CONVENÇÃO SOBRE O CIBERCRIME

PROTOCOLO RELATIVO À INCRIMINAÇÃO DE ACTOS DE NATUREZA RACISTA E XENÓFOBA

SEGUNDO PROTOCOLO RELATIVO AO REFORÇO DA COOPERAÇÃO E DA DIVULGAÇÃO DE PROVAS SOB A FORMA ELETRÓNICA

Relatórios explicativos e
Notas de orientação

www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

CONVENÇÃO SOBRE O CIBERCRIME

PROTOCOLO RELATIVO À INCRIMINAÇÃO DE ACTOS DE NATUREZA RACISTA E XENÓFOBA

SEGUNDO PROTOCOLO RELATIVO AO REFORÇO DA COOPERAÇÃO E DA DIVULGAÇÃO DE PROVAS SOB A FORMA ELETRÓNICA

Relatórios explicativos e
Notas de orientação

Conselho da Europa

Capa e layout: Documentos e Departamento de Produção de Publicações (DPDP), Conselho da Europa

Impresso no Conselho da Europa

Índice

Convenção sobre o cibercrime (STE No. 185)

Preâmbulo

Os Estados membros do Conselho da Europa e os seguintes Estados signatários,

Considerando que o objectivo do Conselho da Europa é realizar uma união mais estreita entre os seus membros;

Reconhecendo a importância de intensificar a cooperação com os outros Estados Partes da presente Convenção;

Convictos da necessidade de prosseguir, com carácter prioritário, uma política criminal comum, com o objectivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adopção de legislação adequada e da melhoria da cooperação internacional;

Conscientes das profundas mudanças provocadas pela digitalização, pela convergência e pela globalização permanente das redes informáticas;

Preocupados com o risco de que as redes informáticas e a informação electrónica, sejam igualmente utilizadas para cometer infracções criminais e de que as provas dessas infracções sejam armazenadas e transmitidas através dessas redes;

Reconhecendo a necessidade de uma cooperação entre os Estados e a indústria privada no combate à cibercriminalidade, bem como a necessidade de proteger os interesses legítimos ligados ao uso e desenvolvimento das tecnologias da informação;

Acreditando que uma luta efectiva contra a cibercriminalidade requer uma cooperação internacional em matéria penal acrescida, rápida e eficaz;

Convictos de que a presente Convenção é necessária para impedir os actos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta de desses sistemas, redes e dados, assegurando a incriminação desses comportamentos tal como descritos na presente Convenção, e da adopção de

poderes suficientes para combater eficazmente essas infracções, facilitando a detecção, a investigação e o procedimento criminal relativamente às referidas infracções, tanto ao nível nacional como internacional, e estabelecendo disposições materiais com vista a uma cooperação internacional rápida e fiável;

Tendo presente a necessidade de garantir um equilíbrio adequado entre os interesses da aplicação da lei e o respeito pelos direitos fundamentais do ser humano, tal como garantidos pela Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa de 1950, pelo Pacto Internacional sobre os Direitos Civis e Políticos das Nações Unidas de 1966, bem como por outros tratados internacionais aplicáveis em matéria de direitos do Homem, que reafirmam o direito à liberdade de opinião sem qualquer ingerência, o direito à liberdade de expressão, incluindo a liberdade de procurar, de receber e transmitir informações e ideias de qualquer natureza sem considerações de fronteiras e, ainda, o direito ao respeito pela vida privada;

Tendo igualmente presente o direito à protecção de dados pessoais, tal como é conferido, por exemplo, pela Convenção do Conselho da Europa de 1981, para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal;

Considerando a Convenção das Nações Unidas sobre os Direitos da Criança de 1989, e a Convenção da Organização Internacional do Trabalho sobre as Piores Formas do Trabalho Infantil de 1999;

Tendo em conta as convenções existentes do Conselho da Europa sobre a cooperação em matéria penal, bem como outros tratados similares celebrados entre os Estados membros do Conselho da Europa e outros Estados, e sublinhando que a presente Convenção tem por finalidade complementar as referidas convenções, de modo a tornar mais eficazes as investigações e as acções penais relativas a infracções penais relacionadas com sistemas e dados informáticos, bem como permitir a recolha de provas em forma electrónica de uma infracção penal;

Saudando os recentes desenvolvimentos destinados a aprofundar o entendimento e cooperação internacionais no combate à criminalidade no ciberespaço, nomeadamente, as acções empreendidas pelas Nações Unidas, pela OCDE, pela União Europeia e pelo G8;

Recordando as Recomendações do Comité de Ministros N.º R (85) 10 relativa à aplicação prática da Convenção Europeia sobre Auxílio Judiciário Mútuo em Matéria Penal quanto às cartas rogatórias para a intercepção de

telecomunicações, N.º R (88) 2 sobre as medidas destinadas a combater a pirataria no domínio do direito de autor e dos direitos conexos, N.º R (87) 15 que regula a utilização de dados de carácter pessoal no sector da polícia, N.º R (95) 4 relativa à protecção dos dados de carácter pessoal no sector das telecomunicações, tendo em conta, designadamente os serviços telefónicos e a N.º R (89) 9 sobre a criminalidade informática que estabelece directrizes para os legisladores nacionais respeitantes à definição de certos crimes informáticos e, ainda, a N.º R (95) 13 relativa a problemas processuais penais relacionados com as tecnologias da informação;

Tendo em conta a Resolução n.º 1 adoptada pelos Ministros Europeus da Justiça na sua 21ª Conferência (Praga, 10 e 11 de Junho de 1997), que recomenda ao Comité de Ministros para apoiar o trabalho desenvolvido pelo Comité Europeu para os Problemas Criminais (CDPC) sobre a cibercriminalidade a fim de aproximar as legislações penais nacionais e de permitir a utilização de meios de investigação eficazes em matéria de crimes informáticos, bem como a Resolução n.º 3, adoptada na 23ª Conferência dos Ministros Europeus da Justiça (Londres, 8 e 9 de Junho de 2000), que incentiva as partes intervenientes nas negociações a prosseguirem os seus esforços para encontrar soluções apropriadas que permitam o maior número possível de Estados a tornarem-se Partes da Convenção e reconhece a necessidade de dispor de um mecanismo rápido e eficaz de cooperação internacional, que tenha devidamente em conta as exigências específicas da luta contra a cibercriminalidade;

Tendo igualmente em conta o Plano de Acção adoptado pelos Chefes de Estado e de Governo do Conselho da Europa, por ocasião da sua Segunda Cimeira (Estrasburgo, 10 e 11 de Outubro de 1997), para procurar respostas comuns face ao desenvolvimento das novas tecnologias da informação, com base nas normas e princípios do Conselho da Europa;

Acordaram no seguinte:

Capítulo I –Terminologia

Artigo 1º - Definições

Para os fins da presente Convenção:

a. "Sistema informático" significa qualquer dispositivo isolado ou grupo de dispositivos relacionados ou interligados, em que um ou mais de entre eles, desenvolve, em execução de um programa, o tratamento automatizado dos dados;

b. "Dados informáticos" significa qualquer representação de factos, de informações ou de conceitos sob uma forma susceptível de processamento num sistema de computadores, incluindo um programa, apto a fazer um sistema informático executar uma função;

c. "Fornecedor de serviço" significa:

i. Qualquer entidade pública ou privada que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático e

ii. Qualquer outra entidade que processe ou armazene dados informáticos em nome do referido serviço de comunicação ou dos utilizadores desse serviço.

d. "Dados de tráfego" significa todos os dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.

Capítulo II – Medidas a tomar a nível nacional

Secção 1 – Direito penal material

Título 1 – Infracções contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos

Artigo 2º - Acesso ilegítimo

Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, o acesso intencional e ilegítimo à totalidade ou a parte de um sistema informático. As Partes podem exigir que a infracção seja cometida com a violação de medidas de segurança, com a intenção de obter dados informáticos ou outra intenção ilegítima, ou que seja relacionada com um sistema informático conectado a outro sistema informático.

Artigo 3º - Intercepção ilegítima

Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, a intercepção intencional e ilegítima de dados informáticos, efectuada por meios técnicos,

em transmissões não públicas, para, de ou dentro de um sistema informático, incluindo emissões electromagnéticas provenientes de um sistema informático que veicule esses dados. As Partes podem exigir que a infracção seja cometida com dolo ou que seja relacionada com um sistema informático conectado com outro sistema informático.

Artigo 4º - Interferência em dados

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, o acto de intencional e ilegitimamente danificar, apagar, deteriorar, alterar ou eliminar dados informáticos.

2. Uma Parte pode reservar-se o direito de exigir que a conduta descrita no n.º 1 provoque danos graves.

Artigo 5º - Interferência em sistemas

Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, a obstrução grave, intencional e ilegítima, ao funcionamento de um sistema informático, através da introdução, transmissão, danificação, eliminação, deterioração, modificação ou supressão de dados informáticos.

Artigo 6º - Uso abusivo de dispositivos

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracções penais, em conformidade com o seu direito interno, quando cometidas intencional e ilegitimamente:

a. A produção, a venda, a obtenção para utilização, a importação, a distribuição, ou outras formas de disponibilização de:

   i. Um dispositivo, incluindo um programa informático, concebido ou adaptado essencialmente para permitir a prática de uma das infracções definidas em conformidade com os artigos 2º a 5º;

   ii. Uma palavra-passe, um código de acesso ou dados informáticos semelhantes que permitam aceder a todo, ou a parte de um sistema informático

com a intenção de serem utilizados para cometer qualquer uma das infracções definidas nos Artigos 2º a 5º; e

b. A posse de um elemento referido nos alínea a), i. ou ii., com a intenção de ser utilizado com o objectivo de cometer qualquer uma das infracções referidas nos artigos 2º a 5º. As Partes podem exigir que no direito interno se reuna um certo número desses elementos para que seja determinada a responsabilidade criminal.

2. O presente artigo não deve ser interpretado como impondo responsabilidade criminal quando a produção, a venda, a aquisição para utilização, a importação, a distribuição, ou outra forma de disponibilização ou posse, mencionadas no n.º1 do presente artigo não tenham por objectivo cometer uma infracção estabelecida em conformidade com os artigos 2º a 5º da presente Convenção, como é o caso de ensaios autorizados ou de protecção de um sistema informático.

3. Cada Parte pode reservar-se o direito de não aplicar o disposto no n.º 1 do presente artigo desde que essa reserva não diga respeito à venda, distribuição, ou a qualquer outra forma de disponibilização dos elementos referidos no n.º 1, *a)*, *ii.*

Título 2 – Infracções relacionada com computadores

Artigo 7º - Falsidade informática

Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, a introdução, a alteração, a eliminação ou a supressão intencional e ilegítima de dados informáticos, produzindo dados não autênticos, com a intenção de que estes sejam considerados ou utilizados para fins legais como se fossem autênticos, quer sejam ou não directamente legíveis e inteligíveis. Uma Parte pode exigir no direito interno uma intenção fraudulenta ou uma intenção ilegítima similar para que seja determinada a responsabilidade criminal.

Artigo 8º - Burla informática

Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, o acto intencional e ilegítimo, que origine a perda de bens a terceiros através:

a. Da introdução, da alteração, da eliminação ou da supressão de dados informáticos,

b. De qualquer intervenção no funcionamento de um sistema informático, com a intenção de obter um benefício económico ilegítimo para si ou para terceiros.

Título 3 – Infracções relacionadas com o conteúdo

Artigo 9º - Infracções relacionadas com pornografia infantil

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, as seguintes condutas, quando cometidas de forma intencional e ilegítima:

a. Produzir pornografia infantil com o objectivo da sua difusão através de um sistema informático;

b. Oferecer ou disponibilizar pornografia infantil através de um sistema informático;

c. Difundir ou transmitir pornografia infantil através de um sistema informático;

d. Obter pornografia infantil através de um sistema informático para si próprio ou para terceiros;

e. Possuir pornografia infantil num sistema informático ou num meio de armazenamento de dados informáticos.

2. Para efeitos do n.º 1, a expressão "pornografia infantil" inclui qualquer material pornográfico que represente visualmente:

a. Um menor envolvido num comportamento sexualmente explícito;

b. Uma pessoa que aparente ser menor envolvida num comportamento sexualmente explícito;

c. Imagens realísticas que representem um menor envolvido num comportamento sexualmente explícito;

3. Para efeitos do n.º 2, a expressão "menor" inclui qualquer pessoa com idade inferior a 18 anos. Uma Parte, pode, no entanto, exigir um limite de idade inferior, que não será menos que 16 anos.

4. Cada Parte pode reservar-se o direito de não aplicar, no todo ou em parte, o disposto nos n.ºs 1, alínea d), e., 2, alíneas b) e c).

Título 4 – Infracções relacionadas com a violação do direito de autor e direitos conexos

Artigo 10º - Infracções relacionadas com a violação do direito de autor e dos direitos conexos

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, a violação do direito de autor definido pela legislação dessa Parte, em conformidade com as obrigações que a mesma assumiu em aplicação da Convenção Universal sobre o Direito de Autor, revista em Paris, em 24 de Julho de 1971, da Convenção de Berna para a Protecção das Obras Literárias e Artísticas, do Acordo sobre os Aspectos dos Direitos de Propriedade Intelectual Relacionados com o Comércio, e do Tratado da OMPI sobre o Direito de Autor, com excepção de quaisquer direitos morais conferidos por essas Convenções, quando esses actos forem praticados intencionalmente, a uma escala comercial e por meio de um sistema informático.

2. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, a violação dos direitos conexos definidos pela legislação dessa Parte, em conformidade com as obrigações assumidas por força da Convenção Internacional para a Protecção dos Artistas Intérpretes ou Executantes, dos Produtores de Fonogramas e dos Organismos de Radiodifusão (Convenção de Roma) do Acordo sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados com o Comércio, e do Tratado da OMPI sobre Interpretações, Execuções e Fonogramas, com excepção de qualquer direito moral conferido por essas Convenções, quando esses actos forem praticados intencionalmente, a uma escala comercial e por meio de um sistema informático.

3. Uma Parte pode, em circunstâncias bem delimitadas, reservar-se o direito de não determinar a responsabilidade penal nos termos dos n.ºs 1 e 2 do presente artigo, na condição de estarem disponíveis outros meios eficazes e essa reserva não prejudique as obrigações internacionais que incumbem a essa Parte, em aplicação dos instrumentos internacionais mencionados nos n.ºs 1 e 2 do presente artigo.

Título 5 – Outras formas de Responsabilidade e Sanções

Artigo 11º - Tentativa e cumplicidade

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, a cumplicidade, quando cometida intencionalmente, na prática de qualquer uma das infracções estabelecidas de acordo com os artigos 2º a 10º da presente Convenção, com a intenção de que essa infracção seja cometida.

2. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, a tentativa de cometer uma das infracções estabelecidas nos artigos 3º, 5º, 7º, 8º, 9º, 1., alínea a) e 9, 1. alínea c) da presente Convenção.

3. Cada Parte pode reservar-se o direito de não aplicar, no todo ou em parte, o disposto no n.º 2 do presente artigo.

Artigo 12º - Responsabilidade de pessoas colectivas

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para assegurar que as pessoas colectivas possam ser consideradas responsáveis por infracções estabelecidas de acordo com a presente Convenção, quando cometidas em seu benefício por uma pessoa singular agindo quer individualmente, quer como membro de um órgão da pessoa colectiva que exerça no seu seio uma posição de direcção, com base no seguinte:

a. Poder de representação da pessoa colectiva;

b. Autoridade para tomar decisões em nome da pessoa colectiva;

c. Autoridade para exercer controlo no seio da pessoa colectiva.

2. Além dos casos já previstos no n.º 1 deste artigo, cada Parte adoptará as medidas necessárias para assegurar que uma pessoa colectiva possa ser considerada responsável quando a ausência de supervisão ou de controlo por parte de uma pessoa singular, mencionada no n.º 1 tornou possível a prática de infracções previstas na presente Convenção, em benefício da referida pessoa colectiva por uma pessoa singular agindo sob a sua autoridade.

3. De acordo com os princípios jurídicos da Parte, a responsabilidade de uma pessoa colectiva pode ser criminal, civil ou administrativa.

4. Essa responsabilidade deve ser determinada sem prejuízo da responsabilidade criminal das pessoas singulares que cometeram a infracção.

Artigo 13º - Sanções e medidas

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para assegurar que as infracções penais verificadas em aplicação dos Artigos 2º a 11º sejam passíveis de sanções eficazes, proporcionais e dissuasivas, incluindo penas privativas da liberdade.

2. Cada Parte assegurará que as pessoas colectivas consideradas responsáveis nos termos do artigo 12º, fiquem sujeitas à aplicação de sanções ou medidas, penais ou não penais eficazes, proporcionais e dissuasivas, incluindo sanções pecuniárias.

Secção 2 – Direito Processual

Título 1 – Disposições comuns

Artigo 14º - Âmbito das disposições processuais

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias, para instituir os poderes e os procedimentos previstos na presente Secção, para fins de investigação ou de procedimento penal.

2. Salvo disposição em contrário constante do artigo 21º, cada Parte aplicará os poderes e procedimentos referidos no n.º 1:

a. Às infracções penais em conformidade com o disposto nos artigos 2º a 11º da presente Convenção;

b. A outras infracções penais cometidas por meio de um sistema informático;

c. À recolha de prova em suporte electrónico provas electrónicas de qualquer infracção penal.

3. a. Cada Parte pode reservar-se o direito de apenas aplicar as medidas referidas no artigo 20º às infracções ou categorias de infracções especificadas na reserva, desde que o conjunto dessas infracções ou categorias de infracções não seja mais reduzido do que o conjunto de infracções às quais aplica as medidas referidas no artigo 21º. Cada Parte procurará limitar essa reserva de modo a permitir a aplicação mais ampla possível da medida referida no Artigo 20º.

b. Nos casos em que uma Parte, devido a restrições impostas pela sua legislação em vigor no momento da adopção da presente Convenção, não puder aplicar as medidas referidas nos Artigos 20º e 21º às comunicações transmitidas num sistema informático de um fornecedor de serviços, que

i. Esteja em funcionamento para benefício de um grupo fechado de utilizadores, e

ii. Não utilize redes públicas de telecomunicações e não esteja em conexão com outro sistema informático, quer seja público ou privado,

essa Parte pode reservar-se o direito de não aplicar essas medidas às referidas comunicações. Cada Parte procurará limitar essa reserva de modo a permitir a aplicação mais ampla possível das medidas referidas nos Artigos 20º e 21º.

