspensão tenha sido corrigida" e que "qualquer suspensão recíproca será levantada nesse momento". É aplicável uma regra semelhante à aplicada no artigo 24.º, n.º 4, no contexto da suspensão ao abrigo do presente número. Ou seja, o n.º 15 prevê que "quaisquer dados pessoais transferidos antes da suspensão continuarão a ser tratados em conformidade com o presente Protocolo".

286. As Partes são incentivadas a tornar públicos ou a notificar formalmente os fornecedores de serviços e as entidades a quem podem ser dirigidos pedidos ou injunções ao abrigo da secção 2 do Capítulo II, de qualquer suspensão ou suspensão provisória ao abrigo do presente número. Essa comunicação pode ser importante para suspender efetivamente as transferências de dados pessoais para uma Parte que realize uma violação substancial ou sistemática do artigo 14.º, mas também para assegurar que os fornecedores de serviços e as entidades não restrinjam a transferência de informação ou elementos de prova ao abrigo do presente Protocolo com base na convicção errada de que uma Parte está sujeita a esta disposição de suspensão.

287. Embora o n.º 15 preveja procedimentos específicos relacionados com a consulta e a suspensão das transferências de dados pessoais por motivos de proteção de dados, os procedimentos previstos no n.º 15 não se destinam a afetar as consultas ao abrigo do artigo 23.º, n.º 1, nem os direitos de suspensão que possam ser aplicáveis ao abrigo do direito internacional em relação a outros artigos do presente Protocolo.

Capítulo IV - Disposições finais

288. As disposições contidas no presente capítulo baseiam-se essencialmente nas "Cláusulas finais tipo para as convenções, protocolos adicionais e protocolos de alterações celebrados no quadro do Conselho da Europa", as quais foram adotados pelo Comité de Ministros na 1291.ª reunião dos Delegados dos Ministros, realizada em fevereiro de 2017, bem como nas cláusulas finais da

Convenção. Dado que alguns dos artigos deste capítulo remetem para o texto das cláusulas-tipo ou são inspirados na longa prática de elaboração de Convenções do Conselho da Europa, não suscitam comentários específicos. No entanto, algumas alterações das cláusulas tipo normais e o desvio em relação às disposições finais da Convenção exigem alguma explicação.

Artigo 15.º – Efeitos do presente protocolo

289. O artigo 15.º, n.º 1, alínea a), incorpora o artigo 39.º, n.º 2, da Convenção. Tal como reconhecido no n.º 312 do relatório explicativo da Convenção, este número prevê que as Partes são livres de aplicar acordos já existentes ou que venham a entrar em vigor no futuro. O presente Protocolo, tal como a Convenção prevê, em geral, a existência de obrigações mínimas, por conseguinte, o presente número reconhece às Partes a liberdade de assumirem as obrigações que se revestem de uma maior especificidade, adicionalmente às obrigações já definidas pelo Protocolo, sempre que se trate de estabelecer as suas relações no que toca a questões abrangidas pela Convenção. No entanto, as Partes deverão respeitar os objetivos e os princípios do Protocolo, pelo que não poderão assumir obrigações que se revelem contrárias ou incompatíveis com os seus fins.

290. O n.º 1, alínea b), deste artigo reconhece igualmente a crescente integração da União Europeia (UE) desde que a Convenção foi aberta à assinatura em 2001, em especial nos domínios da aplicação da lei e da cooperação judiciária em matéria penal, bem como da proteção de dados. Por conseguinte, permite que os Estados-Membros da UE apliquem entre si o direito da União Europeia que rege as matérias tratadas no presente Protocolo. Os redatores pretenderam que o direito da União Europeia incluísse medidas, princípios e procedimentos previstos na ordem jurídica da UE, em especial disposições legislativas, regulamentares ou administrativas, bem como outros requisitos, incluindo decisões judiciais. O n.º 1, alínea b), destina-se, por conseguinte, a abranger as relações internas entre os Estados-Membros da UE e entre estes e as instituições, órgãos e agências da UE. Se não existir legislação da União Europeia relativa a uma matéria abrangida pelo âmbito de aplicação do presente Protocolo, o presente Protocolo continuará a reger essa questão entre as Partes que são Estados-Membros da UE.

291. O n.º 1, alínea c), esclarece que o n.º 1, alínea b), não afeta a plena aplicação do presente Protocolo entre as Partes que são membros da UE e outras Partes. O n.º 1, alínea b), não se destina, portanto, a produzir efeitos para além das relações internas da UE, tal como descritas no n.º 290, acima; o presente Protocolo é plenamente aplicável entre as Partes que são Estados-Membros da UE e outras Partes. Os redatores consideraram esta disposição essencial para garantir que as Partes que não são Estados-Membros da UE usufruem de todos os benefícios do presente Protocolo nas suas relações com as Partes que são Estados-Membros da UE. Por exemplo, os redatores debateram que um Estado-Membro da UE que receba informação ou elementos de prova de uma Parte não pertencente à UE terá de solicitar o consentimento da Parte não pertencente à UE antes de transferir a informação ou elementos de prova para outra Parte pertencente à UE, em conformidade com o artigo 14.º, n.º 10. Do mesmo modo, o n.º 1, alínea a), do presente artigo será plenamente aplicável entre as Partes que sejam Estados-Membros da UE e outras Partes que não o sejam.

292. O artigo 15.º, n.º 2, incorpora o artigo 39.º, n.º 3, da Convenção. À semelhança da Convenção, tal como explicado no n.º 314 do relatório explicativo da Convenção, o presente Protocolo não pretende abordar todas as questões pendentes relacionadas com as formas de cooperação entre as Partes ou entre as Partes e entidades privadas relacionadas com cibercrime e com a recolha de provas sob a forma eletrónica de infrações penais. Assim, foram introduzidas as disposições do artigo 15.º. n.º 2, a fim de tornar claro que o Protocolo abrange ou afeta apenas aquilo que nele é tratado. Permanecerão pois, inalterados todos os outros direitos, restrições, obrigações e responsabilidades, eventualmente existentes mas que não sejam tratados pelo presente Protocolo.

293. O artigo 15.º não contém uma disposição análoga à do artigo 39.º, n.º 1, da Convenção. Esta disposição da Convenção explicava que esta tinha por finalidade complementar os tratados ou convénios bilaterais aplicáveis entre as Partes, incluindo determinados tratados de extradição e de assistência mútua. O presente Protocolo não contém quaisquer disposições em matéria de extradição e tem muitas disposições que não são disposições relativas à assistência mútua. Tal como explicado mais pormenorizadamente no artigo 5.º no relatório explicativo que o

acompanha, cada secção das medidas de cooperação do Capítulo II interage de diferentes formas com os tratados de assistência mútua. Por conseguinte, os redatores concluíram que não necessitam de incluir uma disposição semelhante ao artigo 39.º, n.º 1.

Artigo 16° - Assinatura e entrada em vigor

294. O artigo 16.º permite que todas as Partes na Convenção assinem e se tornem Partes no presente Protocolo. Ao contrário do Primeiro Protocolo (artigo 11.º), este Protocolo não prevê um procedimento de adesão ao presente Protocolo. Um Estado que pretenda assinar e tornar-se Parte no presente Protocolo terá, primeiro, de se tornar Parte na Convenção.

295. O n.º 2 estabelece que o presente "Protocolo entrará em vigor no primeiro dia do mês seguinte ao termo de um período de três meses a contar da data em que cinco Partes na Convenção tenham expresso o seu consentimento em ficarem vinculadas pelo presente Protocolo". Embora a Convenção previsse, no artigo 36.º, n.º 3, que pelo menos três das cinco Partes tinham de ser Estados-Membros do Conselho da Europa para que a Convenção entrasse em vigor, tal requisito não é aqui incluído, uma vez que se trata de um protocolo adicional a uma convenção e que todas as Partes devem ter o mesmo direito de aplicar o presente Protocolo logo que um número mínimo de cinco Partes na Convenção tenha manifestado o seu consentimento em ficar vinculadas. Isto segue a abordagem do artigo 10.º do Primeiro Protocolo.

296. O n.º 4 descreve o processo de entrada em vigor do presente Protocolo para as Partes na Convenção que manifestem o seu consentimento em ficar vinculadas pelo presente Protocolo após a sua entrada em vigor nos termos do n.º 3. Tal segue a abordagem do artigo 36.º, n.º 4, da Convenção.