Artigo 15º - Condições e salvaguardas

1. Cada Parte assegurará que o estabelecimento, a entrada em vigor e a aplicação dos poderes e procedimentos previstos na presente Secção são sujeitos às condições e salvaguardas estabelecidas pela legislação nacional, que deve assegurar uma protecção adequada dos direitos do Homem e das liberdades, designadamente estabelecidas em conformidade com as obrigações decorrentes da aplicação da Convenção do Conselho da Europa para a Protecção dos Direitos do Homem e das Liberdades Fundamentais dos Cidadãos (1950), do Pacto Internacional das Nações Unidas sobre os Direitos Civis e Políticos, (1966), bem como de outros instrumentos internacionais aplicáveis relativos aos Direitos do Homem e que deve integrar o princípio da proporcionalidade.

2. Quando for apropriado, tendo em conta a natureza do poder ou do procedimento em questão, as referidas condições e salvaguardas incluirão, designadamente, um controlo judicial ou outras formas de controlo independente, os fundamentos que justificam a sua aplicação, bem como a limitação do âmbito de aplicação e a duração do poder ou procedimento em causa.

3. Na medida em que seja do interesse público, em particular da boa administração da justiça, cada Parte examinará o efeito dos poderes e dos procedimentos da presente Secção sobre os direitos, responsabilidades e interesses legítimos de terceiros.

Título 2 – Conservação expedita de dados informáticos armazenados

Artigo 16º - Conservação expedita de dados informáticos armazenados

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para permitir às suas autoridades competentes exigir ou obter de uma outra forma a conservação expedita de dados informáticos específicos, incluindo dados relativos ao tráfego, armazenados por meio de um sistema informático, nomeadamente nos casos em que existem motivos para pensar que os mesmos são susceptíveis de perda ou alteração.

2. Sempre que a Parte aplique o disposto no n.º 1, através de uma injunção ordenando a uma pessoa que conserve os dados informáticos específicos armazenados que estão na sua posse ou sob o seu controlo, esta Parte adoptará as medidas legislativas e outras que se revelem necessárias para obrigar essa pessoa a conservar e proteger a integridade dos referidos dados durante um período de tempo tão longo quanto necessário, até um máximo de 90 dias, de modo a permitir às autoridades competentes obter a sua divulgação. Uma Parte pode prever que essa injunção seja subsequentemente renovada.

3. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para obrigar o responsável pelos dados, ou outra pessoa encarregada de os conservar a manter segredo sobre a execução dos referidos procedimentos durante o período previsto pelo seu direito interno.

4. Os poderes e procedimentos referidos no presente artigo devem estar sujeitos aos artigos 14º e 15º.

Artigo 17º - Conservação expedita e divulgação parcial de dados de tráfego

1. A fim de assegurar a conservação de dados relativos ao trafego em aplicação do artigo 16º, cada Parte adoptará as medidas legislativas e outras que se revelem necessárias, para:

a. Assegurar a conservação rápida desses dados de tráfego, quer tenham participado na transmissão dessa comunicação um ou vários fornecedores de serviços; e

b. Assegurar a divulgação rápida à autoridade competente da Parte ou a uma pessoa designada por essa autoridade, de uma quantidade de dados de

tráfego, suficiente para permitir a identificação dos fornecedores de serviços e da via através do qual a comunicação foi efectuada.

2. Os poderes e procedimentos referidos no presente artigo devem estar sujeitos aos artigos 14º e 15º.

Título 3 – Injunção

Artigo 18º - Injunção

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes para ordenar:

a. A uma pessoa que se encontre no seu território que comunique os dados informáticos específicos, na sua posse ou sob o seu controlo e armazenados num sistema informático ou num outro suporte de armazenamento de dados informáticos; e

b. A um fornecedor de serviços que preste serviços no território da Parte, que comunique os dados na sua posse ou sob o seu controlo, relativos aos assinantes e respeitantes a esses serviços

2. Os poderes e procedimentos referidos no presente artigo devem estar sujeitos aos artigos 14º e 15º.

3. Para os fins do presente artigo, a expressão "dados relativos aos assinantes" designa qualquer informação, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida por um fornecedor de serviços e que diga respeito aos assinantes 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 assinante, e qualquer outro número de acesso, os dados respeitantes à facturação 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.

Título 4 – Busca e Apreensão de dados informáticos armazenados

Artigo 19º - Busca e apreensão de dados informáticos armazenados

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes para proceder a buscas ou aceder de modo semelhante:

a. A um sistema informático ou a uma parte do mesmo, bem como a dados informáticos que nele se encontrem armazenados; e

b. A um suporte que permita armazenar dados informáticos.

2. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para assegurar que, nos casos em que as suas autoridades procedam a buscas ou acedam de forma semelhante a um sistema informático específico ou a uma parte do mesmo, em conformidade com o disposto no n.º 1, a), e tenham razões para pensar que os dados procurados se encontram armazenados noutro sistema informático ou numa parte do mesmo situado no seu território, e que esses dados são legalmente acessíveis a partir do sistema inicial ou obteníveis a partir desse sistema inicial, as referidas autoridades estejam em condições de estender de forma expedita a busca, ou o acesso de forma semelhante ao outro sistema.

3. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes para apreender ou para obter de forma semelhante os dados informáticos relativamente aos quais o acesso foi realizado em aplicação dos n.ºs 1 ou 2. Essas medidas incluem as prerrogativas seguintes:

a. Apreender ou obter de forma semelhante um sistema informático ou uma parte deste ou um suporte de armazenamento informático;

b. Realizar e conservar uma cópia desses dados informáticos;

c. Preservar a integridade dos dados informáticos pertinentes armazenados;

d. Tornar inacessíveis ou eliminar esses dados do sistema informático acedido.

4. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes a ordenar a qualquer pessoa que conheça o funcionamento do sistema informático ou as medidas utilizadas para proteger os dados informáticos nele contidos, que forneça na

medida do razoável as informações razoavelmente necessárias, para permitir a aplicação das medidas previstas nos n.ºs 1 e 2.

5. Os poderes e procedimentos referidos no presente artigos devem estar sujeitos aos artigos 14º e 15º.

Título 5 – Recolha em tempo real de dados informáticos

Artigo 20º - Recolha em tempo real de dados relativos ao tráfego

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes a:

a. Recolher ou registar, através da aplicação de meios técnicos existentes no seu território, e

b. Obrigar um fornecedor de serviços, no âmbito da sua capacidade técnica existente, a:

i. Recolher ou registar por meio da aplicação de meios técnicos no seu território, ou

ii. Prestar às autoridades competentes o seu apoio e assistência para recolher ou registar, em tempo real, dados de tráfego relativos a comunicações específicas no seu território transmitidas através de um sistema informático.

2. Quando uma Parte, em virtude dos princípios estabelecidos pela sua ordem jurídica interna, não pode adoptar as medidas descritas no nº 1, alínea a), pode, em alternativa, adoptar as medidas legislativas e outras que se revelem necessárias para assegurar a recolha ou o registo em tempo real dos dados de tráfego associados a comunicações específicas transmitidas no seu território através da aplicação de meios técnicos existentes nesse território.

3. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para obrigar um fornecedor de serviços a manter secreto o facto de qualquer um dos poderes previstos ter sido executado, bem como qualquer informação a esse respeito.

4. Os poderes e procedimentos referidos no presente artigo devem estar sujeitos aos artigos 14º e 15º.

Artigo 21º - Intercepção de dados relativos ao conteúdo

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes relativamente a um leque de infracções graves, a definir em direito interno, a:

a. Recolher ou registar, através da aplicação de meios técnicos existentes no seu território, e

b. Obrigar um fornecedor de serviços, no âmbito da sua capacidade técnica existente, a:

   i. Recolher ou registar através da aplicação de meios técnicos no seu território, ou

   ii. Prestar às autoridades competentes o seu apoio e a sua assistência para recolher ou registar, em tempo real, dados relativos ao conteúdo de comunicações específicas no seu território, transmitidas através de um sistema informático.

2. Quando a Parte em virtude dos princípios estabelecidos pela sua ordem jurídica interna, não pode adoptar as medidas descritas no n.º 1, alínea a), pode, em alternativa, adoptar as medidas legislativas e outras que se revelem necessárias, para assegurar a recolha ou o registo em tempo real dos dados relativos ao conteúdo associados a comunicações específicas transmitidas no seu território através da aplicação de meios técnicos existentes nesse território.

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias, para obrigar um fornecedor de serviços a manter secreto o facto de qualquer um dos poderes previstos no presente artigo ter sido executado, bem como qualquer informação a esse respeito.

2. Os poderes e procedimentos referidos no presente artigo devem estar sujeitos aos artigos 14º e 15º.

Secção 3 – Competência

Artigo 22º - Competência

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer a sua competência relativamente a qualquer infracção penal definida em conformidade com os artigos 2º a 11º da presente Convenção, sempre que a infracção seja cometida:

a. No seu território; ou

b. A bordo de um navio arvorando o pavilhão dessa Parte;

c. A bordo de uma aeronave matriculada nessa Parte e segundo as suas Leis; ou

d. Por um dos seus cidadãos nacionais, se a infracção for punível criminalmente onde foi cometida ou se a infracção não for da competência territorial de nenhum Estado.

2. Cada Parte pode reservar-se o direito de não aplicar ou de apenas aplicar em casos ou em condições específicas, as regras de competência definidas no n.º1, alínea *b)* a alínea *d)* do presente artigo ou em qualquer parte dessas alíneas.

3. Cada Parte adoptará as medidas que se revelem necessárias para estabelecer a sua competência relativamente a qualquer infracção referida no artigo 24º, n.º1 da presente Convenção, quando o presumível autor da infracção se encontre no seu território e não puder ser extraditado para outra Parte, apenas com base na sua nacionalidade, após um pedido de extradição.

4. A presente Convenção não exclui qualquer competência penal exercida por uma Parte em conformidade com o seu direito interno.

5. Quando mais que uma Parte reivindique a competência em relação uma presumível infracção prevista na presente Convenção, as Partes em causa, se for oportuno, consultar-se-ão a fim de determinarem qual é a jurisdição mais apropriada para o procedimento penal.

Capítulo III – Cooperação Internacional

Secção 1 – Princípios gerais

Título 1 – Princípios gerais relativos à cooperação internacional

Artigo 23º - Princípios gerais relativos à cooperação internacional

As Partes cooperarão entre si, em conformidade com as disposições do presente capítulo, em aplicação dos instrumentos internacionais pertinentes sobre a cooperação internacional em matéria penal, de acordos celebrados com base nas legislações uniformes ou reciprocas, e do seu direito nacional, na medida mais ampla possível, para efeitos de investigações ou de procedimentos relativos a infracções penais relacionadas com sistemas e dados informáticos, ou para recolher provas sob a forma electrónica de uma infracção penal.

Título 2 – Princípios relativos à extradição

Artigo 24º - Extradição

1.a. O presente artigo aplica-se à extradição entre as Partes relativamente a infracções penais definidas em conformidade com os artigos 2º a 11º da presente Convenção, desde que sejam puníveis na legislação de duas Partes envolvidas, por uma pena privativa de liberdade por um período máximo de, pelo menos um ano ou através de uma pena mais grave.

b. Quando for exigida uma pena mínima diferente, com base num tratado de extradição aplicável entre duas ou mais Partes, incluindo a Convenção Europeia de Extradição (STE Nº 24), ou num acordo baseado em legislações uniformes ou recíprocas, é a pena mínima prevista por esse tratado ou acordo que se aplica.

2. As infracções penais descritas no n.º 1 do presente artigo são consideradas como infracções passíveis de extradição em qualquer tratado de extradição existente ou que venha a existir entre as Partes. As Partes comprometer-se-ão a incluir essas infracções como infracções passíveis de extradição em qualquer tratado de extradição que possa ser firmado entre as Partes.

3. Quando uma Parte condicionar a extradição à existência de um tratado e receba um pedido de extradição de outra Parte com a qual não tenha celebrado qualquer tratado de extradição, pode considerar a presente Convenção como base jurídica para a extradição relativamente a qualquer infracção penal referida no n.º 1 do presente artigo.

4. As Partes que não condicionem a extradição à existência de um tratado, reconhecerão entre si as infracções penais referidas no n.º 1 do presente artigo como infracções passíveis de extradição.

5. A extradição ficará sujeita às condições previstas pelo direito interno da Parte requerida ou pelos tratados de extradição aplicáveis, incluindo os fundamentos com base nos quais a Parte requerida pode recusar a extradição.

6. No caso de a extradição por uma infracção penal mencionada no n.º 1 do presente artigo ser recusada unicamente com base na nacionalidade da pessoa procurada, ou pelo facto de a Parte requerida se considerar competente relativamente a essa infracção, a Parte requerida remeterá o processo, a pedido da Parte requerente, às suas autoridades competentes para fins de procedimento criminal e comunicará em tempo útil o resultado do processo à Parte requerente. As autoridades em questão tomarão a sua decisão e

conduzirão a investigação e o procedimento do mesmo modo que em relação a qualquer outra infracção de natureza comparável, em conformidade com a legislação desta Parte.

7. a. Cada Parte comunicará ao Secretário Geral do Conselho da Europa, no momento da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, o nome e morada de cada autoridade responsável pelo envio ou pela recepção de um pedido de extradição ou de detenção preventiva, no caso de ausência de tratado.

b. O Secretário Geral do Conselho da Europa constituirá e manterá actualizado um registo das autoridades assim designadas pelas Partes. Cada Parte deve assegurar com permanência a exactidão dos dados que constam do registo.

Título 3 – Princípios Gerais relativos ao auxílio mútuo

Artigo 25º - Princípios gerais relativos ao auxílio mútuo

1. As Partes concederão entre si o auxílio mútuo mais amplo possível para efeitos de investigações ou de procedimentos relativos a infracções penais relacionadas com sistemas e dados informáticos, ou para efeitos de recolha de provas sob a forma electrónica de uma infracção penal.

2. Cada Parte adoptará igualmente as medidas legislativas e outras que se revelem necessárias para darem cumprimento às obrigações estabelecidas nos artigos 27º a 35º.

3. Em caso de urgência, cada Parte pode formular os pedidos de auxílio mútuo ou comunicações com ele relacionadas, através de meios de comunicação rápidos, tais como o fax ou o correio electrónico, desde que esses meios ofereçam condições de segurança e de autenticação (incluindo, se necessário, o uso da encriptação) com posterior confirmação oficial sempre que o Estado requerido o exigir. O Estado requerido aceitará o pedido e responderá através de qualquer desses meios de comunicação rápidos.

4. Salvo disposição em contrário expressamente prevista nos artigos do presente Capítulo, o auxílio mútuo será sujeito 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. A Parte requerida não deve exercer o seu direito de recusar o auxílio mútuo relativamente às infracções previstas nos artigos 2º a 11º apenas

com fundamento em que o pedido se refere a uma infracção que considera ser de natureza fiscal.

5. Quando em conformidade com as disposições do presente capítulo, a Parte requerida estiver autorizada a subordinar o auxílio mútuo à existência de dupla incriminação, esta condição será considerada como satisfeita se o comportamento que constitui a infracção relativamente à qual foi efectuado o pedido de auxílio, for qualificado como infracção penal pelo seu direito interno, quer o direito interno classifique ou não a infracção na mesma categoria de infracções ou a designe ou não pela mesma terminologia que o direito da Parte requerente.

Artigo 26º - Informação espontânea

1. Uma Parte pode, dentro dos limites da sua legislação nacional e na ausência de pedido prévio, comunicar a outra Parte informações obtidas no quadro das suas próprias investigações, sempre que considerar que isso pode ajudar a Parte destinatária a iniciar ou a levar a cabo investigações ou procedimentos relativos a infracções penais, estabelecidas em conformidade com a presente Convenção, ou sempre que essas informações possam conduzir a um pedido formulado por essa Parte, nos termos do presente Capítulo.

2. Antes de comunicar essas informações, a Parte que as fornece pode solicitar que as mesmas permaneçam confidenciais ou apenas sejam utilizadas em determinadas condições. Caso a Parte destinatária não puder dar satisfação a esse pedido, deve informar a outra Parte desse facto que determinará se as informações devem contudo ser fornecidas. Se a Parte destinatária aceitar a informação nas condições estipuladas, fica obrigada a observar essas condições.

Título 4 – Procedimentos relativos aos pedidos de auxílio mútuo na ausência de acordos internacionais aplicáveis

Artigo 27º - Procedimentos relativos aos pedidos de auxílio mútuo na ausência de acordos internacionais aplicáveis

1. Na ausência de tratado de auxílio mútuo ou de acordo de que se baseie em legislação uniforme ou recíproca em vigor entre a Parte requerente e a Parte requerida, serão aplicáveis as disposições dos n.ºs 2 a 9 do presente artigo. Não serão aplicáveis se existir um tratado, um acordo, ou legislação deste tipo, a menos que as Partes em causa decidam aplicar em sua substituição o presente artigo no todo ou em parte.

2. a. Cada Parte designará uma ou mais autoridades centrais encarregadas de enviar os pedidos de auxílio mútuo ou de lhes responder, de os executar ou de os transmitir às autoridades competentes para a sua execução;

b. As autoridades centrais comunicarão directamente entre si;

c. Cada Parte, no momento da assinatura ou do depósito dos seus instrumentos de ratificação, aceitação, aprovação ou adesão, comunicará ao Secretário Geral do Conselho da Europa os nomes e moradas das autoridades designadas em aplicação do presente parágrafo.

d. O Secretário Geral do Conselho da Europa constituirá e manterá actualizado um registo das autoridades centrais designadas pelas Partes. Cada Parte assegurará em permanência a exactidão dos dados constantes do registo.

3. Os pedidos de auxílio ao abrigo do presente artigo serão executados em conformidade com os procedimentos especificados pela Parte requerente, excepto se forem incompatíveis com a legislação da Parte requerida.