Artigo 17.º – Cláusula federal

297. À semelhança da cláusula federal prevista no artigo 41.º da Convenção, o artigo 17.º do presente Protocolo contém uma cláusula federal que permite a uma Parte que seja um Estado federal formular uma reserva "na medida em que seja compatível com os princípios fundamentais que governam as relações entre o seu governo central e os Estados federados, ou outras entidades territoriais análogas". O objetivo do artigo 17.º é o mesmo do artigo 41.º da Convenção. Ou seja, tal como referido no n.º 316 do relatório explicativo da Convenção, "para ter em conta as dificuldades que os Estados federais poderão enfrentar, em resultado da sua típica divisão de poderes entre as autoridades federais e regionais".

298. Os Estados federais podem formular uma reserva às obrigações previstas no Capítulo II da Convenção (determinação das infrações penais nacionais e das medidas processuais nacionais), na medida em que a sua regulamentação não seja da competência do governo central de um Estado federal. No entanto, os Estados federais devem poder prestar cooperação internacional a outras Partes nos termos do Capítulo III da Convenção.

299. Embora este Protocolo preveja a cooperação internacional e não medidas nacionais, os negociadores reconheceram que continua a ser necessária uma cláusula federal no presente Protocolo. Não obstante a Convenção não ter previsto qualquer reserva do federalismo para a assistência mútua, a maioria das medidas deste protocolo não funciona da mesma forma que a assistência mútua tradicional. O presente Protocolo prevê uma série de medidas de cooperação mais eficazes do que a assistência mútua tradicional e que não exigem necessariamente a participação do governo central. Em especial, o presente Protocolo introduz duas medidas, os artigos 6.º e 7.º, em que as autoridades competentes de uma Parte podem solicitar a cooperação diretamente a empresas privadas de outra Parte. Estas medidas exigem determinadas etapas processuais que um Estado federal pode ter dificuldade em exigir que as autoridades competentes dos Estados constituintes ou das entidades territoriais cumpram. Por exemplo, o artigo 7.º prevê que uma Parte pode, mediante notificação ao Secretário-Geral, exigir que as autoridades de outras Partes notifiquem simultaneamente uma autoridade governamental nomeada quando transmitem uma injunção a um fornecedor de serviços que procura obter informação sobre subscritores. Outros artigos contêm requisitos para a adoção de medidas legislativas ou outras que um Estado federal possa não poder exigir que os seus Estados constituintes ou outras entidades territoriais similares adotem. Por último, o presente Protocolo

contém disposições pormenorizadas em matéria de proteção de dados, ao passo que a Convenção não. Por exemplo, nos Estados Unidos, ao abrigo da sua Constituição e dos princípios fundamentais do federalismo, os Estados que os constituem adotam as suas próprias leis processuais criminais e penais (distintas das leis federais), estabelecem os seus próprios tribunais, procuradores e polícia, e investigam e instauram ações penais contra as infrações penais do Estado. As autoridades competentes do Estado são independentes e não estão subordinadas às autoridades federais.

300. Caso as autoridades de um Estado federal ou de uma entidade territorial similar procurem as formas de cooperação previstas no presente Protocolo, pode acontecer que: i) operem ao abrigo de leis processuais e de proteção da vida privada diferentes daquelas ao abrigo das quais operam as autoridades governamentais centrais, ii) não respondam ao governo central em termos de hierarquia organizativa, ou iii) o governo central não tenha competência jurídica para orientar as suas ações. Em tais situações, só poderá haver a garantia de que um Estado constituinte ou uma entidade territorial similar cumprirá os requisitos do presente Protocolo – os relacionados com a procura de informação ou elementos de prova, bem como os relacionados com o tratamento subsequente dessa informação ou elementos de prova – se: i) ele próprio os aplicar, ou ii) se as suas autoridades procurarem cooperar através ou com a participação de autoridades do governo central que asseguram o seu cumprimento (por exemplo, através de assistência mútua ou do ponto de contacto 24/7, ou com a participação do governo central numa equipa de investigação conjunta).

301. Tendo em conta estas considerações, o n.º 1 prevê uma possibilidade de formulação de reserva para as Partes que sejam Estados federais. Essas Partes podem reservar-se o direito de assumir as obrigações nos termos do presente Protocolo na medida em que sejam compatíveis com os seus princípios fundamentais que regem as relações entre o seu governo central e os seus Estados ou outras entidades territoriais análogas, sob reserva do n.º 1, alíneas a) a c), que limitam o âmbito de aplicação de tal reserva. Nos termos do n.º 1, alínea a), o governo central de um Estado federal que invoque esta reserva deve aplicar todas as disposições do presente Protocolo (sujeito às reservas e declarações disponíveis). No que diz respeito às obrigações em matéria de proteção de dados ao abrigo do presente Protocolo, para as Partes que procedem ao abrigo do artigo 14.º, n.º 1, alínea a), tal inclui as obrigações previstas no artigo 14.º, n.º 9, alínea b), relativas à partilha ulterior com Estados constituintes ou outras entidades territoriais similares (ver relatório explicativo, n.º 260), sempre que uma autoridade federal tenha solicitado informação ao abrigo do presente Protocolo, quer para as suas próprias finalidades, quer em nome de uma autoridade a nível subfederal, e partilhe posteriormente essas informação com essa autoridade a nível subfederal. Além disso, o n.º 1, alínea b), prevê que, à semelhança do artigo 41.º, n.º 1, da Convenção, essa reserva não afeta as obrigações desse Estado federal de disponibilizar a cooperação pretendida por outras Partes em conformidade com o disposto no Capítulo II. Por último, nos termos do n.º 1, alínea c), não obstante uma reserva de um Estado federal, o artigo 13.º do presente Protocolo – que exige, em conformidade com o artigo 15.º da Convenção, a proteção dos direitos humanos e das liberdades ao abrigo do direito interno – é aplicável aos Estados constituintes do Estado federal ou a entidades territoriais similares, para além do governo central, nos termos do n.º 1, alínea a).

302. O n.º 2 prevê que, se um Estado federal formular uma reserva ao abrigo do n.º 1 e as autoridades de um Estado constituinte ou de uma entidade territorial similar dessa Parte solicitarem a cooperação diretamente a uma autoridade, fornecedor ou entidade de outra Parte, essa outra Parte "poderá impedir as autoridades, fornecedores ou entidades no seu território de cooperarem em resposta". A outra Parte poderá determinar a forma de impedir a cooperação das suas autoridades, fornecedores ou entidades no seu território. Existem duas exceções ao poder de outra Parte de impedir a cooperação.

303. Em primeiro lugar, o n.º 2 prevê que a cooperação não pode ser impedida por essa outra Parte se, pelo facto de o Estado constituinte ou outra entidade territorial similar cumprir as obrigações do presente Protocolo, o Estado Federal em causa tiver "notificado o Secretário-Geral do Conselho da Europa de que um Estado constituinte ou outra entidade territorial similar aplica as obrigações do presente Protocolo aplicáveis a esse Estado federal". A expressão "obrigações do presente Protocolo aplicáveis a esse Estado federal" significa que uma autoridade de um Estado constituinte ou de uma entidade territorial similar não pode estar sujeita a qualquer requisito a que o governo central não esteja sujeito, por exemplo devido a uma reserva aplicável.

Se o Estado federal tiver apresentado essa notificação ao Secretário-Geral relativamente a um determinado Estado constituinte, a outra Parte é obrigada a disponibilizar a execução de uma injunção ou pedido desse Estado da mesma forma como se fosse recebido das autoridades do governo central. É evidente que os requisitos e procedimentos contidos em cada medida de cooperação prevista no Capítulo II continuam a aplicar-se aos pedidos ou injunções apresentados por esses Estados constituintes ou entidades territoriais similares, sendo necessário o cumprimento desses requisitos. Este número exige que o Secretário-Geral do Conselho da Europa crie e mantenha atualizado um registo dessas notificações. As Partes são incentivadas a fornecer ao Secretário-Geral informação atualizada.