4. Além das condições ou fundamentos de recusa previstos no artigo 25º, n.º 4, o auxílio pode ser recusado pela Parte requerida:

a. Se o pedido respeitar a infracções consideradas pela Parte requerida como infracções políticas ou com elas conexas; ou

b. Se a Parte considerar que o cumprimento do pedido pode atentar contra a sua soberania, segurança, ordem pública ou qualquer outro interesse essencial do seu país.

5. A Parte requerida pode adiar a execução de um pedido, se isso puder prejudicar as investigações criminais ou os procedimentos levados a cabo pelas suas autoridades.

6. Antes de recusar ou adiar a cooperação, a Parte requerida examinará após ter consultado, se for caso disso, a Parte requerente, se pode satisfazer o pedido no todo ou em parte ou sujeitá-lo às condições que considere necessárias.

7. A Parte requerida informará rapidamente a Parte requerente do seguimento que entende dar ao pedido de auxílio mútuo. Deve ser fundamentada a eventual recusa ou adiamento do pedido. A Parte requerida informará igualmente a Parte requerente de qualquer fundamento que torne impossível a execução do pedido ou que seja susceptível de o retardar significativamente.

8. A Parte requerente pode solicitar que a Parte requerida mantenha confidenciais os factos e o objecto de qualquer pedido formulado ao abrigo do presente

Capítulo, excepto na medida necessária à execução do referido pedido. Se a Parte requerida não puder dar satisfação a esse pedido de confidencialidade, deve informar prontamente a Parte requerente, a qual determinará então se o pedido deve contudo ser executado.

9. a. Em caso de urgência, as autoridades judiciárias da Parte requerente podem enviar directamente às suas homólogas da Parte requerida os pedidos de auxílio mútuo ou as comunicações que lhes digam respeito. Nesses casos, uma cópia será dirigida às autoridades centrais da Parte requerida por intermédio da autoridade central da Parte requerente.

b. Qualquer pedido ou comunicação ao abrigo do presente parágrafo pode ser efectuado através da Organização Internacional de Polícia Criminal (Interpol).

c. Quando um pedido tiver sido efectuado em aplicação da alínea a) do presente parágrafo e a autoridade não for competente para o tratar, transmiti-lo-á à autoridade nacional competente e informará desse facto directamente a Parte requerente.

d. Os pedidos ou comunicações efectuados em aplicação do presente parágrafo, que não impliquem uma acção coerciva, podem ser directamente transmitidos pelas autoridades competentes da Parte requerente às autoridades competentes da Parte requerida.

e. Cada Parte pode informar o Secretário Geral do Conselho da Europa, no momento da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão que, por razões de eficácia, os pedidos efectuados em conformidade com o presente número devem ser dirigidos à sua autoridade central.

Artigo 28º - Confidencialidade e restrição de utilização

1. Na ausência de tratados ou acordos de auxílio judiciário mútuo celebrados com base em legislações uniformes ou recíprocas em vigor entre a Parte requerente e a Parte requerida, serão aplicáveis as disposições do presente Artigo. Estas não serão aplicáveis quando exista um tratado, um acordo ou legislação daquele tipo, excepto se as Partes envolvidas decidirem aplicar em sua substituição o presente Artigo no todo ou em parte.

2. A Parte requerida pode sujeitar a comunicação da informação ou de material em resposta a um pedido à condição de que:

a. Seja mantida confidencial quando o pedido de auxílio judiciário mútuo não puder ser satisfeito na ausência dessa condição, ou

b. Não seja utilizada para fins de outra investigação ou de procedimento diferente dos indicados no pedido.

3. Se a Parte requerente não puder satisfazer uma das condições mencionadas no n.º 2, informará prontamente a Parte requerida, a qual determinará então se a informação deve, ainda assim, ser fornecida. Se a Parte requerente aceitar esta condição, ficará vinculada pela mesma.

4. Qualquer Parte que forneça informações ou material sujeita a uma das condições referidas no n.º2, pode exigir à outra Parte que lhe forneça esclarecimentos relativos a essa condição, quanto à utilização dessa informação ou desse material.

Secção 2 – Disposições específicas

Título 1 – Auxílio mútuo em matéria de medidas provisórias

Artigo 29º - Conservação expedita de dados informáticos armazenados

1. Uma Parte pode pedir a outra Parte que ordene ou obtenha de outra forma a conservação rápida dos dados armazenados por meio de um sistema informático, que se encontre no território dessa outra Parte, e relativamente aos quais a Parte requerente pretenda apresentar um pedido de auxílio mútuo para fins de busca ou de acesso similar, apreensão ou obtenção por meio similar, ou divulgação dos dados.

2. Um pedido de conservação efectuado nos termos do n.º 1 deve especificar:

a. A autoridade que pede a conservação;

b. A infracção que é objecto de investigação criminal ou de procedimento e uma breve exposição dos factos relacionados;

c. Os dados informáticos armazenados a conservar e a sua relação com a infracção;

d. Todas as informações disponíveis que permitam identificar o responsável pelos dados informáticos armazenados ou a localização do sistema informático;

e. A necessidade da medida de conservação; e

f. Que a Parte tenciona apresentar um pedido de assistência mútua com vista à busca ou outra forma de acesso, apreensão ou obtenção semelhante, ou divulgação dos dados informáticos armazenados.

3. Após ter recebido o pedido de outra Parte, a Parte requerida deve tomar as medidas apropriadas a fim de proceder, de forma expedita, à conservação dos dados especificados, em conformidade com o seu direito interno. Para poder responder a esse pedido, a dupla incriminação não é exigida como condição prévia à conservação.

4. Uma Parte que exija a dupla incriminação como condição necessária para responder a um pedido de auxílio mútuo para fins de busca ou acesso semelhante, apreensão ou obtenção por meio semelhante, ou a divulgação dos dados, pode, no que diz respeito a outras infracções diferentes das estabelecidas em conformidade com os artigos 2º a 11º da presente Convenção, reservar-se o direito de recusar o pedido de conservação ao abrigo do presente artigo, se tiver razões para crer que no momento da divulgação, a condição de dupla incriminação não pode ser preenchida.

5. Além disso, um pedido de conservação só pode ser recusado se:

a. O pedido respeitar a infracções consideradas pela Parte requerida como infracções políticas ou com elas conexas; ou

b. A Parte requerida considerar que o cumprimento do pedido pode atentar contra a sua soberania, segurança, ordem pública ou qualquer outro interesse essencial.

6. Quando a Parte requerida considerar que a simples conservação não é suficiente para garantir a disponibilidade futura dos dados, e comprometerá a confidencialidade da investigação da Parte requerente, ou prejudica de outra forma a mesma, informará prontamente disso a Parte requerente que decidirá, então, se o pedido deve, ainda assim, ser executado.

7. Qualquer conservação efectuada em resposta a um pedido referido no n.º 1 será válida por um período não inferior a 60 dias, a fim de permitir à Parte requerente apresentar um pedido para fins de busca ou acesso semelhante, apreensão ou obtenção semelhante, ou divulgação dos dados. Após a recepção desse pedido, os dados devem continuar a ser conservados até à adopção de uma decisão respeitante ao pedido.

Artigo 30º - Divulgação expedita dos dados de tráfego conservados

1. Se ao executar um pedido de conservação de dados relativos ao tráfego relacionados com uma comunicação específica efectuada em aplicação do artigo 29º, a Parte requerida descobrir que um fornecedor de serviços noutro Estado participou na transmissão dessa comunicação, a Parte requerida divulgará rapidamente à Parte requerente uma quantidade suficiente de dados relativos ao tráfego que permita identificar esse fornecedor de serviços e a via através da qual a comunicação foi transmitida.

2. A divulgação de dados de tráfego nos termos do disposto no n.º 1 apenas pode ser recusada se:

a. Se o pedido respeitar a uma infracção considerada pela Parte requerida como infracção de natureza política ou com ela conexa; ou

b. Se a Parte requerida considerar que o cumprimento do pedido pode atentar contra a sua soberania, segurança, ordem pública ou qualquer outro interesse essencial.

Título 2 – Auxílio mútuo relativamente a poderes de investigação

Artigo 31º - Auxílio mútuo relativamente ao acesso a dados informáticos armazenados

1. Uma Parte pode pedir a outra Parte para investigar ou aceder de forma semelhante, apreender, ou obter de forma semelhante, e divulgar dados armazenados por meio de sistema informático que se encontre no território dessa outra Parte, incluindo os dados conservados em conformidade com o artigo 29º.

2. A Parte requerida dará satisfação ao pedido aplicando os instrumentos internacionais, acordos e legislação referida no artigo 23º, e dando cumprimento às disposições pertinentes do presente Capítulo.

3. O pedido deve ser satisfeito o mais rapidamente possível nos casos em que:

a. Existam motivos para crer que os dados relevantes são especialmente vulneráveis à perda ou modificação; ou

b. Os instrumentos, acordos e legislação referida no n.º 2 prevejam uma cooperação rápida.

Artigo 32º - Acesso transfronteiríço a dados informáticos armazenados, com consentimento ou quando são acessíveis ao público

Uma Parte pode, sem autorização de outra Parte:

a. Aceder a dados informáticos armazenados acessíveis ao público (fonte aberta), seja qual for a localização geográfica desses dados; ou

b. aceder ou receber, através de um sistema informático situado no seu território, dados informáticos armazenados situados no território de outra Parte, se obtiver o consentimento legal e voluntário da pessoa legalmente autorizada a divulgar esses dados, através deste sistema informático.

Artigo 33º - Auxílio mútuo relativamente à recolha de dados de tráfego em tempo real

1. As Partes concederão entre si o auxílio mútuo no que diz respeito à recolha, em tempo real, de dados de tráfego associados a comunicações específicas transmitidas no seu território por meio de um sistema informático. Sem prejuízo do disposto no n.º2, esse auxílio regular-se-à pelas condições e procedimentos previstos em direito interno.

2. Cada Parte concederá o auxílio pelo menos no que diz respeito às infracções penais relativamente às quais seria possível a recolha ao nível interno a recolha em tempo real dos dados de tráfego em caso semelhante.

Artigo 34º - Auxílio mútuo em matéria de intercepção de dados de conteúdo

As Partes concederão auxílio judiciário mútuo, na medida em que é permitido pelos tratados e pelas legislações aplicáveis no que diz respeito à recolha ou ao registo, em tempo real, de dados relativos ao conteúdo de comunicações específicas transmitidas por meio de um sistema informático.

Título 3 - Rede 24/7

Artigo 35º - Rede 24/7

1. Cada Parte designará um ponto de contacto disponível 24 horas sobre 24 horas, 7 dias por semana, a fim de assegurar a prestação de assistência imediata a investigações ou procedimentos respeitantes a infracções penais relacionadas com dados e sistemas informáticos, ou a fim de recolher provas, sob forma electrónica, de uma infracção penal. O auxílio incluirá a facilitação, ou

se o direito e práticas internas o permitirem, a aplicação directa das seguintes medidas:

a. A prestação de aconselhamento técnico;

b. A conservação de dados em conformidade com os artigos 29º e 30º; e

c. A recolha de provas, informações de carácter jurídico e localização de suspeitos.

2. a. O ponto de contacto de uma Parte deve ter capacidade técnica para corresponder-se com o ponto de contacto de outra Parte de uma forma rápida;

b. Se o ponto de contacto designado por uma Parte não depender da autoridade ou autoridades dessa Parte responsáveis pela cooperação internacional ou extradição dessa Parte, o ponto de contacto assegurará que pode agir em coordenação com essa ou essas autoridades de forma rápida.

3. Cada Parte assegurará que pode dispor de pessoal formado e equipado a fim de facilitar o funcionamento da rede.

Capítulo IV – Disposições Finais

Artigo 36º - Assinatura e entrada em vigor

1. A presente Convenção está aberta à assinatura dos Estados membros do Conselho da Europa e dos Estados não membros que participaram na elaboração da mesma.

2. A presente Convenção é submetida a ratificação, aceitação ou aprovação. Os instrumentos de ratificação, aceitação ou aprovação serão depositados junto do Secretário Geral do Conselho da Europa.

3. A presente Convenção entrará em vigor no primeiro dia do mês seguinte ao termo de um período de três meses após a data na qual cinco Estados, incluindo pelo menos três Estados membros do Conselho da Europa, tenham manifestado o seu consentimento em ficar vinculados pela Convenção, em conformidade com as disposições dos n.ºs 1 e 2.

4. Em relação a qualquer Estado signatário que posteriormente exprima o seu consentimento em vincular-se à Convenção, esta entrará em vigor no primeiro dia do mês seguinte ao termo de um período de três meses após a data em que tenha sido expresso o seu consentimento em vincular-se à Convenção, em conformidade com as disposições dos n.ºs 1 e 2.

Artigo 37º - Adesão à Convenção

1. Após a entrada em vigor da presente Convenção, o Comité de Ministros do Conselho da Europa pode, depois de ter consultado os Estados contratantes da Convenção e de ter obtido o acordo unânime, convidar qualquer Estado não membro do Conselho e que não tenha participado na sua elaboração, a aderir à presente Convenção. A decisão é tomada pela maioria prevista no artigo 20º, alínea *d)*, dos Estatutos do Conselho da Europa e por unanimidade dos representantes dos Estados contratantes com direito de voto no Comité de Ministros.

2. Em relação a qualquer Estado aderente à Convenção, em conformidade com o n.º 1, a Convenção entrará em vigor no primeiro dia do mês seguinte ao termo de um período de três meses após a data do depósito do instrumento de adesão junto do Secretário Geral do Conselho da Europa.

Artigo 38º - Aplicação territorial

1. Qualquer Estado pode, no momento da assinatura ou no momento do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, designar o, ou os territórios aos quais se aplicará a presente Convenção.

2. Qualquer Estado pode, em qualquer momento posterior, mediante declaração dirigida ao Secretário Geral do Conselho da Europa, tornar extensível a aplicação da presente Convenção a qualquer outro território designado na declaração. A Convenção entrará em vigor em relação a esse território no primeiro dia do mês seguinte ao termo de um período de três meses após a data de recepção da declaração pelo Secretário Geral.

3. Qualquer declaração feita nos termos dos dois parágrafos anteriores pode ser retirada, no que diz respeito a qualquer território designado na declaração, mediante notificação dirigida ao Secretário Geral do Conselho da Europa. Essa declaração produzirá efeitos no primeiro dia do mês seguinte ao termo de um período de três meses após a data de recepção da referida notificação pelo Secretário Geral.

Artigo 39º - Efeitos da Convenção

1. O objectivo da presente Convenção é complementar os tratados ou acordos multilaterais ou bilaterais aplicáveis existentes entre as Partes, incluindo as disposições:

- Da Convenção Europeia de Extradição, aberta para assinatura em Paris a 13 de Dezembro de 1957 (STE Nº 24);

– Da Convenção Europeia de Auxílio Mútuo em Matéria Penal, aberta para assinatura em Estrasburgo, a 20 de Abril de 1959 (STE n.º 30);
– Do Protocolo Adicional à Convenção Europeia de Auxílio Mutuo em Matéria Penal, aberta para assinatura em Estrasburgo, a 17 de Março de 1978 (STE n.º 99).

2. Se duas ou mais Partes tiverem já celebrado um acordo ou tratado relativo às matérias tratadas pela presente Convenção ou se, de outra forma, tiverem estabelecido relações a este respeito, ou se vierem a fazê-lo no futuro, terão a possibilidade de aplicar o referido acordo ou tratado ou estabelecer essas relações em substituição da presente Convenção. Todavia, sempre que as Partes estabeleçam relações respeitantes a matérias objecto da presente Convenção de forma diferente daquela que é prevista pela mesma, fa-lo-ão de uma forma que não seja incompatível com os princípios e objectivos da presente Convenção.

3. Nada na Convenção prejudicará outros direitos, restrições, obrigações e responsabilidades de uma Parte.

Artigo 40º - Declarações

Qualquer Estado pode, mediante notificação por escrito dirigida ao Secretário Geral do Conselho da Europa no acto da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, declarar que fará uso da faculdade de exigir, se for caso disso, um ou mais elementos suplementares, tal como previsto nos artigos 2º, 3º, 6º, n.º 1, alínea *b)*, 7º, 9º, n.º 3 e 27º, n.º 9, alínea *e)*.

Artigo 41º - Cláusula federal

1. Um Estado federal pode reservar-se o direito de assumir as obrigações nos termos do capítulo II da presente Convenção na medida em que sejam compatíveis com os princípios fundamentais que governam as relações entre o seu Governo central e os Estados federados, ou outras entidades territoriais análogas, desde que esteja em condições de cooperar com base no Capítulo III.

2. Quando tiver feito uma reserva prevista no n.º1, não pode utilizar essa reserva para excluir ou diminuir de forma substancial as suas obrigações nos termos do Capítulo II. Em qualquer caso, dotar-se-á de meios amplos e eficazes que permitam a aplicação das medidas previstas no referido capítulo.

3. No que se refere às disposições da presente Convenção, cuja execução seja da competência legislativa dos Estados federados ou de outras entidades territoriais análogas que não são, nos termos do sistema constitucional da federação obrigados a tomar medidas legislativas, o governo federal levará com parecer favorável as referidas disposições ao conhecimento das autoridades competentes dos Estados federais incitando-os a adoptar as medidas adequadas para as executar.

Artigo 42º - Reservas

Qualquer Estado pode, mediante notificação por escrito dirigida ao Secretário Geral do Conselho da Europa no momento da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, declarar a sua intenção de fazer uso da(s) reserva(s) previstas nos artigos 4º, n.º 2, 6º, n.º 3, 9º, n.º 4, 10º, n.º 3, 11º, n.º 3, 14º, n.º 3, 22º, n.º 2, 29º, n.º 4, e 41, n.º 1. Nenhuma outra reserva poderá ser formulada.

Artigo 43º - Estatuto e levantamento das reservas

1. Uma Parte que tenha formulado uma reserva em conformidade com o artigo 42º pode retirá-la no todo ou em parte, mediante notificação dirigida ao Secretário-Geral do Conselho da Europa. A declaração produzirá efeitos na data de recepção da referida notificação pelo Secretário Geral. Se a notificação indicar que o levantamento da reserva deve produzir efeitos numa data precisa e essa data for posterior à da recepção da notificação pelo Secretário Geral, a declaração produz efeitos nessa data posterior.