304. Em segundo lugar, nos termos do n.º 3, se um pedido ou injunção de um Estado constituinte ou de outra entidade territorial similar tiver sido apresentado através do governo central ou, nos termos do artigo 12.º, ao abrigo de um acordo de equipa de investigação conjunta celebrado com a participação do governo central, a outra Parte não pode impedir as autoridades, fornecedores ou entidades no seu território de transferir informação ou elementos de prova nos termos do presente Protocolo, com base no facto de a cooperação ser solicitada por um Estado constituinte ou entidade territorial similar de um Estado federal que tenha formulado a reserva prevista no n.º 1. Com efeito, quando o pedido ou injunção é apresentado através do governo central ou quando o acordo de equipa de investigação conjunta é celebrado com a participação do governo central, é o governo central que é obrigado a "prever o cumprimento das obrigações aplicáveis do Protocolo". Uma vez que o governo central apresenta o pedido ou a injunção (ou participa na equipa de investigação conjunta), tem a oportunidade e a obrigação de verificar o cumprimento dos requisitos do presente Protocolo no que respeita a essas medidas. Por exemplo, se, nos termos do artigo 7.º, n.º 5, alínea a), outra Parte tiver de ser notificada da transmissão de uma injunção para obter informação sobre os subscritores, o governo central é obrigado a apresentar essa notificação. No que diz respeito à proteção de dados (para as Partes que atuam ao abrigo do artigo 14.º, n.º 1, alínea a), se um Estado ou outra entidade territorial similar solicitar a cooperação através do governo central, o governo central fornece os dados ao Estado constituinte ou a outra entidade territorial similar e deve aplicar os requisitos estabelecidos no artigo 14.º, n.º 9, alínea b) (partilha ulterior no seio de uma Parte). Ou seja, o governo central deve dispor de medidas para que as autoridades que recebem os dados continuem a proteger eficazmente os dados, prevendo um nível de proteção comparável ao proporcionado pelo artigo 14.º. As autoridades de um Estado constituinte ou de uma entidade territorial similar que procuram e recebem dados pessoais desta forma não são obrigadas a aplicar o artigo 14.º. Se as Partes em causa aplicarem outro acordo ou convénio descrito no artigo 14.º, n.º 1, alínea b) ou alínea c), são aplicáveis os termos desse acordo ou convénio.

305. O n.º 4 apresenta praticamente o mesmo texto e tem efeitos idênticos aos do artigo 41.º, n.º 3, da Convenção. Assim, no que diz respeito às disposições da Convenção cuja aplicação é da competência dos Estados constituintes ou de outras entidades territoriais similares (a menos que tenha sido enviada uma notificação ao Secretário-Geral do Conselho da Europa nos termos do n.º 2 do presente artigo), o governo central do Estado federal deve: i) informar as autoridades dos seus Estados constituintes ou outras entidades territoriais similares das disposições do presente Protocolo, e ii) dar "parecer favorável, incitando-os a adotar as medidas adequadas para as executar", o que incentiva os Estados constituintes ou entidades territoriais similares a aplicarem plenamente o presente Protocolo. Para efeitos do presente Protocolo, pretende-se igualmente permitir que os Estados constituintes ou outras entidades territoriais similares sejam notificados nos termos do n.º 2 do presente artigo.

Artigo 18° – Aplicação territorial

306. O artigo 38.º da Convenção permite que as Partes especifiquem o território ou territórios aos quais a Convenção se aplica. O artigo 18.º do presente Protocolo aplica automaticamente o este Protocolo a territórios especificados numa declaração realizada por uma Parte nos termos do artigo 38.º, n.º 1 ou 2, da Convenção, na medida em essa declaração não tenha sido levantada nos termos do artigo 38.º, n.º 3, da Convenção. Os redatores consideraram que seria preferível que o mesmo âmbito de aplicação territorial da Convenção e do presente Protocolo fosse aplicado como regra geral.

307. O n.º 2 do presente artigo prevê que "uma Parte poderá, no momento da assinatura do presente Protocolo ou aquando do depósito do seu instrumento de ratificação, aceitação ou aprovação,

declarar que o presente Protocolo não será aplicável a um ou mais territórios especificados na declaração da Parte nos termos do artigo 38.º, n.º 1 e/ou 2 da Convenção. Nos termos do n.º 3, as Partes podem retirar a declaração prevista no n.º 2 do presente artigo, de acordo com os procedimentos especificados. A retirada da declaração referida no n.º 2 terá por efeito a aplicação do presente Protocolo a territórios adicionais abrangidos pela Convenção, mas aos quais o presente Protocolo não tinha sido anteriormente aplicado.

308. Este artigo não permite a aplicação do presente Protocolo a territórios não abrangidos pela Convenção.

Artigo 19° – Reservas e declarações

309. O presente artigo prevê um conjunto de situações nas quais é possível formular uma reserva. Tendo em conta o alcance global da Convenção e o objetivo de alcançar o mesmo nível de adesão ao presente Protocolo, essas reservas permitem que as Partes na Convenção se tornem Partes no presente Protocolo, ao mesmo tempo que lhes permite manter determinadas abordagens e conceitos compatíveis com o seu direito interno, princípios jurídicos fundamentais ou considerações políticas, conforme aplicável.

310. As possibilidades de reservas são limitadas a fim de assegurar, tanto quanto possível, a aplicação uniforme do presente Protocolo pelas Partes. Assim, não podem ser formuladas outras reservas para além das enumeradas. Além disso, uma Parte na Convenção só pode formular reservas no momento da assinatura do presente Protocolo ou após o depósito do seu instrumento de ratificação, aceitação ou aprovação.

311. Tal como na Convenção, as reservas ao presente Protocolo excluem ou alteram o efeito jurídico das obrigações estabelecidas no presente Protocolo (ver n.º 315 do relatório explicativo da Convenção). No presente Protocolo, é permitido que as reservas excluam todas as formas de cooperação. Especificamente, o artigo 7.º, n.º 9, alínea a), permite que uma Parte se reserve o direito de não aplicar o artigo 7.º na sua totalidade. É igualmente permitido que as reservas excluam a cooperação relativa a artigos completos no que diz respeito a determinados tipos de dados. Especificamente, o artigo 7.º, n.º 9, alínea b), permite que uma Parte se reserve o direito de não aplicar o artigo 7.º a certos tipos de números de acesso se a divulgação desses números de acesso for incompatível com os princípios fundamentais da sua ordem jurídica interna. Do mesmo modo, o artigo 8.º, n.º 13, permite que uma Parte se reserve o direito de não aplicar o artigo 8.º aos dados de tráfego.

312. O artigo 19.º faz igualmente referência às declarações. À semelhança da Convenção, através de declarações no presente Protocolo, as Partes estão autorizadas a incluir determinados procedimentos adicionais específicos que alteram o âmbito de aplicação das disposições. Esses procedimentos adicionais visam ter em conta certas diferenças conceptuais, jurídicas ou práticas, que se justificam tendo em conta o alcance global da Convenção e a aspiração ao mesmo alcance do presente Protocolo. As declarações enumeradas dividem-se em duas categorias gerais.

313. Várias declarações permitem a uma Parte declarar que determinados poderes ou medidas devem ser executados por autoridades específicas ou por uma cooperação transmitida através de canais específicos. É o caso do artigo 10.º, n.º 9 (que permite uma declaração de que os pedidos podem ser enviados às autoridades para além da autoridade central), do artigo 12.º, n.º 3 (a autoridade central deve ser signatária ou de outra forma aceitar o acordo de equipas de investigação conjuntas), do artigo 8.º, n.º 11 (uma Parte declarante pode exigir que os pedidos de outras Partes ao abrigo do presente artigo sejam transmitidos pelas respetivas autoridades centrais ou por outra autoridade mutuamente determinada).

314. Uma segunda categoria de declarações permite que as Partes exijam medidas processuais separadas ou adicionais para determinadas medidas de cooperação, a fim de dar cumprimento ao direito interno ou evitar sobrecarregar as autoridades. Por exemplo, o artigo 7.º, n.º 8, e o artigo 9.º, n.º 1, alínea b), permitem que uma Parte faça declarações para exigir que as outras Partes tomem medidas processuais específicas no que diz respeito à informação dos subscritores. O artigo 7.º, n.º 2, alínea b), e n.º 5, alínea a), o artigo 8.º, n.º 4, e o artigo 9.º, n.º 5,

permitem medidas processuais adicionais para prever salvaguardas adicionais ou para cumprir o direito interno. Os efeitos das declarações não se destinam a ser recíprocos. Por exemplo, se uma Parte apresentar uma declaração nos termos do artigo 10.º, n.º 9 – ou seja, que os pedidos ao abrigo do presente artigo podem ser enviados a autoridades para além da sua autoridade central – as outras Partes podem dirigir pedidos às autoridades adicionais da Parte declarante, mas a Parte declarante só pode dirigir pedidos às autoridades centrais de outras Partes, a menos que também apresentem essa declaração.

315. As declarações enumeradas no n.º 2 do presente artigo devem ser apresentadas no momento da assinatura de uma Parte ou aquando do depósito do seu instrumento de ratificação, aceitação ou aprovação. Em contrapartida, as declarações referidas no n.º 3 podem ser apresentadas a qualquer momento.