2. Uma Parte que tenha formulado uma reserva nos termos do artigo 42º retirará essa reserva no todo ou em parte, logo que as circunstâncias o permitam.

3. O Secretário-Geral do Conselho da Europa pode, periodicamente, pedir às Partes que formularam uma ou mais reservas nos termos do artigo 42º, informações sobre as perspectivas de levantamento dessas reservas.

Artigo 44º - Aditamentos

1. Quaisquer aditamentos à presente Convenção podem ser propostas por qualquer uma das Partes e serão comunicadas pelo Secretário Geral do Conselho da Europa aos Estados membros do Conselho da Europa, aos Estados não membros que participaram na elaboração da presente Convenção, bem

como a qualquer Estado que tenha aderido, ou sido convidado a aderir em conformidade com as disposições do artigo 37º.

2. Qualquer aditamentos proposta por uma Parte deve ser comunicada ao Comité Europeu para os Problemas Criminais (CDPC), que submeterá ao Comité de Ministros o seu parecer relativamente à alteração proposta.

3. O Comité de Ministros examinará o aditamento proposto e o parecer submetido pelo Comité Europeu para os Problemas Criminais (CDPC) e, após consulta dos Estados não membros, Partes na presente Convenção, pode adoptar o referido aditamento.

4. O texto de qualquer aditamento adoptado pelo Comité de Ministros em conformidade com o n.º 3 do presente artigo será comunicado às Partes para aceitação.

5. Qualquer aditamento adoptado em conformidade com o n.º 3 do presente artigo entrará em vigor no trigésimo dia após todas Partes terem informado o Secretário Geral acerca da sua aprovação.

Artigo 45º - Resolução de litígios

1. O Comité Europeu para os Problemas Criminais (CDPC) será mantido informado sobre a interpretação e a aplicação da presente Convenção.

2. No caso de litígio entre as Partes sobre a interpretação ou a aplicação da presente Convenção, as mesmas esforçar-se-ão por encontrar uma solução para o litígio através da negociação ou de qualquer outro meio pacífico à sua escolha, incluindo submeter o litígio ao Comité Europeu para os Problemas Criminais (CDPC), a um tribunal arbitral, cujas decisões vincularão as Partes no litígio, ou ao Tribunal Internacional de Justiça, de comum acordo entre as Partes envolvidas.

Artigo 46º - Consulta entre as Partes

1. As Partes consultar-se-ão periodicamente, se necessário, a fim de facilitar:

a. A utilização e a execução efectiva da presente Convenção, incluindo a identificação de qualquer problema na matéria, bem como os efeitos de qualquer declaração ou reserva feita em conformidade com a presente Convenção;

b. A troca de informações sobre os desenvolvimentos jurídicos, políticos ou técnicos importantes verificados no domínio da cibercriminalidade e a recolha de provas sob forma electrónica;

c. A análise de eventuais complementos ou aditamentos à Convenção.

2. O Comité Europeu para os Problemas Criminais (CDPC) será mantido periodicamente informado do resultado da consulta referida no n.º 1.

3. O Comité Europeu para os Problemas Criminais (CDPC) facilitará, se necessário, as consultas referidas no n.º 1 e adoptará as medidas necessárias para ajudar as Partes nos seus esforços destinados a complementar ou a fazer aditamentos à Convenção. O mais tardar no final de um prazo de três anos a contar da entrada em vigor da presente Convenção, o Comité Europeu para os Problemas Criminais (CDPC) procederá em cooperação com as Partes a um reexame de todas as disposições constantes da Convenção e, se necessário, proporá os aditamentos adequados.

4. Salvo quando o Conselho da Europa assuma as despesas ocasionadas pela aplicação do disposto no n.º 1, as mesmas serão suportadas pelas Partes.

5. As Partes são assistidas pelo Secretariado do Conselho da Europa no exercício das suas funções decorrentes do presente artigo.

Artigo 47º - Denúncia

1. Qualquer Parte pode, em qualquer momento, denunciar a presente Convenção através de notificação dirigida ao Secretário Geral do Conselho da Europa.

2. A denúncia produzirá efeitos no primeiro dia do mês seguinte ao termo de um período de três meses após a data de recepção da notificação pelo Secretário Geral.

Artigo 48º - Notificação

O Secretário Geral do Conselho da Europa notificará os Estados membros do Conselho da Europa, os Estados não membros que participaram na elaboração da presente Convenção, bem como qualquer Estado aderente, ou que tenha sido convidado a aderir à presente Convenção de:

a. Todas as assinaturas;

b. O depósito de qualquer instrumento de ratificação, aceitação, aprovação ou adesão;

c. Todas as datas de entrada em vigor da presente Convenção, em conformidade com os artigos 36º e 37º;

d. Todas as declarações efectuadas em aplicação do(s) artigo(s) 40º, 41º, ou as reservas formuladas em aplicação do artigo 42º:

e. Qualquer outro acto, notificação ou comunicação relacionados com a presente Convenção.

Em fé do que os abaixo assinados, devidamente autorizados para este efeito, assinaram a presente Convenção.

Feito em Budapeste, em 23 de Novembro de 2001, em francês e inglês, ambos os textos fazendo igualmente fé, num único exemplar, que será depositado nos arquivos do Conselho da Europa. O Secretário Geral do Conselho da Europa enviará cópias autenticadas a cada um dos Estados membros do Conselho da Europa, aos Estados não membros que participaram na elaboração da presente Convenção, e a qualquer Estado que tenha sido convidado a aderir à Convenção.

Relatório explicativo à Convenção sobre o cibercrime

I. A convenção e o respetivo Relatório explicativo foram aprovados pelo Comité de Ministros do Conselho Europeu, na sua 109.ª sessão (8 de novembro de 2001) e a Convenção foi aberta para assinatura em Budapeste, a 23 de novembro de 2001, sobre a questão da Conferência Internacional sobre o cibercrime.

II. O texto deste relatório explicativo não constitui um instrumento que forneça uma interpretação autoritária da Convenção, embora possa ser de natureza a facilitar a aplicação das disposições nele contidas.

I. Introdução

1. A revolução nas tecnologias da informação operou mudanças fundamentais na sociedade e irá provavelmente continuar a fazê-lo num futuro previsível. Foram inúmeras as tarefas cuja execução se tornou mais fácil. Enquanto que, inicialmente, apenas alguns sectores específicos da sociedade procederam a uma racionalização dos seus métodos de trabalho, com a ajuda das tecnologias da informação, actualmente, não existe praticamente nenhum sector da sociedade que não tenha sido abrangido pelas mesmas. As tecnologias da informação vieram, de uma forma ou de outra, conferir novos contornos a quase todos os aspectos das actividades do Homem.

2. Uma característica notável da tecnologia da informação reside no impacto que esta teve, e ainda virá a ter certamente, na evolução da tecnologia das telecomunicações. Os clássicos sistemas telefónicos, envolvendo a transmissão da voz do Homem, foram suplantados por sistemas de permuta de grandes quantidades de dados, incluindo sob a forma de voz, texto e música, assim como de imagens estáticas e móveis. Esta permuta não se dá apenas entre os seres humanos, mas também entre estes e os computadores, e ao nível dos sistemas de computadores entre si. As ligações por comutação de circuitos foram substituídas por ligações por comutação de pacotes. Nos dias de hoje, já não é importante o facto de se poder ou não estabelecer uma ligação directa; basta que os dados em questão sejam introduzidos numa rede com um endereço de destino ou que sejam disponibilizados a todos quantos desejem aceder-lhes.

3. A utilização universal do correio electrónico e o acesso aos inúmeros sites através da Internet constituem o exemplo desses desenvolvimentos que tão profundamente contribuíram para a mudança ocorrida na nossa sociedade.

4. A fácil acessibilidade e pesquisa da informação contida em sistemas informáticos, aliada às possibilidades quase ilimitadas relativamente à sua permuta e difusão, não obstante as distâncias geográficas, traduziu-se por um crescimento explosivo da quantidade de informação disponível e do conhecimento que daí advém.

5. Estes desenvolvimentos deram origem a mutações sociais e económicas sem precedentes, mas apresentam simultaneamente uma faceta negativa: a emergência de novos tipos de criminalidade, bem como a prática dos crimes tradicionais com recurso às novas tecnologias. Além disso, as consequências do comportamento de índole criminosa poderão ser mais extensas e ter um maior alcance uma vez que não são restringidas por quaisquer limites geográficos ou fronteiras nacionais. A recente disseminação de vírus informáticos prejudiciais, um pouco por todo o mundo, comprova esta realidade. As medidas de carácter técnico que visam proteger os sistemas informáticos deverão, pois, ser tomadas concomitantemente com medidas de natureza jurídica a fim de evitar e deter a prática de crimes.

6. As novas tecnologias representam um desafio face aos conceitos jurídicos existentes. O fluxo da informação e das comunicações, a nível mundial, é agora substancialmente mais fácil. As fronteiras já não constituem um limite para este fluxo. Cada vez mais, os autores dos crimes encontram-se em locais diferentes daqueles em que os seus actos produzem efeitos. No entanto, as legislações nacionais estão geralmente confinadas a um território específico. Assim sendo, impõe-se que as soluções para os problemas que se colocam sejam abordadas por uma legislação internacional, pelo que se requer a adopção de instrumentos jurídicos de âmbito internacional. A presente Convenção propõe-se responder a este desafio, atribuindo o devido respeito aos direitos do Homem no seio da nova Sociedade de Informação.

II. Trabalhos preparatórios

7. O Comité Europeu para os Problemas Criminais (CDPC), mediante a deliberação CDPC/103/211196, datada de Novembro de 1996, decidiu formar um comité de especialistas para lidar com as questões da cibercriminalidade. O CDPC baseou a sua decisão nos seguintes pressupostos:

8. "Os rápidos progressos verificados no domínio da tecnologia da informação têm repercussões directas em todos os sectores da sociedade moderna. A integração de sistemas de telecomunicação e de informação, permitindo, independentemente da distância, o armazenamento e a transmissão de

todos os tipos de dados, significa que se assiste ao abrir de um vasto leque de novas possibilidades. Estes desenvolvimentos foram impulsionados pela emergência de vias e redes de informação, nestas se incluindo a Internet, através das quais qualquer pessoa poderá, virtualmente, aceder a qualquer serviço de informação electrónico, não obstante a sua localização em qualquer parte do mundo. Ao efectuarem a sua ligação aos serviços de comunicação e informação, os utilizadores estão a criar uma espécie de espaço comum, designado por "ciberespaço", o qual é utilizado para a prossecução de fins legítimos mas que poderá igualmente ser objecto de usos abusivos. Estas "infracções ao ciberespaço" tanto podem ser cometidas contra a integridade, disponibilidade e confidencialidade de sistemas informáticos e redes de telecomunicações, como podem consistir na utilização das referidas redes e dos seus serviços com a finalidade de cometer as tradicionais infracções. O carácter transfronteiriço das ditas infracções, por exemplo, quando cometidas através da Internet, entra em conflito com a territorialidade das autoridades nacionais competentes para a aplicação da lei.

9. O direito penal deverá, pois, manter-se a par destes avanços tecnológicos que, por meios altamente sofisticados, propiciam uma utilização indevida das funcionalidades do ciberespaço e um consequente lesar dos interesses legítimos. Visto que as redes de informação ignoram a existência de fronteiras, afigura-se como sendo necessário um esforço internacional concertado no sentido de fazer face a esta utilização indevida. Embora a Recomendação Nº (89) 9 tenha tido como resultado uma aproximação dos conceitos nacionais relativamente a determinadas formas de utilização indevida de um sistema informático, somente um instrumento internacional vinculatório poderá garantir a eficácia necessária na luta contra estes novos fenómenos. No âmbito de um tal instrumento, e adicionalmente às acções de cooperação internacional, deverão ser abordadas as questões do direito substantivo e processual bem como todas as temáticas estreitamente relacionadas com o uso da tecnologia de informação."

10. O CDPC levou ainda em linha de conta o Relatório elaborado, a seu pedido, pelo Professor H.W.K. Kaspersen, no qual se concluía que "... deveria ser ponderado um outro instrumento jurídico com maior peso do que uma Recomendação, como por exemplo uma Convenção. Uma tal Convenção deveria não só lidar com as questões do direito penal substantivo, mas também com os aspectos de processo penal e os acordos e procedimentos do

foro do direito penal."[1] Uma conclusão semelhante figura também no Relatório apenso à Recomendação Nº R (89) 9[2] relativamente ao direito substantivo e na Recomendação Nº R (95) 13[3] relativamente aos problemas do direito processual no que concerne à tecnologia de informação.

11. Descreve-se, em seguida, o mandato específico do novo comité:

    i. "Analisar, à luz das Recomendações Nº R (89) 9 sobre o crime relacionado com computadores e Nº R (95) 13 sobre os problemas do direito processual penal em relação à tecnologia da informação, nomeadamente os seguintes assuntos:

    ii. infracções ao ciberespaço, em particular, as cometidas através da utilização de redes de telecomunicação, por exemplo, a Internet, tais como transacções financeiras ilegais, oferta de serviços ilegais, violação dos direitos de autor, bem como as infracções que implicam a violação da dignidade humana e da protecção de menores;

    iii. outras questões de direito penal substantivo, para as quais se afigure pertinente a adopção de uma abordagem comum para os fins da cooperação internacional, tais como as definições, as sanções e as responsabilidades relativas aos intervenientes no ciberespaço, incluindo os fornecedores de serviços da Internet;

    iv. o uso, incluindo um eventual uso de carácter transfronteiriço, e a aplicabilidade de poderes coercivos num meio tecnológico, a saber, a intercepção de telecomunicações e a vigilância electrónica das redes de informação, por exemplo, através da Internet, a investigação e apreensão no que se refere a sistemas de tratamento da informação (incluindo os *sites* da Internet), tornando inacessível o material ilegal e exigindo dos fornecedores de serviços o cumprimento de obrigações especiais, tendo em consideração os problemas resultantes de medidas específicas de segurança da informação como, por exemplo, a encriptação;

    v. a questão da jurisdição sobre as infracções relacionadas com a tecnologia da informação, por exemplo, a determinação do local onde

---

1. Implementação da Recomendação Nº R (89) 9 sobre o crime relacionado com computadores, Relatório elaborado pelo Professor Dr. H.W.K. Kaspersen (doc. CDPC (97) 5 e PC-CY (97) 5, pág. 106).
2. Consultar o Relatório do Comité Europeu para os Problemas Criminais, sobre o crime relacionado com computadores, na pág. 86.
3. Consultar a Recomendação Nº R (95) 13, princípio nº 17, sobre os problemas do direito processual penal em relação à tecnologia da informação

a infracção foi cometida *(locus delicti)* e qual a legislação aplicável em consonância com tal facto, incluindo o problema do princípio *ne bis idem* em caso de multiplicidade de competências e a questão de como resolver os conflitos de jurisdição positiva e evitar os de jurisdição negativa;

vi. questões de cooperação internacional no quadro das investigações sobre as infracções cometidas no ciberespaço, em estreita colaboração com o Comité de Especialistas sobre o Funcionamento das Convenções Europeias em Matéria Penal (PC-OC).

O Comité deverá preparar um instrumento jurídico vinculatório e baseado, tanto quanto possível, nos pontos i) – v), com particular ênfase nas questões internacionais e, caso tal se mostre apropriado, nas recomendações anexas relativamente a assuntos específicos. O Comité poderá apresentar sugestões sobre outras questões à luz da evolução tecnológica."

12. Na sequência da decisão do CDPC, o Comité de Ministros constituiu o novo comité denominado por "Comité de Especialistas sobre a Criminalidade no Ciberespaço (PC-CY)", mediante deliberação nº CM/Del/Dec(97)583, a qual foi tomada na 583ª assembleia dos delegados dos Ministros (realizada a 4 de Fevereiro de 1997). O Comité PC-CY iniciou os seus trabalhos em Abril de 1997, tendo-se dedicado a negociações relativas a um projecto de convenção internacional sobre o cibercrime. De acordo com os termos do seu mandato original, o Comité deveria terminar os seus trabalhos até à data de 31 de Dezembro de 1999. Uma vez que, por essa ocasião, o Comité não se encontrava ainda em posição de concluir as suas negociações relativamente a determinados assuntos que integram o projecto de convenção, o seu mandato foi prorrogado até 31 de Dezembro de 2000, por deliberação nº CM/Del/Dec(99)679 dos delegados dos Ministros. Os Ministros da Justiça Europeus formalizaram, por duas vezes, o seu apoio às negociações: através da Resolução Nº 1, adoptada na sua 21ª Conferência (Praga, Junho de 1997), a qual recomendava que o Comité de Ministros prestasse o seu apoio ao trabalho desenvolvido sob a égide do CDPC no que se refere ao cibercrime, visando a harmonização das disposições legais nacionais, em matéria penal, e a utilização de meios de investigação eficazes relativamente a tais delitos, bem como, através da Resolução Nº 3 adoptada na 23ª Conferência dos Ministros da Justiça Europeus (Londres, Junho de 2000), a qual incentivava as partes intervenientes nas negociações a prosseguirem os seus esforços no sentido de apresentar soluções apropriadas, de forma a permitir a participação do maior número possível de países na Convenção. A referida Resolução

reconheceu ainda a necessidade de criação de um sistema rápido e eficaz de cooperação internacional, que reflectisse devidamente os requisitos específicos do combate ao cibercrime. Os Estados-membros da União Europeia expressaram o seu apoio ao trabalho desenvolvido pelo PC-CY através de uma Posição Comum, adoptada em Maio de 1999.

13. Entre Abril de 1997 e Dezembro de 2000, o Comité PC-CY realizou 10 sessões plenárias e 15 assembleias do seu Grupo de Redacção de participação ilimitada. Após a data de expiração do período de prorrogação do seu mandato, os especialistas realizaram ainda, sob a égide do CDPC, três reuniões suplementares cujo objectivo foi o da finalização do Memorando Explicativo preliminar e a revisão do projecto de Convenção à luz do parecer emitido pela Assembleia Parlamentar, já que em Outubro de 2000, a referida Assembleia havia sido convidada pelo Comité de Ministros a emitir o seu parecer sobre o projecto de Convenção, o qual viria a adoptar na 2ª parte da sua sessão parlamentar realizada em Abril de 2001.

14. No seguimento de uma decisão tomada pelo Comité PC-CY, foi abolido o regime de segredo e publicada uma versão preliminar do projecto de Convenção, em Abril de 2000, tendo-se seguido a divulgação das subsequentes minutas de cada assembleia plenária realizada, a fim de permitir aos Estados participantes nas negociações proceder a uma consulta junto de todas as partes interessadas. Este processo de consulta comprovou-se ter sido de alguma utilidade.

15. O projecto de Convenção e o seu Memorando Explicativo revistos e finalizados foram submetidos ao CDPC para aprovação, na sua 50ª sessão plenária realizada em Junho de 2001, após o que o texto do projecto de Convenção foi submetido ao Comité de Ministros a fim de ser adoptado e aberto para assinatura.

III. A Convenção

16. A Convenção tem por objecto principal (1) a harmonização dos elementos relativos a infracções no contexto do direito penal substantivo de âmbito nacional e das disposições conexas na área da cibercriminalidade, (2) a definição, ao abrigo do código de processo penal interno, dos poderes necessários para investigar e intentar acções penais relativamente a tais infracções, assim como a outras infracções cometidas por meio de um sistema informático ou às provas com elas relacionadas e existentes sob a forma electrónica (3) a implantação de um regime rápido e eficaz de cooperação internacional.

17. A Convenção engloba, portanto, quatro capítulos: (I) Utilização de terminologia; (II) Medidas a empreender ao nível nacional – direito substantivo e direito processual; (III) Cooperação Internacional; (IV) Disposições Finais.

18. O Capítulo I (questões de direito substantivo) abrange as disposições relativas à criminalização e outras disposições na área do crime informático ou relacionado com computadores: começa por definir 9 infracções agrupadas em 4 categorias diferentes, abordando depois a responsabilidade acessória e as sanções. São definidas pela Convenção as seguintes infracções: acesso ilícito, intercepção ilícita, interferência nos dados, interferência nos sistemas, utilização indevida de equipamentos, falsificação relacionada com computadores, fraude relacionada com computadores, infracções relacionadas com pornografia infantil e infracções relacionadas com a violação dos direitos de autor e dos direitos conexos.

19. O Capítulo II (questões de direito processual) – cujo âmbito ultrapassa as infracções definidas no Capítulo II na medida em que se aplica a qualquer infracção cometida por meio de um sistema informático ou à prova da mesma, existindo esta última sob a forma electrónica – determina, primeiramente, as condições e salvaguardas gerais, aplicáveis a todos os poderes do foro processual neste capítulo. Em seguida, define os seguintes poderes processuais: preservação expedita de dados informatizados armazenados; preservação expedita e divulgação parcial de dados de tráfego; ordem de produção; investigação e apreensão de dados informatizados; recolha de dados de tráfego em tempo real; intercepção de dados de conteúdo. O Capítulo II termina com as disposições relativas à jurisdição.

20. O Capítulo III contém as disposições relativas à assistência mútua em casos de crime tradicional e crime informático, bem como as regras de extradição. Este capítulo cobre a assistência mútua tradicional em duas situações: a primeira, quando se verifica a inexistência de uma base jurídica (tratado, legislação recíproca, etc.) entre as Partes – sendo que neste caso se aplicam as suas disposições – e segunda, quando a referida base jurídica existe – sendo que neste caso os acordos existentes deverão ser igualmente aplicáveis à assistência prestada ao abrigo da presente Convenção. A assistência específica relativa a crime informático, ou relacionado com computadores, é aplicável a ambas as situações e abrange, embora sujeito a condições adicionais, o mesmo leque de poderes processuais tal como definido no Capítulo II. O Capitulo III inclui ainda uma disposição relativa a um tipo específico de acesso transfronteiriço a dados informatizados armazenados, que não requer assistência mútua (com consentimento ou quando

publicamente disponíveis) e prevê a constituição de uma rede 24/7 a fim de assegurar uma assistência agilizada entre as Partes.

21. Por fim, o capítulo IV contém as cláusulas finais, as quais – com algumas excepções – retomam as disposições de referência constantes dos tratados do Conselho da Europa.

Comentário sobre os artigos da Convenção

Capítulo I – Utilização de terminologia

Introdução às definições do Artigo 1º

22. Foi considerado pelos autores do projecto que, ao abrigo da presente Convenção, as Partes não ficariam obrigadas a copiar textualmente, para as suas legislações nacionais, os quatro conceitos definidos no Artigo 1º, desde que tais conceitos se encontrem abrangidos nas referidas legislações de uma forma coerente com os princípios da Convenção e proporcionem uma estrutura equivalente para a sua implementação.

Artigo 1 (a) – Sistema informático

23. Um sistema informático, nos termos a que se refere a Convenção, é um equipamento composto por *hardware* e *software* desenvolvidos para o tratamento automático de dados digitais. Poderá incluir dispositivos de entrada, saída e armazenamento. Poderá funcionar independentemente ou estar ligado em rede com outros dispositivos semelhantes. O termo "Automático" significa sem a intervenção directa do Homem e a expressão "tratamento de dados" significa que os dados no sistema informático são operados através da execução de um programa de computador. Um "programa de computador" é um conjunto de instruções passíveis de serem executadas pelo computador para obter o resultado pretendido. Um computador pode executar diferentes programas. Um sistema informático é, normalmente, composto por vários dispositivos, distinguindo-se o processador ou unidade central de processamento e os periféricos. Um "periférico" consiste num aparelho que desempenha determinadas funções específicas em interacção com a unidade de processamento, tal como uma impressora, um monitor de vídeo, um leitor/gravador de CD ou outro dispositivo de armazenamento.

24. Uma rede é uma interligação entre dois ou mais sistemas informáticos. As ligações podem ser de terra (por exemplo, fio ou cabo), sem fio (por

exemplo, rádio, infravermelhos, ou satélite) ou ambas. Uma rede poderá ser geograficamente limitada a uma pequena área (rede de área local - LAN) ou cobrir uma vasta área (rede de área alargada - WAN), podendo estas redes estar interligadas entre si. A Internet é uma rede global composta por muitas redes interligadas, sendo que todas usam os mesmos protocolos. Existem outros tipos de redes, ligadas ou não à Internet, que permitem comunicar dados entre sistemas informáticos. Estes sistemas informáticos podem estar conectados à rede como terminais de saída ou como um meio de facilitar a comunicação na rede. O importante é que os dados sejam permutados através da rede.

Artigo 1(b) – Dados informatizados

25. A definição de dados informatizados assenta na definição de dados, de acordo com a norma ISO. Esta definição contém os termos "adequado para tratamento". Isto significa que os dados são colocados de tal forma que podem ser directamente processados pelo sistema informático. De modo a tornar claro que o termo "dados", ao abrigo da Convenção, deverá ser entendido como referindo-se a dados sob a forma electrónica ou outra forma directamente processável, foi introduzida a noção de "dados informatizados". Os dados informatizados que são automaticamente processados poderão constituir o alvo de uma das infracções penais definidas na presente Convenção, bem como o objecto de aplicação de uma das medidas de investigação definidas pela presente Convenção.

Artigo 1 (c) – Fornecedor de Serviços

26. O termo "fornecedor de serviços" cobre uma ampla categoria de pessoas que desempenham um papel particular no que diz respeito à comunicação ou ao tratamento de dados em sistemas informáticos (consultar igualmente os comentários relevantes na Secção 2). No ponto (i) da definição, refere-se explicitamente que se encontram abrangidas por este termo as entidades, tanto públicas como privadas, que proporcionam aos utilizadores a capacidade de comunicarem entre si. Assim sendo, é irrelevante o facto de saber se os utilizadores formam um grupo fechado ou se o fornecedor oferece os seus serviços ao público, quer gratuitamente quer mediante o pagamento de uma taxa. O grupo fechado poderá ser constituído, por exemplo, pelos funcionários de uma empresa privada à qual o serviço é oferecido através de uma rede corporativa.

27. No ponto (ii) da definição, refere-se explicitamente que o termo "fornecedor de serviços" também se aplica às entidades que procedem ao armazenamento, ou de uma outra forma, ao tratamento dos dados, em nome das pessoas mencionadas no ponto (i). Além disso, o termo inclui as entidades que procedem ao armazenamento, ou de outra forma, ao tratamento dos dados em nome dos utilizadores dos serviços daqueles mencionados no ponto (i). Por exemplo, de acordo com esta definição, um fornecedor de serviços engloba quer os serviços de hosting e caching, quer os serviços de ligação a uma rede. No entanto, um mero fornecedor de conteúdos (tal como uma pessoa que contrata uma empresa de hosting para armazenar a sua página web) não deverá ser abrangido por esta definição caso não ofereça igualmente serviços de comunicação ou serviços relacionados com o tratamento de dados.

Artigo 1 (d) – Dados de tráfego

28. Para os fins da presente Convenção, os dados de tráfego, tal como definidos no artigo 1, alínea d., constituem uma categoria de dados informatizados que se encontra sujeita a um regime jurídico específico. Estes dados são gerados por computadores na cadeia de comunicação de forma a encaminhar uma comunicação desde a sua origem até ao seu destino. São portanto elementos auxiliares da comunicação propriamente dita.

29. No caso da investigação de uma infracção penal cometida relativamente a um sistema informático, os dados de tráfego são necessários para localizar a origem de uma comunicação como ponto de partida para a recolha de provas adicionais ou como parte integrante da prova da infracção. Os dados de tráfego podem ter uma duração efémera, pelo que se torna necessário requerer a sua preservação expedita. Consequentemente, a sua rápida divulgação poderá ser necessária para distinguir o destino da comunicação, de modo a recolher provas complementares antes que tais dados sejam apagados, ou para efeitos de identificação de um suspeito. O procedimento normal de recolha e divulgação de dados informatizados poderá, pois, revelar-se insuficiente. Além disso, a recolha destes dados é encarada como implicando, em princípio, uma menor intrusão uma vez que se desconhece o conteúdo da comunicação que é visto como sendo mais delicado.

30. A definição inclui uma listagem exaustiva de categorias de dados de tráfego que são tratadas por um regime específico na presente Convenção: a origem de uma comunicação, o seu destino, o caminho, a hora, a data, a dimensão, a duração ou o tipo do serviço subjacente à mesma. Nem sempre todas estas categorias estarão tecnicamente disponíveis, serão passíveis de

ser produzidas por um fornecedor de serviços ou serão necessárias para uma dada investigação criminal. A "origem" refere-se a um número de telefone, um endereço IP (Protocolo da Internet) ou uma identificação semelhante de um dispositivo de comunicações ao qual um fornecedor de serviços presta os seus serviços. O "destino" refere-se a uma indicação comparável de dispositivo de comunicação ao qual são transmitidas as comunicações. O termo "tipo de serviço subjacente" refere-se ao tipo de serviço que é utilizado no seio da rede, por exemplo, a transferência de ficheiros, o correio electrónico ou o serviço de mensagens instantâneas.

31. A definição confere aos legisladores de cada país a possibilidade de introduzir uma diferenciação relativa à protecção jurídica dos dados de tráfego, em consonância com a sua sensibilidade. Neste contexto, o Artigo 15º obriga a que as Partes contemplem as condições e salvaguardas necessárias a uma adequada protecção das liberdades e dos direitos do ser humano. Isto implica, entre outros aspectos, que os critérios de fundo e o procedimento relativos à aplicação de um poder de investigação podem ser variáveis em função da sensibilidade dos dados.

Capítulo II – Medidas a empreender ao nível nacional

32. O Capítulo II (Artigos 2º – 22º) engloba três secções: direito penal substantivo (Artigos 2º - 13º), direito processual (Artigos 14º - 21º) e jurisdição (Artigo 22º).

Secção 1 – Direito penal substantivo

33. O objectivo da Secção 1 da Convenção (Artigos 2º a 13º) é o de melhorar os meios a serem utilizados no sentido da prevenção e eliminação do crime informático ou relacionado com computadores, através da determinação de uma norma mínima comum das respectivas infracções. Este tipo de harmonização representa um adjuvante no combate a estes crimes tanto no plano nacional como no plano internacional. A concordância nas legislações nacionais poderá evitar eventuais abusos resultantes de uma transferência para uma Parte que possuía anteriormente uma norma menos rigorosa. Consequentemente, também o útil intercâmbio de experiências comuns, em termos do tratamento prático dos casos, poderá ser assim intensificado. A cooperação internacional (em especial, na extradição e na assistência jurídica mútua) fica pois facilitada, por exemplo, no que toca aos requisitos de criminalidade dupla.

34. A lista de infracções incluídas representa um consenso mínimo e não exclui as respectivas extensões na legislação nacional. Em larga medida, a referida lista tem por base as directrizes traçadas relativamente à Recomendação Nº R (89) 9 do Conselho da Europa, sobre crime relacionado com computadores, e o trabalho desenvolvido por outras organizações internacionais públicas e privadas (OCDE, ONU, AIDP), mas tendo em conta experiências mais recentes que se prendem com a expansão abusiva de redes de telecomunicações.

35. A secção encontra-se dividida em cinco títulos. O Título 1 incluí o essencial das infracções relacionadas com computadores, das infracções que atentam contra a confidencialidade, a integridade e a disponibilidade dos sistemas informáticos e dos dados informatizados, representando estas as ameaças principais, tal como identificado nas discussões sobre a segurança de dados e computadores, às quais estão expostos os sistemas de comunicação e de tratamento de dados electrónicos. Sob este título descreve-se o tipo de crimes cobertos, isto é, o acesso não autorizado e a manipulação ilícita de sistemas, programas ou dados. Os Títulos 2 a 4 incluem outros tipos de "infracções relacionadas com computadores", que na prática desempenham um papel mais importante dado que os sistemas informáticos e de telecomunicações são utilizados como um meio para lesar determinados interesses legais que, na sua maioria, se encontram já protegidos pela legislação penal contra tais atentados através dos meios tradicionais. No Título 2 foram acrescentadas as infracções (falsificação e fraude relacionadas com computadores) na sequência das sugestões apresentadas pelas directrizes da Recomendação Nº R (89) 9 do Conselho da Europa. O Título 3 aborda as "infracções relacionadas com o conteúdo" ou a produção ou distribuição ilícitas de pornografia infantil por meio da utilização de sistemas informáticos, representando este, actualmente, um dos mais perigosos modi operandi. O Comité que elaborou a Convenção debateu a possibilidade de incluir outras infracções relacionadas com o conteúdo, tais como a distribuição de propaganda racista através de sistemas informáticos. Todavia, o comité não se encontrava em posição de alcançar um consenso no que respeita à criminalização de uma tal conduta. Se, por um lado, se constatava a existência de uma percentagem significativa a favor da introdução deste ponto enquanto infracção penal, algumas delegações manifestaram grande preocupação face à inclusão desta disposição apontando como fundamento a liberdade de expressão. Ciente da complexidade desta matéria, foi decidido que o Comité iria remeter ao Comité Europeu para os Problemas Criminais (CDPC) a questão da elaboração de um Protocolo adicional à presente Convenção. O Título 4 descreve as "infracções relacionadas com a violação dos direitos de autor e dos direitos conexos". Estas foram incluídas

na Convenção pelo facto de as violações dos direitos de autor constituírem uma das formas mais vulgarizadas de crime informático ou relacionado com computadores, cujas proporções têm vindo a ser alvo de preocupação a nível internacional. Finalmente, o Título 5 inclui disposições adicionais sobre tentativa, auxílio e cumplicidade, bem como sobre as respectivas sanções e medidas e, em conformidade com os recentes instrumentos internacionais aplicáveis, sobre a responsabilidade corporativa.

36. Embora as disposições do direito substantivo digam respeito às infracções cometidas por meio da utilização das tecnologias da informação, a Convenção recorre a uma linguagem neutra em termos tecnológicos, de modo a que as infracções definidas ao abrigo do direito penal substantivo possam ser aplicáveis quer às tecnologias actuais quer às tecnologias futuras envolvidas.

37. Os redactores da Convenção entenderam que as Partes poderão excluir as infracções menores ou insignificantes do campo de aplicação dos Artigos 2º - 10º.

38. Uma especificidade das infracções englobadas reside no requisito expresso de que a conduta em causa seja seguida "sem que tal direito lhe assista". Isto reflecte a noção de que a conduta descrita nem sempre é punível per se, mas poderá ser legal ou justificada não só em casos nos quais se aplicam as clássicas excepções prescritas nos termos da lei, como por exemplo o consentimento, a autodefesa ou a necessidade, mas também quando estamos perante outros princípios ou interesses que levam à exclusão da responsabilidade criminal. A expressão "sem direito" deve o seu significado ao contexto em que é utilizada. Assim, não constituindo uma restrição à forma como as Partes implementam o conceito na sua legislação interna, a expressão poderá referir-se a uma conduta seguida sem autoridade (quer seja de natureza legislativa, executiva, administrativa, judicial, contratual ou consensual) ou a uma conduta que não se encontra, de outra forma, coberta pelas defesas legais, alegações, justificações ou princípios relevantes ao abrigo da legislação nacional. A Convenção coloca, portanto, de lado a conduta assumida em consonância com a autoridade governamental legítima (por exemplo, quando o governo da Parte age no sentido de manter a ordem pública, proteger a segurança nacional ou investigar infracções penais). Além do mais, as actividades comuns e legítimas inerentes à concepção de redes, ou às práticas comuns de exploração e de comércio legítimas não deverão ser penalizadas. São, pois, enumerados exemplos específicos de tais excepções à criminalização, relativamente a infracções específicas, na parte correspondente do texto do Memorando Explicativo abaixo. Cabe assim às Partes determinar

a forma como tais exemplos são implementados no âmbito dos seus sistemas jurídicos internos (ao abrigo do direito penal ou outro).

39. Todas as infracções enunciadas na Convenção deverão ser cometidas "intencionalmente" para que seja imputável a responsabilidade criminal. Em determinados casos, a infracção inclui um elemento intencional específico adicional. Por exemplo, no Artigo 8º sobre fraude relacionada com computadores, a intenção de obter um benefício de cariz económico é um elemento constitutivo da infracção. Os redactores do projecto de Convenção acordaram que o significado exacto do termo "intencionalmente" deveria ser deixado aos critérios de interpretação nacionais.