316. O n.º 3 exige que as Partes notifiquem o Secretário-Geral do Conselho da Europa de quaisquer declarações, notificações ou comunicações referidas no artigo 7.º, n.º 5, alíneas a) e e), no artigo 8.º, n.º 4 e n.º 10, alíneas a) e b), no artigo 14.º, n.º 7, alínea c), e n.º 10, alínea b), e no artigo 17.º, n.º 2, do presente Protocolo, nos termos especificados nesses artigos. Por exemplo, nos termos do artigo 7.º, n.º 5, alínea e), uma "Parte deverá, no momento da primeira notificação ao Secretário-Geral do Conselho da Europa comunicar-lhe os dados de contacto dessa autoridade".

Além disso, as Partes devem comunicar ao Secretário-Geral do Conselho da Europa, as "autoridades" referidas no artigo 8.º, n.º 10, alíneas a) e b). O Secretário-Geral foi incumbido de criar e manter atualizado um registo dessas autoridades nomeadas pelas Partes e as Partes são instruídas no sentido de assegurar que os dados que fornecem para o registo são sempre corretos (ver artigo 7.º, n.º 5, alínea f), e artigo 8.º, n.º 12).

Artigo 20.º – Estatuto e levantamento de reservas

317. Tal como o artigo 43.º da Convenção, este artigo, sem impor prazos específicos, exige que as Partes retirem as reservas logo que as circunstâncias o permitam. A fim de poder exercer alguma pressão sobre as Partes para que estas, pelo menos, ponderem a revogação das suas reservas, o n.º 2 autoriza o Secretário Geral do Conselho da Europa a, periodicamente, inquirir as Partes relativamente às perspetivas de revogação das reservas formuladas. Esta possibilidade de inquirir as Partes constitui uma prática corrente no quadro de diversos instrumentos do Conselho da Europa e reflete-se no artigo 43.º, n.º 3, da Convenção e no artigo 13.º, n.º 2. do Primeiro Protocolo. As Partes poderão, assim, indicar as reservas que, do seu ponto de vista, se impõe que sejam mantidas relativamente a determinadas disposições, bem como a retirar posteriormente as reservas cuja necessidade já não se justifica. Espera-se que, com o decorrer do tempo, as Partes estejam em posição de retirar o maior número possível de reservas, de modo a favorecer uma implementação uniforme do presente Protocolo.

Artigo 21.º – Aditamentos

318. O artigo 21.º segue o mesmo procedimento que o previsto para as alterações do artigo 44.º da Convenção. Este procedimento simplificado permite alterações sem necessidade de negociação de um protocolo de alteração, se necessário. Considera-se que os resultados das consultas com as Partes na Convenção nos termos do n.º 3 do presente artigo não são vinculativos para as Partes no Protocolo. Tal como indicado no n.º 323 do relatório explicativo da Convenção, "considera-se que o processo de modificação é, essencialmente, aplicável a alterações pouco significativas de caráter técnico e processual".

Artigo 22.º – Resolução de litígios

319. O artigo 22.º prevê que os mecanismos de resolução de litígios previstos no artigo 45.º da Convenção se aplicam igualmente a este Protocolo (ver o n.º 326 do relatório explicativo da Convenção).

Artigo 23.º – Consultas das Partes e avaliação da aplicação

320. O artigo 23.º, n.º 1, prevê que o artigo 46.º da Convenção (Consultas das Partes) é aplicável ao

presente Protocolo. De acordo com o n.º 327 do relatório explicativo da Convenção, o artigo 46.º criou "uma estrutura de consulta das Partes no que refere à implementação da Convenção, às repercussões dos desenvolvimentos importantes verificados no plano jurídico, político ou tecnológico relativamente à questão da criminalidade informática ou relacionada com computadores e à recolha de provas sob a forma eletrónica, bem como à possibilidade de complemento e modificação da Convenção". O processo foi concebido para ser flexível, na medida em que caberá às Partes a decisão sobre a forma e o momento de se reunirem. Na sequência da entrada em vigor da Convenção em 2004, as Partes começaram a reunir-se regularmente como "Comité da Convenção sobre o Cibercrime" (T-CY). Ao longo do tempo, o T-CY, criado nos termos do artigo 46.º com base no Regulamento Interno adotado pelas Partes na Convenção, procedeu a avaliações da aplicação da Convenção pelas Partes, adotou notas de orientação para facilitar um entendimento comum das Partes quanto à utilização da Convenção e preparou o projeto do presente Protocolo. Os procedimentos para as consultas das Partes continuam a ser flexíveis e podem, por conseguinte, ser adaptados pelas Partes no presente Protocolo, conforme apropriado, para ter em conta as necessidades que possam surgir da aplicação do presente Protocolo.