40. Certos artigos desta secção permitem subordinar a implementação da Convenção na legislação nacional a determinadas circunstâncias condicionantes. Noutros casos, é mesmo concedida a possibilidade de formular uma reserva (cf. Artigos 40º e 42º). Estas diferentes modalidades de uma abordagem mais restritiva da criminalização, traduzem a existência de diferentes avaliações do perigo inerente ao comportamento envolvido, ou da necessidade de utilização do direito penal como uma medida repressiva. Esta abordagem confere uma certa flexibilidade aos governos e parlamentos no que se refere à determinação da sua política penal nesta área.

41. As leis que regulamentam estas infracções deverão ser elaboradas com a maior clareza e especificidade possíveis, de modo a conferir uma previsibilidade adequada do tipo de conduta que irá resultar numa sanção penal.

42. No decorrer do processo de elaboração do projecto, os redactores ponderaram a conveniência de criminalização de outras condutas que não as definidas nos Artigos 2º a 11º, nomeadamente o chamado "cyber-squatting", isto é, o facto de registar um nome de domínio que é idêntico ou ao nome de uma entidade já existente e em geral conhecida ou à denominação comercial ou marca registada de um produto ou de uma empresa. Os "cyber-squatters" não têm intenção de fazer um uso activo do nome de domínio e procuram obter uma vantagem financeira, forçando a entidade em causa, ainda que indirectamente, a pagar a transferência de propriedade para readquirir o controlo sobre o seu nome de domínio. Actualmente, esta conduta é considerada como sendo uma questão relacionada com as marcas. Uma vez que as violações das marcas registadas não se encontram regulamentadas pela presente Convenção, os redactores julgaram não ser apropriado tratar a questão da criminalização de tal conduta.

Título 1 - Infracções relativas à confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informatizados

43. As infracções penais definidas ao abrigo dos Artigos 2º a 6º destinam-se a proteger a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informatizados, e não a criminalizar as actividades legítimas e comuns inerentes à concepção de redes ou às práticas comuns de exploração e de comércio.

Acesso ilícito (Artigo 2º)

44. O termo "Acesso ilícito" abrange basicamente a infracção relativa às perigosas ameaças e atentados à segurança (isto é, confidencialidade, integridade e disponibilidade) dos sistemas informáticos e dados informatizados. A necessidade de protecção reflecte os interesses de organizações e indivíduos em gerir, operar e controlar os seus sistemas de forma livre e tranquila. A mera intrusão não autorizada, ou seja, o "*hacking*" (pirataria), o *"cracking"* (desprotecção) ou o delito de "fraude informática" ou "invasão" de um sistema informático deverão, em princípio, ser ilegais por si mesmos. Tal poderá representar um obstáculo ou conduzir a situações de impedimentos relativamente aos utilizadores legítimos de sistemas e dados, podendo provocar a sua alteração ou destruição com elevados custos de reconstrução. As ditas intrusões poderão dar acesso a dados confidenciais (incluindo "passwords", informação sobre o sistema visado) e códigos secretos, para fins de utilização gratuita do sistema, podendo mesmo incentivar os piratas informáticos a cometer infracções relacionadas com computadores sob formas mais perigosas, tais como a falsificação ou a fraude informáticas.

45. O meio mais viável de prevenção do acesso não autorizado é, evidentemente, a introdução e o desenvolvimento de medidas de segurança eficazes. Contudo, uma resposta abrangente terá igualmente que englobar a ameaça e a utilização de medidas contempladas no direito penal. Uma interdição penal de acesso não autorizado poderá conferir uma protecção adicional ao sistema e aos dados e, numa primeira fase, também uma protecção contra os perigos acima mencionados.

46. O termo "Acesso" entende-se como sendo a entrada no todo ou numa parte de um sistema informático (hardware, componentes, dados armazenados no sistema instalado, directorias, dados de tráfego e dados relativos ao conteúdo). No entanto, não inclui o simples envio por correio electrónico de uma mensagem ou ficheiro para esse sistema. "Acesso" inclui a penetração

noutro sistema informático, acessível através de redes de telecomunicações públicas, ou num sistema informático na mesma rede, tal como uma LAN (rede de área local) ou Intranet no seio de uma organização (rede privada de uma empresa). O método de comunicação (por exemplo, à distância, incluindo através de ligações sem fio ou de curto alcance) não é importante.

47. O acto deverá ser praticado "sem direito". Em complemento da explicação dada anteriormente sobre esta expressão, tal significa que não existe penalização do acesso autorizado, pelo proprietário ou outro titular do direito sobre o sistema ou parte do mesmo (como por exemplo, para efeitos de teste ou protecção do sistema informático em questão). Além disso, não existe criminalização associada ao facto de se aceder a um sistema informático que permite o acesso livre e aberto ao público, uma vez que tal acesso se faz "com direito".

48. A aplicação de ferramentas técnicas específicas poderá implicar um acesso nos termos referidos no Artigo 2º, como é o caso do acesso a uma página na web, directamente ou através de ligações de hipertexto, incluindo os "deep-links" ou a aplicação de "cookies" ou "bots" para localizar e recuperar informação no interesse da comunicação. A aplicação das referidas ferramentas por si só não constitui uma forma não autorizada ou "sem direito". A manutenção de uma página Web pública implica o consentimento por parte do seu proprietário de que a mesma poderá ser acedida por qualquer outro utilizador da Web. A aplicação das ferramentas previstas nos programas e protocolos de comunicação geralmente utilizados, não constitui por si só uma forma não autorizada ou "sem direito", nomeadamente quando se considera que o titular do direito sobre o sistema acedido aceitou a sua aplicação, por exemplo, no caso dos "cookies", ao não ter recusado a sua instalação inicial ou por não ter procedido à sua remoção.

49. A legislação interna vigente em vários países contempla já algumas disposições relativas a infracções de "pirataria" mas o âmbito e os elementos constituintes das mesmas variam consideravelmente. A abordagem geral de criminalização que se apresenta na primeira frase do Artigo 2º não é, pois, incontestável. A oposição surge a partir de situações em que a simples intrusão não deu forçosamente origem a quaisquer perigos, ou de casos em que os actos de pirataria conduziram mesmo à detecção de lacunas e fraquezas na segurança dos sistemas. Isto levou a que, numa série de países, se tenha optado por uma abordagem mais restrita que exige condicionantes suplementares para que se possa falar de infracção, indo ao encontro da abordagem adoptada pela Recomendação Nº (89) 9 e da proposta do Grupo de Trabalho da OCDE datada de 1985.

50. As Partes poderão considerar a abordagem mais geral e penalizar a pirataria, pura e simples, de acordo com a primeira frase do Artigo 2º. Alternativamente, as Partes poderão fixar quaisquer ou todos os elementos condicionais listados na segunda frase: violação de medidas de segurança, especial intenção de obter dados informatizados ou outra intenção desonesta que justifique a culpabilidade criminal, ou o requisito de que a infracção seja cometida em relação a um sistema informático que se encontre conectado remotamente a um outro sistema informático. Esta última opção permite que as Partes excluam a situação em que se verifica o acesso físico de uma pessoa a um computador cujo funcionamento é autónomo, e sem qualquer utilização de outro sistema informático. As Partes poderão limitar a infracção ao acesso ilícito a sistemas de computadores que operam em rede (incluindo as redes públicas servidas através de serviços de telecomunicações e redes privadas, tais como as Intranets ou Extranets).

Intercepção ilícita (Artigo 3º)

51. Esta disposição tem por objectivo proteger o direito à privacidade na comunicação de dados. A infracção representa a mesma violação da privacidade de comunicações que as tradicionais escutas e gravações de conversas telefónicas entre indivíduos. O direito à privacidade de correspondência encontra-se contemplado no Artigo 8º da Convenção Europeia sobre os Direitos do Homem. A infracção definida ao abrigo do Artigo 3º aplica este princípio a todas as formas de transferência electrónica de dados, quer se trate de uma transferência por telefone, fax, correio electrónico ou ficheiro.

52. O texto da referida disposição reporta-se principalmente ao da infracção relativa a "intercepção não autorizada" contido na Recomendação (89) 9. Na presente Convenção ficou explícito que as comunicações envolvidas dizem respeito a "transmissões de dados informatizados", bem como a radiação electromagnética nas circunstâncias abaixo descritas.

53. A intercepção por "meios técnicos" refere-se à escuta, monitorização ou vigilância do conteúdo das comunicações, à obtenção do conteúdo dos dados quer directamente, através do acesso e utilização do sistema informático, quer indirectamente, através da utilização de dispositivos electrónicos de intercepção de mensagens ou de escuta clandestina. A intercepção poderá igualmente envolver a gravação. Os meios técnicos englobam os equipamentos técnicos ligados a linhas de transmissão, bem como os dispositivos de recolha e gravação de comunicações sem fio. Poderão incluir o uso de software,

"passwords" e códigos. O requisito da utilização de meios técnicos constitui uma condição restritiva a fim de evitar a sobrepenalização.

54. A infracção aplica-se a transmissões "não públicas" de dados informatizados. O termo "não públicas" delimita a natureza do processo de transmissão (comunicação) e não a natureza dos dados transmitidos. Os dados comunicados poderão ser informação disponível ao público, mas as partes desejarem comunicar confidencialmente. Ou os dados poderão ser mantidos em sigilo para fins comerciais até que o serviço seja remunerado, tal como acontece com a televisão por assinatura, sujeita a pagamento. Portanto, o termo "não públicas" não exclui per se as comunicações efectuadas através de redes públicas. As comunicações de funcionários, quer se destinem ou não a fins profissionais, que constituam "transmissões não públicas de dados informatizados" encontram-se igualmente protegidas contra a intercepção não autorizada ao abrigo do disposto no Artigo 3º (consultar, por exemplo, a Sentença proferida pelo Tribunal Europeu dos Direitos do Homem (TEDH) no caso Halford vs. Reino Unido, datada de 25 de Junho de 1997, 20605/92).

55. A comunicação sob a forma de transmissão de dados informatizados poderá ter lugar no interior de um único sistema informático (por exemplo, o fluxo de dados que é enviado da CPU para o monitor ou impressora), entre dois sistemas informáticos pertencentes à mesma pessoa, dois computadores em comunicação entre si, ou entre um computador e uma pessoa (por exemplo, através do teclado). No entanto, as Partes poderão requerer como condição suplementar que a comunicação seja transmitida entre sistemas informáticos com ligação remota.

56. Deverá ser salientado que o facto de a noção de "sistema informático" poder também incluir as ligações de rádio, não significa que a Parte fique obrigada a penalizar a intercepção de qualquer transmissão de rádio que, embora "não pública", ocorra de uma forma relativamente aberta e facilmente acessível e que portanto possa ser interceptada, por exemplo por radioamadores.

57. A instituição de uma infracção relativa às "emissões electromagnéticas" imprime um âmbito mais alargado à disposição. As emissões electromagnéticas poderão ser provenientes de um computador durante o seu funcionamento. As referidas emissões não são consideradas como "dados" de acordo com a definição constante do Artigo 1º. No entanto, os dados podem ser reconstituídos a partir dessas emissões. Assim sendo, a intercepção de dados a partir de emissões electromagnéticas de um sistema informático, encontra-se classificada como uma infracção ao abrigo da presente disposição.

58. Para que seja imputável a responsabilidade criminal, a intercepção ilícita deverá ser praticada "intencionalmente" e "sem direito". O acto é justificado, por exemplo, se à pessoa que efectua a intercepção assistir o direito de o fazer, se a mesma estiver a agir sob as instruções ou com a autorização dos participantes na transmissão (incluindo no contexto de actividades autorizadas de teste ou de protecção aprovadas pelos participantes), ou se a vigilância for legalmente autorizada pelas entidades responsáveis por uma investigação, no interesse da segurança nacional ou da detecção de infracções. Entende-se igualmente que as práticas comerciais comuns, tal como a utilização de "cookies", não deverão ser penalizadas enquanto tal, uma vez que não se tratam de intercepções "sem direito". No que respeita às comunicações não públicas dos funcionários, as quais se encontram protegidas em virtude do Artigo 3º (consultar o parágrafo 54 acima), a legislação nacional poderá prever um fundamento legítimo para uma tal intercepção. Em conformidade com o disposto no Artigo 3º, a intercepção nas referidas circunstâncias considerar-se-á como tendo sido efectuada de forma autorizada ou "com direito".

59. Em alguns países, a intercepção poderá estar intimamente ligada à infracção de acesso não autorizado a um sistema informático. A fim de garantir a uniformidade ao nível da interdição e da aplicação da lei, os países que requerem que a infracção seja cometida com uma intenção desonesta ou em relação a um sistema informático que, por sua vez, se encontre conectado a um outro sistema, de acordo com o Artigo 2º, poderão igualmente requerer outras condições adicionais para que a responsabilidade criminal seja imputável ao abrigo do presente artigo. Estes elementos deverão ser interpretados e aplicados em conjunto com outros elementos relativos à infracção, tais como a "intencionalidade" e a "não autorização".

Interferência nos dados (Artigo 4º)

60. A presente disposição visa assegurar aos dados e programas informáticos uma protecção semelhante aquela de que gozam os bens corpóreos relativamente aos danos ocasionados de forma deliberada. Neste caso, os interesses jurídicos protegidos são a integridade e o adequado funcionamento ou a correcta utilização dos dados e programas informáticos armazenados.

61. No parágrafo 1, os termos "danificação" e "deterioração" enquanto actos de sobreposição, referem-se em particular a uma alteração negativa da integridade ou do conteúdo informativo dos dados ou programas. A "eliminação" de dados corresponde à destruição de bens corpóreos, uma vez que os suprime e os torna irreconhecíveis. A supressão de dados informatizados significa todo e qualquer

acto no sentido de impedir ou extinguir a disponibilização dos dados à pessoa que tem acesso ao computador ou ao suporte no qual os dados se encontravam armazenados. O termo "alteração" significa a modificação dos dados existentes. A introdução de códigos dolosos, tais como vírus e rotinas como os chamados "cavalos de Tróia", encontra-se pois abrangida por este parágrafo, da mesma maneira que a modificação dos dados resultante deste acto.

62. Os actos supracitados apenas serão passíveis de punição se forem cometidos "sem direito". As actividades comuns inerentes à concepção de redes ou às práticas comuns de exploração e de comércio, como é o caso das operações de teste ou de protecção da segurança de um sistema informático, quando autorizadas pelo proprietário ou operador, ou ainda da reconfiguração do sistema operativo de um computador, que normalmente é efectuada aquando da aquisição de novo software por parte do operador de um sistema (por exemplo, software de acesso à Internet que desactiva os programas equivalentes previamente instalados), considera-se serem realizadas "com direito" e não são portanto penalizadas pelo presente artigo. A modificação de dados de tráfego para fins de viabilização de comunicações anónimas (por exemplo, as actividades de sistemas de re-expedição anónima), ou a modificação de dados para fins de protecção das comunicações (por exemplo, a encriptação), deveriam em princípio ser consideradas como servindo os fins legítimos de protecção da privacidade e, por esse motivo, ser entendidas como sendo efectuadas de forma autorizada. Todavia, as Partes poderão desejar que sejam penalizados certos actos abusivos relativos a comunicações anónimas, tal como no caso de alteração da informação no cabeçalho de um pacote de dados a fim de ocultar a identidade do autor de um crime.

63. Além disso, o infractor deverá ter agido "intencionalmente".

64. O Parágrafo 2 permite que as Partes formulem uma reserva relativamente à infracção, na medida em que poderão requerer que um tal comportamento acarrete um prejuízo grave. A interpretação dos aspectos que constituem o prejuízo grave é da competência dos legisladores de cada país, devendo pois notificar o Secretário Geral do Conselho da Europa sobre a sua interpretação, caso recorram a esta possibilidade de formulação de reserva.

Interferência no sistema (Artigo 5º)

65. A Recomendação Nº 89 (9) refere-se a esta rubrica designando-a por sabotagem informática. A presente disposição tem como finalidade a penalização do impedimento intencional da utilização legítima de sistemas informáticos,

nos quais se incluem sistemas de telecomunicações, utilizando ou influenciando os dados informáticos. O interesse jurídico protegido, neste caso, reside no interesse de operadores e utilizadores de sistemas informáticos e de telecomunicações em que os mesmos apresentem um funcionamento adequado. O texto utiliza, assim, uma linguagem neutra para que todos os tipos de funções possam ficar abrangidos.

66. Pelo termo "impedimento" entende-se todo e qualquer acto que interfira com o correcto funcionamento do sistema informático. O referido impedimento deverá ter lugar através da introdução, transmissão, danificação, eliminação, alteração ou supressão de dados informatizados.

67. O impedimento deverá ainda ser "grave" para que possa dar origem a uma sanção penal. Cada Parte deverá determinar, individualmente, quais os critérios a seguir ou os requisitos a preencher de forma a que o impedimento seja considerado "grave". Uma Parte poderá, por exemplo, requerer uma quantidade mínima de danos causados de modo a que o impedimento seja tido como grave. Os redactores consideraram "grave" o envio de dados para um sistema particular, sob uma forma e com uma dimensão ou frequência susceptíveis de produzir efeitos nocivos no que respeita à capacidade de utilização do sistema, por parte do proprietário ou do operador, ou de comunicação com outros sistemas (por exemplo, por meio de programas que geram interferências no sistema sob a forma de problemas de "recusa de serviço", códigos dolosos, tais como vírus que obstam à operação do sistema ou provocam um abrandamento substancial da velocidade de operação do mesmo, ou ainda, de programas que enviam enormes quantidades de correio electrónico para um destinatário de maneira a bloquear as funções de comunicação do sistema).

68. O impedimento deverá ser causado "sem direito". As actividades comuns inerentes à concepção de redes ou às práticas comuns de exploração e de comércio, consideram-se ser levadas a cabo "com direito". É o caso, por exemplo, das operações de teste ou de protecção da segurança de um sistema informático, quando autorizadas pelo proprietário ou operador, ou ainda da reconfiguração do sistema operativo de um computador que normalmente é efectuada aquando da instalação de novo software por parte do operador de um sistema e que desactiva os programas equivalentes previamente instalados. Portanto, o presente artigo não penaliza uma tal conduta, mesmo que esta cause um impedimento grave.

69. O envio de mensagens de correio electrónico não solicitadas, para fins comerciais ou outros, poderá causar transtornos ao seu destinatário, em especial quando estas mensagens são enviadas em grandes quantidades

ou com uma elevada frequência ("spamming"). Na opinião dos redactores, a referida conduta somente deverá ser penalizada em caso de impedimento grave e intencional da comunicação. Não obstante, as Partes poderão adoptar diferentes abordagens do impedimento, ao abrigo das suas legislações nacionais, por exemplo, considerando determinados actos de impedimento como sendo infracções de natureza administrativa ou sujeitando-os à aplicação de outras sanções. O texto permite às Partes decidir em que medida terá que ser colocado o entrave ao sistema - parcial ou totalmente, temporária ou permanentemente – de forma a atingir o limite a partir do qual passa a justificar-se a aplicação de uma sanção administrativa ou penal, ao abrigo da sua legislação interna.

70. A infracção deverá ser cometida intencionalmente, ou seja, o infractor deverá ter a intenção de provocar um impedimento grave.

Utilização indevida de equipamentos (Artigo 6º)

71. A presente disposição estabelece como sendo uma infracção penal distinta e independente, a prática intencional de actos ilegais específicos relativamente a certos dispositivos ou dados de acesso, indevidamente utilizados para cometer as infracções acima descritas contra a confidencialidade, integridade e disponibilidade dos sistemas ou dados informáticos. Dado que a prática de tais infracções exige frequentemente a posse de meios de acesso ("ferramentas de pirataria") ou outros instrumentos, verifica-se um forte incentivo à aquisição dos mesmos para fins criminais, o que poderá pois conduzir à criação de uma espécie de mercado negro para a sua produção e distribuição. De modo a combater estes riscos mais eficazmente, o direito penal deveria interditar na sua origem, alguns actos específicos, especialmente perigosos, antes de serem cometidas as infracções a que se referem os Artigos 2º a 5º. Quanto a este aspecto, a disposição baseia-se nos recentes desenvolvimentos ocorridos ao nível do Conselho da Europa (Convenção Europeia sobre a protecção jurídica dos serviços que se baseiem ou consistam num acesso condicional – STE nº 178) e da União Europeia (Directiva 98/84/CE do Parlamento Europeu e do Conselho de 20 de Novembro de 1998 relativa à protecção jurídica dos serviços que se baseiem ou consistam num acesso condicional) bem como nas respectivas disposições adoptadas em alguns países. Uma abordagem semelhante fora igualmente adoptada na Convenção de Genebra de 1929 sobre a falsificação de moeda.

72. O parágrafo 1(a)1 penaliza a produção, a venda, a obtenção para utilização, a importação, a distribuição ou, de outra forma, a disponibilização de

um dispositivo, incluindo um programa informático, concebido ou adaptado basicamente com a finalidade de cometer quaisquer das infracções definidas ao abrigo dos Artigos 2º a 5º da presente Convenção. O termo "distribuição" refere-se ao acto de enviar dados para terceiros, enquanto o termo "disponibilização" se refere à colocação de dispositivos on-line para utilização de terceiros. Este termo também engloba a criação ou compilação de hiperligações de modo a facilitar o acesso a tais dispositivos. A menção a um "programa informático" refere-se a programas que são, por exemplo, concebidos para alterar ou mesmo destruir dados, ou para interferir na operação de sistemas, tais como programas de vírus, ou a programas concebidos ou adaptados para permitir o acesso a sistemas informáticos.

73. Os redactores debateram longamente a questão de se os dispositivos abrangidos deveriam limitar-se aos dispositivos que são concebidos exclusiva ou especificamente para a prática de infracções, excluindo assim os dispositivos de utilização dupla. No entanto, esta abordagem foi considerada como sendo demasiado restritiva, podendo dar origem a dificuldades insuperáveis no que diz respeito à definição da prova no âmbito das acções penais intentadas, e assim, tornar esta disposição praticamente inaplicável ou aplicável apenas em raras circunstâncias. A alternativa de inclusão de todos os dispositivos, incluindo aqueles cuja produção e distribuição é legal, foi igualmente rejeitada. Deste modo, apenas o elemento subjectivo da intenção de cometer uma infracção informática, poderia ser decisivo em termos da imposição de uma punição, abordagem essa que também não foi adoptada na área da falsificação de moeda. A Convenção adopta uma posição de compromisso razoável, limitando o seu âmbito de aplicação aos casos em que os dispositivos são objectivamente concebidos, ou adaptados, essencialmente para efeitos de cometimento de uma infracção, o que por si só irá, normalmente, excluir os dispositivos de utilização dupla.

74. O parágrafo 1(a)2 penaliza a produção, a venda, a obtenção para utilização, a importação, a distribuição ou, de outra forma, a disponibilização de uma password, um código de acesso ou dados semelhantes, por meio dos quais é possível aceder integral ou parcialmente a um sistema informático.

75. O parágrafo 1(b) institui enquanto infracção penal a posse dos elementos descritos no parágrafo 1(a)1 ou 1(a)2. De acordo com o teor da última frase do parágrafo 1(b), as Partes ficam autorizadas a exigir, nos termos da lei, a posse de um determinado número dos referidos elementos. O número de elementos possuídos está directamente relacionado com a prova de intenção criminal.

Cabe, pois, a cada Parte decidir qual o número de elementos exigido para que seja imputável a responsabilidade criminal.

76. A infracção deverá ser cometida intencionalmente e sem direito. De forma a evitar o perigo de sobrepenalização, nos casos em que os dispositivos são produzidos e colocados no mercado para fins legítimos, por exemplo, para fazer face aos golpes contra os sistemas informáticos, são adicionados elementos suplementares a fim de restringir a infracção. Para além do requisito geral de intenção, dever-se-á estar na presença de uma intenção específica (isto é, directa) de que o dispositivo seja utilizado para efeitos de cometer qualquer uma das infracções definidas nos Artigos 2º a 5º da Convenção.

77. O parágrafo 2 define, claramente, que as ferramentas criadas para a execução de operações autorizadas de teste ou de protecção de sistemas informáticos não se encontram cobertas pela presente disposição. Este conceito é já subjacente à expressão "sem direito". Por exemplo, os dispositivos de teste (dispositivos de cracking) e os dispositivos de análise de redes concebidos por este sector da indústria, com o objectivo de controlar a fiabilidade dos seus produtos de tecnologia da informação, ou de testar a segurança dos seus sistemas, são fabricados para fins legítimos, pelo que se considera serem utilizados "com direito".

78. Constatando-se a existência de diferentes avaliações da necessidade de aplicar a infracção de "Utilização indevida de equipamentos" a todos os tipos de infracções informáticas mencionadas nos Artigos 2º a 5º, o parágrafo 3 permite, com base na formulação de uma reserva, limitar a infracção ao abrigo da legislação interna das Partes. Cada Parte obrigar-se-á, contudo, a penalizar, pelo menos, a venda, a distribuição ou a disponibilização de uma password ou dados de acesso a computadores, tal como descrito no parágrafo 1 (a) 2.

Título 2 – Infracções relacionadas com computadores

79. Os artigos 7º a 10º dizem respeito a infracções comuns que são frequentemente cometidas por meio da utilização de um sistema informático. A maioria dos Estados já definiu a criminalização destas infracções comuns, pelo que as suas legislações internas serão ou não suficientemente abrangentes para englobar situações que envolvam redes informáticas (por exemplo, as leis em vigor nalguns países, relativamente à pornografia infantil, poderão não ser aplicáveis a imagens electrónicas). Portanto, aquando da implementação destes artigos, os Estados deverão proceder a uma análise das suas leis vigentes, de forma a determinar se as mesmas são aplicáveis a situações que impliquem

a utilização de redes ou sistemas informáticos. Caso as infracções instituídas ao abrigo da legislação nacional contemplem já a referida conduta, não será necessário modificar tais disposições nem proceder à elaboração de novas disposições nesse sentido.

80. Os artigos intitulados "falsificação relacionada com computadores" e "fraude relacionada com computadores" referem-se a determinadas infracções relacionadas com computadores, isto é, à falsificação relacionada com computadores e à fraude relacionada com computadores enquanto dois tipos específicos de manipulação de dados ou de sistemas informáticos. A inclusão destas infracções reflecte a realidade patente em vários países, de que determinados interesses jurídicos tradicionais não se encontram suficientemente protegidos contra as novas formas de interferência e de golpes.

Falsificação relacionada com computadores (Artigo 7º)

81. O objectivo deste artigo é o de instituir uma infracção paralela à falsificação de documentos tangíveis, isto é, em suporte de papel. A sua finalidade é a de colmatar as lacunas existentes ao nível do direito penal relativamente à clássica falsificação, a qual exige uma legibilidade visual das declarações contidas num documento e não se aplica aos dados armazenados electronicamente. As manipulações de tais dados com valor probatório poderão acarretar as mesmas consequências graves que os tradicionais actos de falsificação, caso se verifique a indução em erro de terceiros. A falsificação relacionada com computadores consiste na criação ou alteração não autorizada de dados armazenados, de forma a que os mesmos se revistam de um valor probatório diferente e que as transacções legais, baseadas na autenticidade da informação veiculada por esses dados, sejam objecto de dolo. Neste caso, o interesse jurídico protegido será o da segurança e credibilidade dos dados electrónicos que poderão ter consequências ao nível das relações jurídicas.

82. Deverá ser salientado o facto de que os conceitos nacionais de falsificação poderão variar significativamente. Um dos conceitos assenta na autenticidade de acordo com o autor do documento, enquanto outros se baseiam na veracidade da declaração contida no documento. Todavia, ficou acordado que o dolo relativo à autenticidade se refere, no mínimo, ao emissor dos dados, não obstante a exactidão ou veracidade do conteúdo dos dados. As Partes poderão ir mais além e especificar que o termo "autêntico" se aplica também ao carácter genuíno dos dados.

83. A presente disposição aplica-se a dados que equivalem a um documento público ou privado que produz os seus efeitos em termos jurídicos. A "introdução" não autorizada de dados correctos ou incorrectos dá origem a uma situação que corresponde à elaboração de um documento falso. As alterações subsequentes (modificações, variações, mudanças parciais), eliminações (remoção de dados de um suporte de dados) e supressão (retenção e ocultação de dados) correspondem, de um modo geral, à falsificação de um documento autêntico.

84. A expressão "para fins legais" refere-se igualmente às transacções e aos documentos jurídicos que são relevantes nos termos da lei.

85. A última frase desta disposição permite que as Partes, ao implementarem a infracção ao abrigo da sua legislação interna, possam requerer adicionalmente uma intenção fraudulenta ou uma intenção desonesta semelhante, para que seja imputável a responsabilidade criminal.

Fraude relacionada com computadores (Artigo 8º)

86. A revolução tecnológica veio multiplicar as possibilidades de cometer infracções de cariz económico, tais como as fraudes, das quais citamos as fraudes verificadas com os cartões de crédito. Os activos representados ou administrados por sistemas informáticos (fundos electrónicos, dinheiro de depósitos) tornaram-se alvo de manipulações da mesma maneira que as tradicionais formas de propriedade. Estes crimes consistem principalmente na manipulação da entrada no sistema, em que são introduzidos dados incorrectos, ou em manipulações de programas e outras interferências no tratamento dos dados. O objectivo deste artigo é o de penalizar toda e qualquer manipulação indevida durante o tratamento dos dados, cuja intenção seja a de efectuar uma transferência de propriedade ilegal.

87. De modo a garantir que todas as formas relevantes de manipulações se encontram abrangidas, os elementos constitutivos de "introdução", "alteração", "eliminação" ou "supressão" que constam do artigo 8º(a) são complementados pelo acto geral de "interferência no funcionamento de um programa ou sistema informático" tal como mencionado no artigo 8º(b). Os elementos de "introdução, alteração, eliminação ou supressão revestem-se do mesmo significado que nos artigos anteriores. O artigo 8º(b) cobre actos tais como as manipulações de hardware, os actos que impedem as saídas para a impressora, bem como os actos que afectam o registo ou o fluxo de dados, ou a sequência pela qual os programas são executados.

88. As manipulações informáticas fraudulentas serão penalizadas caso as mesmas resultem directamente em perdas materiais ou económicas de terceiros e caso o infractor tenha agido com a intenção de obter uma vantagem lucrativa ilícita para si próprio ou por conta de outrém. A expressão "perdas materiais ou económicas", implicando uma noção generalizada, inclui o prejuízo monetário bem como as perdas de bens corpóreos e incorpóreos aos quais é atribuído um valor económico.

89. A infracção deverá ser cometida "sem direito", e o benefício económico terá igualmente que ser obtido sem que tal direito lhe assista. Naturalmente, que as práticas comerciais legítimas comuns que visam a obtenção de um benefício económico não são consideradas como fazendo parte integrante da infracção definida pelo presente artigo, uma vez que são levadas a cabo de forma autorizada e com direito a tal. Por exemplo, as actividades realizadas em consonância com o disposto num contrato válido entre as partes interessadas, são pois realizadas "com direito" (por exemplo, desactivar uma página da Web em virtude dos termos e condições do contrato).

90. A infracção deverá ser cometida "intencionalmente". O elemento geral de intenção prende-se com a manipulação ou a interferência informática passíveis de causar perdas de propriedade a terceiros. A infracção exige igualmente que exista uma intenção fraudulenta específica ou outra intenção desonesta de obtenção de uma vantagem de cariz económico ou outro, em favor do próprio ou de terceiros. Assim, por exemplo, as práticas comerciais relativas à competitividade no mercado, que são susceptíveis de ocasionar um prejuízo económico a uma pessoa e um benefício para outra pessoa, mas que não são levadas a cabo com uma intenção fraudulenta ou desonesta, não constituem uma infracção tal como definida pelo presente artigo. Por exemplo, a utilização de programas de recolha de informação para estabelecer a concorrência no seio da Internet ("bots"), mesmo que não autorizada por uma página visitada pelo "bot" não se pressupõe como devendo ser criminalizada.

Título 3 – Infracções relacionadas com o conteúdo

Infracções relacionadas com pornografia infantil (Artigo 9º)

91. O Artigo 9º sobre pornografia infantil visa reforçar as medidas de protecção relativas às crianças, nestas se incluindo a sua protecção contra a exploração sexual, através da modernização das disposições do direito penal, de modo a circunscrever mais eficazmente o uso de sistemas informáticos no contexto dos crimes de natureza sexual praticados contra menores.

92. A presente disposição veio dar resposta à preocupação manifestada pelos Chefes de Estado e de Governo do Conselho da Europa, aquando da realização da sua 2ª Cimeira (Estrasburgo, 10 e 11 de Outubro de 1997), no seu Plano de Acção (alínea III.4) e corresponde a uma tendência a que se assiste, ao nível internacional, no sentido da proibição da pornografia infantil, tal como demonstrado pela recente adopção do Protocolo Opcional relativo à Convenção das Nações Unidas sobre os Direitos da Criança, no que concerne à venda de crianças, à prostituição de menores e à pornografia infantil, bem como pela recente iniciativa da Comissão Europeia relativa à luta contra a exploração sexual de crianças e a pornografia infantil (COM2000/854).

93. Esta disposição penaliza os vários aspectos inerentes à produção electrónica, posse e distribuição de pornografia infantil. A maioria dos Estados contemplam já a penalização da clássica produção e distribuição física de artigos de pornografia infantil mas, a par com a crescente utilização da Internet como instrumento de base para a comercialização desse material, surgiu a necessidade imperativa de recorrer a disposições específicas no âmbito de um instrumento jurídico internacional, afigurando-se estas como essenciais no combate a esta nova forma de exploração sexual e de risco para as crianças. Existe a forte convicção de que o referido material e as práticas on-line que lhe estão associadas, tais como a troca de ideias, fantasias e conselhos entre pedófilos, contribuem para apoiar, incentivar ou facilitar os crimes de natureza sexual praticados contra as crianças.

94. O parágrafo 1(a) penaliza a produção de pornografia infantil para fins de distribuição através de um sistema informático. Esta disposição foi considerada útil para a prossecução da luta contra os perigos acima mencionados, logo desde a sua origem.

95. O parágrafo 1(b) institui enquanto infracção penal a "oferta" de pornografia infantil através de um sistema informático. O termo "oferta" deverá ser entendido como cobrindo o acto de solicitar de terceiros a obtenção de pornografia infantil. Isto torna implícito que a pessoa que oferece o material em questão pode, efectivamente, fornecê-lo. A expressão "disponibilização" entende-se como abrangendo a colocação de pornografia infantil on-line para uso por parte de terceiros, como por exemplo, por meio da criação de sites de pornografia infantil. Este parágrafo aplica-se igualmente à criação ou compilação de hiperligações a sites de pornografia infantil de modo a facilitar o acesso à pornografia infantil.

96. O parágrafo 1(c) penaliza a distribuição ou transmissão de pornografia infantil através de um sistema informático. O termo "distribuição" significa a

disseminação activa do material. O envio de pornografia infantil, através de um sistema informático, para outra pessoa seria abordado pela infracção de "transmitir" pornografia infantil.

97. A expressão "obter para si próprio ou para terceiros" no parágrafo 1(d) significa a obtenção activa de pornografia infantil, isto é, por exemplo através do seu descarregamento (download) num sistema informático.

98. A posse de pornografia infantil num sistema informático ou num suporte de armazenamento de dados, tal como uma disquete ou um CD-Rom é criminalizada segundo o disposto no parágrafo 1(e). A posse de artigos de pornografia infantil estimula a procura do referido material. Uma forma eficaz de pôr termo à produção de pornografia infantil é o estabelecimento e agravamento de sanções penais inerentes à conduta de cada participante na cadeia desde a produção até à posse.

99. A expressão "material pornográfico" no parágrafo 2 deverá ser interpretada em conformidade com as normas nacionais, estando incluída na classificação de materiais como sendo obsceno, incompatível com a moral pública ou, de algum modo, tendo efeitos perversos. Assim sendo, o material ao qual se reconheça um interesse do ponto de vista artístico, médico ou científico, não deverá ser considerado como sendo pornográfico. Os meios de representação visual englobam os dados armazenados em computador, disquete ou outro suporte de armazenamento electrónico, passível de ser convertido para uma imagem visual.