321. À semelhança da Convenção (ver n.º 327 do relatório explicativo), as consultas ao abrigo do artigo 23.º deverão "analisar as questões decorrentes da utilização e implementação da Convenção, entre as quais se contam os efeitos das declarações e das reservas apresentadas". Tal poderá incluir consultas e a avaliação da aplicação do presente Protocolo pelos Estados constituintes ou entidades territoriais similares de Estados federais notificados ao Secretário-Geral do Conselho da Europa nos termos do artigo 17.º, n.º 2, e que as Partes que são membros da UE informem e consultem outras Partes no presente Protocolo sobre a legislação aplicável da UE no que respeita à sua utilização e aplicação do presente Protocolo no tocante ao artigo 15.º, n.º 1, alínea b). Para além das consultas realizadas no âmbito do T-CY ao abrigo do presente artigo, as Partes podem iniciar consultas numa base bilateral. Para os Estados federais, estas consultas e avaliações serão realizadas através do seu governo central.

322. O artigo 23.º, n.º 2, estabelece procedimentos específicos para a avaliação da utilização e aplicação do Protocolo no âmbito do quadro mais abrangente estabelecido pelo artigo 46.º do Tratado e pelo T-CY acima referido. O n.º 2 prevê que "as partes avaliarão periodicamente a utilização e aplicação efetivas das disposições do presente Protocolo" e indica que estas avaliações serão regidas pelo artigo 2.º do Regulamento Interno estabelecido pelo T-CY, com a redação que lhe foi dada em 16 de outubro de 2020. Estes procedimentos estão disponíveis no sítio web do T-CY. Uma vez que o T-CY avaliou várias disposições da Convenção e emitiu relatórios em conformidade com estes procedimentos, os redatores consideraram que estes procedimentos bem estabelecidos se devem aplicar *mutatis mutandis* à avaliação das disposições do presente Protocolo. À luz das obrigações adicionais assumidas pelas Partes no presente Protocolo e das medidas de cooperação únicas nele previstas, os redatores determinaram que apenas as Partes no presente Protocolo procederão a essas avaliações. Tendo em conta os conhecimentos especializados necessários para avaliar a utilização e a aplicação de algumas das disposições do presente Protocolo, nomeadamente no que se refere ao artigo 14.º relativo à proteção de dados, as Partes podem considerar a possibilidade de envolver peritos na matéria nas avaliações.

323. Embora, por um lado, as regras para essas avaliações tenham de ser previsíveis, a experiência real pode levar à necessidade de adaptar esses procedimentos, sem que seja necessária uma alteração formal do presente Protocolo em conformidade com o artigo 21.º. Por conseguinte, o n.º 2 estabelece que a avaliação inicial dos procedimentos terá lugar cinco anos após a entrada em vigor do presente Protocolo, momento em que as Partes podem alterar esses procedimentos por consenso. As Partes podem alterar os procedimentos por consenso em qualquer momento após essa avaliação inicial.

324. Dada a relevância das salvaguardas em matéria de proteção de dados previstas no artigo 14.º, os redatores consideraram que o artigo 14.º deverá ser avaliado logo que haja um registo suficiente da cooperação ao abrigo do presente Protocolo para avaliar eficazmente a utilização e a aplicação desta disposição pelas Partes. Por conseguinte, a avaliação do artigo 14.º terá início logo que dez Partes na Convenção tenham manifestado o seu consentimento em ficar vinculadas pelo presente Protocolo.

Artigo 47.º – Denúncia

325. Os n.os 1 e 2 do artigo 24.º são semelhantes aos do artigo 47.º da Convenção e não requerem mais explicações. O n.º 3 estabelece que "a denúncia da Convenção por uma Parte no presente Protocolo constitui uma denúncia do presente Protocolo". Dada a ênfase dada pelo presente Protocolo à partilha de informação ou de elementos de prova, que podem incluir dados pessoais, os redatores consideraram prudente aditar o n.º 4 para clarificar que "a informação ou elementos de prova transferidos antes da data efetiva da denúncia continuarão a ser tratados em conformidade com o presente Protocolo".