100. Um "comportamento sexualmente explícito" abrange, pelo menos, os seguintes comportamentos reais ou simulados: a) relações sexuais – incluindo as genitais-genitais, orais-genitais, anais-genitais ou orais-anais, - entre menores, ou entre um adulto e um menor, do mesmo sexo ou do sexo oposto; b) relações sexuais entre um ser humano e um animal; c) masturbação; violência sado-masoquista num contexto sexual; ou e) exibição lasciva das partes genitais ou da zona púbica de um menor. Não se considera importante o facto de a conduta representada ser real ou simulada.

101. Os três tipos de material definidos no parágrafo 2 para os fins de cometimento das infracções contidas no parágrafo 1, abrangem as representações reais de abuso sexual de crianças (2a), imagens pornográficas de uma pessoa aparentando ser um menor envolvido numa conduta explicitamente de natureza sexual (2b), e por fim, imagens que, embora "realistas", não espelham efectivamente um menor envolvido numa conduta explicitamente de natureza sexual (2c). Este último caso inclui imagens alvo de alterações, tais como

imagens metamorfoseadas ("morfismo"), ou até mesmo imagens inteiramente geradas por computador.

102. Nos três casos citados no parágrafo 2, os interesses jurídicos protegidos são ligeiramente diferentes. O parágrafo 2(a) focaliza-se mais directamente na protecção das crianças relativamente a abusos sexuais. Os parágrafos 2(b) e 2(c) destinam-se a proporcionar uma protecção contra um comportamento que, embora não prejudique necessariamente a "criança" representada no material em questão, uma vez que a criança pode não ser real, seja susceptível de incentivar ou seduzir as crianças a participarem em tais actos, e assim, fazerem parte de uma sub-cultura que preconiza o abuso de crianças.

103. A expressão "sem direito" não exclui as excepções e defesas legais ou outros princípios ou justificações semelhantes que isentem uma pessoa da responsabilidade criminal sob determinadas circunstâncias específicas. Deste modo, a expressão "sem direito" permite que a Parte tenha em consideração os direitos fundamentais, tais como a liberdade de pensamento, a liberdade de expressão e o respeito pela vida privada. Adicionalmente, uma Parte poderá prever, no âmbito da sua legislação interna, uma excepção relativa a comportamentos que se prendam com "material pornográfico" passível de apresentar um interesse artístico, médico ou científico. Quanto ao parágrafo 2(b), a referência à expressão "sem direito" poderá também, por exemplo, autorizar uma Parte a exonerar uma pessoa de responsabilidade criminal, no caso de a pessoa representada não ser um menor nos termos a que se refere a presente disposição.

104. No que respeita à pornografia infantil em geral, o parágrafo 3 define o termo "menor" como referindo-se a todos os indivíduos com idade inferior a 18 anos, de acordo com a definição de "criança" constante da Convenção das Nações Unidas sobre os Direitos da Criança (Artigo 1º). Considerou-se ser uma questão de base importante o facto de se estabelecer uma norma internacional uniformizada relativamente à idade. Deverá salientar-se que a idade se refere à utilização de crianças (reais ou fictícias) como objectos sexuais, sendo distinta da idade consentida para se ter relações sexuais. Não obstante, e reconhecendo o facto de que em determinados países foi estipulada uma idade limite inferior, ao abrigo da legislação nacional aplicável às questões de pornografia infantil, a última frase do parágrafo 3 autoriza as Partes a definirem um limite de idade diferente, desde que o mesmo não seja inferior a 16 anos.

105. Este artigo enumera os diferentes tipos de actos ilícitos relacionados com pornografia infantil e que, tal como prescrito pelos artigos 2º a 8º, as Partes

ficam obrigadas a penalizar desde que praticados "intencionalmente". Em conformidade com este critério, uma pessoa não poderá ser responsabilizada a menos que estejamos perante uma intenção de oferecer, disponibilizar, distribuir, transmitir, produzir ou possuir artigos de pornografia infantil. As Partes poderão adoptar uma norma mais específica (consultar, por exemplo, a legislação aplicável da Comunidade Europeia relativamente à responsabilidade de fornecedores de serviços), devendo, nesse caso, reger-se pela referida norma. Por exemplo, a responsabilidade será imputável caso exista um "conhecimento e controlo" em relação à informação transmitida ou armazenada. Não será suficiente, por exemplo, que um fornecedor de serviços desempenhe um papel de intermediário no contexto da transmissão deste material, através de uma página Web ou de canais de notícias (newsrooms) que contenham o referido material, sem que esteja preenchido o requisito intencional, neste caso particular, em virtude do disposto na legislação nacional. Além do mais, um fornecedor de serviços não é obrigado a monitorizar tais condutas e conteúdos a fim de evitar a responsabilidade criminal.

106. O parágrafo 4 autoriza as Partes a formularem reservas no que concerne ao disposto pelos parágrafos 1(d) e (e), e 2(b) e (c). O direito à não aplicação destas secções da disposição poderá ser exercido total ou parcialmente. Toda e qualquer reserva, tal como mencionada anteriormente, deverá ser comunicada ao Secretário Geral do Conselho da Europa aquando da assinatura ou do depósito dos instrumentos de ratificação, aceitação, aprovação ou adesão da Parte, em conformidade com o Artigo 42º.

Título 4 – Infracções relacionadas com a violação dos direitos de autor e dos direitos conexos

Infracções relacionadas com a violação dos direitos de autor e dos direitos conexos (Artigo 10º)

107. As violações dos direitos de propriedade intelectual, nomeadamente dos direitos de autor, contam-se entre as infracções que mais frequentemente são cometidas na Internet, e que constituem motivo de preocupação tanto para os titulares de direitos de autor como para todos aqueles que, no exercício da sua actividade profissional, lidam com redes informáticas. A reprodução e disseminação na Internet de obras protegidas, sem o prévio consentimento do titular do direito de autor, são extremamente frequentes. As referidas obras protegidas incluem obras literárias, fotográficas, musicais, audiovisuais e outras. A facilidade com que é possível efectuar cópias não autorizadas devido ao recurso à tecnologia digital e a escala de reprodução

e disseminação das mesmas no contexto de redes electrónicas, fez surgir a necessidade de incluir novas disposições nas sanções decorrentes do direito penal, bem como de reforçar a cooperação internacional neste campo.

108. Em virtude dos acordos citados neste artigo, cada Parte obrigar-se-á a penalizar as violações deliberadas de direitos de autor e direitos conexos, sempre que tais violações sejam cometidas por meio de um sistema informático e a uma escala comercial. O parágrafo 1 prevê as sanções penais aplicáveis a violações de direitos de autor por meio de um sistema informático. A violação dos direitos de autor encontra-se já instituída como infracção penal ao abrigo das legislações em vigor na grande maioria dos países. O parágrafo 2 trata da violação dos direitos conexos por meio de um sistema informático.

109. A violação quer dos direitos de autor, quer dos direitos conexos, encontra-se definida ao abrigo da legislação aplicável de cada Parte e em conformidade com as obrigações assumidas pela Parte relativamente a determinados instrumentos internacionais. Embora cada Parte fique obrigada a instituir enquanto infracções penais as referidas violações, a forma específica como essas violações são definidas ao abrigo das legislações nacionais poderá variar de país para país.

110. No que se refere ao parágrafo 1, os acordos mencionados são o Acto de Paris datado de 24 de Julho de 1971, a Convenção de Berna para a Protecção das Obras Literárias e Artísticas, o Acordo sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados com o Comércio (TRIPS), e o Tratado da Organização Mundial de Propriedade Intelectual (OMPI) sobre os Direitos de Autor. No que respeita ao parágrafo 2, os instrumentos internacionais citados são a Convenção Internacional para a Protecção dos Artistas intérpretes ou executantes, dos Produtores de Fonogramas e dos Organismos de Radiodifusão, (Convenção de Roma), o Acordo sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados com o Comércio, e o Tratado da Organização Mundial de Propriedade Intelectual (OMPI) sobre Prestações e Fonogramas. A utilização, em ambos os parágrafos, da expressão "em conformidade com as obrigações assumidas" significa que uma Parte contratante da presente Convenção não ficará obrigada a aplicar as disposições decorrentes dos acordos citados, dos quais não constitua uma Parte. Além disso, no caso de uma Parte ter formulado uma reserva ou declaração autorizada em virtude de um dos referidos acordos, uma tal reserva poderá limitar o campo de aplicação da obrigação assumida ao abrigo da presente Convenção.

111. Os Tratados da OMPI sobre os Direitos de Autor e sobre Prestações e Fonogramas não entraram em vigor à data de conclusão da presente Convenção. Todavia, os referidos tratados são importantes na medida em que representam uma actualização significativa da protecção da propriedade industrial na cena internacional (em especial no que toca ao novo direito de "disponibilização" de material protegido "mediante solicitação" através da Internet), assim como um aperfeiçoamento dos meios de combate às violações dos direitos de propriedade intelectual, a nível mundial. Contudo, entendeu-se que as violações dos direitos definidas por estes tratados não deverão ser criminalizadas ao abrigo da presente Convenção até que os referidos tratados entrem em vigor relativamente a uma Parte.

112. A obrigação de instituir enquanto infracções penais as violações dos direitos de autor e dos direitos conexos, em conformidade com as obrigações assumidas ao abrigo de instrumentos de âmbito internacional, não se aplica a quaisquer direitos morais conferidos pelos referidos instrumentos (tal como no Artigo 6ºbis da Convenção de Berna e no Artigo 5º do Tratado sobre os Direitos de Autor da OMPI).

113. As infracções relativas a direitos de autor e direitos conexos deverão ser cometidas "deliberadamente" para que seja imputável a responsabilidade criminal. Contrariamente a todas as restantes disposições de direito substantivo constantes da presente Convenção, é utilizado o termo "deliberadamente" em vez de "intencionalmente" em ambos os parágrafos 1 e 2, dado ser este o termo empregue no Acordo sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados com o Comércio (Artigo 61º), o qual regulamenta a obrigação de penalizar as violações dos direitos de autor.

114. As disposições têm por objectivo prever sanções penais relativamente a violações cometidas "à escala comercial" e por meio de um sistema informático, o que se afigura em consonância com o Artigo 61º do Acordo sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados com o Comércio, na medida em que este impõe sanções penais relativas a questões de direitos de autor, somente no caso de "pirataria à escala comercial". No entanto, as Partes poderão desejar ultrapassar o limite da "escala comercial" e penalizar igualmente outros tipos de violações da propriedade intelectual.

115. A expressão "sem direito" foi omitida do texto deste artigo por motivos de redundância, uma vez que o termo "violação" já denota a utilização não autorizada de material protegido por direitos de autor. A ausência da expressão "sem direito" não exclui, pelo contrário, a aplicação das excepções e alegações

legais ou de princípios ou justificações semelhantes que regulamentam a exclusão da responsabilidade criminal, associados à expressão "sem direito" utilizada noutros artigos da Convenção.

116. O parágrafo 3 permite que as Partes não imponham a responsabilidade criminal ao abrigo dos parágrafos 1 e 2 em "circunstâncias limitadas" (por exemplo, no caso de importações paralelas e dos direitos de locação), desde que a lei preveja outras soluções eficazes, nas quais se incluem medidas civis e/ou administrativas. Esta disposição concede, essencialmente, às Partes uma isenção limitada da obrigação de imputar a responsabilidade criminal, no sentido em que aquelas não ficam desobrigadas dos compromissos assumidos em virtude do prescrito pelo Artigo 61º do Acordo sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados com o Comércio, o qual constitui o requisito mínimo de penalização pré-existente.

117. O presente artigo não deverá, de forma alguma, ser interpretado como alargando a protecção conferida a autores, produtores cinematográficos, artistas, produtores de fonogramas, organismos de radiodifusão ou outros titulares de direitos, a indivíduos que não satisfaçam os critérios de elegibilidade em conformidade com as disposições da legislação nacional ou de um acordo de âmbito internacional.

Título 5 – Responsabilidade acessória e sanções

Tentativa e auxílio ou cumplicidade (Artigo 11º)

118. O objectivo deste artigo é o de estabelecer infracções suplementares relativas à tentativa e auxílio ou cumplicidade na prática das infracções definidas na Convenção. Tal como veremos mais adiante, não é exigido que uma Parte proceda à penalização da tentativa de cometer cada infracção definida ao abrigo da Convenção.

119. O parágrafo 1 determina que as Partes deverão instituir como infracções penais o auxílio ou a cumplicidade na prática de quaisquer das infracções definidas ao abrigo do disposto nos artigos 2º a 10º. A responsabilidade advém do auxílio ou da cumplicidade nos casos em que a pessoa que comete uma infracção definida pela Convenção é apoiada por outra pessoa que pretende igualmente que a infracção seja cometida. Por exemplo, embora a transmissão de dados de conteúdo prejudiciais ou de códigos dolosos através da Internet requeira a assistência de fornecedores de serviços enquanto intermediários, um fornecedor de serviços que não apresente qualquer

intenção criminal não poderá ser responsabilizado ao abrigo do disposto nesta secção. Assim, não existe qualquer dever, por parte de um fornecedor de serviços, de fiscalizar activamente os conteúdos em causa de modo a evitar a responsabilidade criminal, tal como definida nesta disposição.

120. Quanto ao parágrafo 2 sobre a tentativa, considerou-se que existe uma probabilidade muito pequena de algumas das infracções definidas pela Convenção, ou dos elementos constitutivos destas infracções, poderem ocasionar uma tentativa (é o caso, por exemplo, dos elementos relativos ao facto de se oferecer ou disponibilizar artigos de pornografia infantil). Além disso, existem alguns sistemas jurídicos que limitam as infracções relativamente às quais a tentativa é punível. Assim sendo, apenas se exige que a tentativa seja penalizada no caso das infracções estipuladas de acordo com o disposto nos artigos 3º, 4º, 5º, 7º, 8º, 9º(1)(c).

121. Tal como se verifica com todas as infracções definidas em conformidade com as disposições da Convenção, a tentativa e o auxílio ou a cumplicidade deverão ocorrer de forma intencional.

122. O parágrafo 3 foi acrescentado com a finalidade de abordar as dificuldades eventualmente sentidas pelas Partes relativamente ao parágrafo 2, dado os conceitos largamente variáveis adoptados pelas diferentes legislações e apesar do esforço subjacente ao teor do parágrafo 2 no sentido de retirar determinados aspectos do campo de aplicação da disposição relativa à tentativa. Uma Parte poderá reservar-se o direito de não aplicar as disposições constantes do parágrafo 1 na sua totalidade ou em parte. Isto significa que qualquer Parte que formule uma reserva relativamente a esta disposição, não terá qualquer obrigação de penalizar a tentativa, podendo mesmo seleccionar as infracções ou as partes constitutivas das infracções às quais irá aplicar sanções penais referentes à tentativa. A reserva tem por objectivo permitir, ao maior número de países possível, a ratificação da Convenção ao mesmo tempo que confere às Partes a possibilidade de preservar alguns dos seus conceitos jurídicos fundamentais.

Responsabilidade corporativa (Artigo 12º)

123. O Artigo 12º trata da responsabilidade das pessoas colectivas. As disposições do referido artigo encontram-se a par com a actual tendência, a nível jurídico, de reconhecimento da responsabilidade das pessoas colectivas. Tem, pois, por objectivo imputar a responsabilidade às empresas, associações e pessoas colectivas semelhantes no que se refere a actos passíveis de penalização, cometidos por uma pessoa que ocupe uma posição de liderança no seio da

pessoa colectiva, sempre que tais actos sejam praticados por conta da referida pessoa colectiva. O artigo 12º contempla igualmente a responsabilidade de uma pessoa que ocupe um cargo de direcção ou uma posição de liderança e se abstenha de exercer o seu controlo e supervisão sobre um funcionário ou um representante da pessoa colectiva, nos casos em que tal omissão facilite a prática, por parte do referido funcionário ou representante, de uma das infracções definidas na Convenção.

124. De acordo com o disposto no parágrafo 1, será necessário satisfazer quatro condições de maneira a que a responsabilidade seja imputável. Primeiramente, deverá ter sido cometida uma das infracções descritas na Convenção. Segundo, a infracção deverá ter sido cometida por conta da pessoa colectiva. Terceiro, a infracção (incluindo o auxílio e a cumplicidade) deverá ter sido cometida por uma pessoa que ocupe um cargo de direcção ou uma posição de liderança. A expressão "uma pessoa que ocupe uma posição de liderança" refere-se a uma pessoa física que tenha um cargo superior no seio da organização, tal como é o caso de um director. E, por fim, a pessoa que ocupe uma posição de liderança deverá ter agido com base numa das suas competências – um poder de representação ou uma autoridade para tomar decisões ou exercer o seu controlo – o que demonstra que a referida pessoa física agiu dentro dos limites permitidos pela sua autoridade, imputando assim a responsabilidade à pessoa colectiva. Em suma, o parágrafo 1 obriga as Partes a dispor dos meios necessários para imputar a responsabilidade à pessoa colectiva, somente no caso de infracções cometidas por pessoas que ocupem posições de liderança.

125. Adicionalmente, o parágrafo 2 obriga as Partes a disporem da capacidade para imputar a responsabilidade a uma pessoa colectiva, nos casos em que a infracção tenha sido cometida não pela pessoa que ocupe uma posição de liderança, tal como descrito no parágrafo 1, mas por uma outra pessoa que actue sob a autoridade da pessoa colectiva, isto é, um dos seus funcionários ou representantes agindo no âmbito das suas competências. As condições que deverão ser preenchidas para que a responsabilidade seja imputável são as seguintes: (1) uma infracção que foi cometida por um funcionário ou representante da pessoa colectiva, (2) a infracção foi cometida por conta e para benefício da pessoa colectiva, (3) a prática da infracção foi proporcionada pela ausência de supervisão ou controlo por parte da pessoa que ocupa a posição de liderança relativamente ao referido funcionário ou representante. Neste contexto, a inexistência de supervisão deverá ser entendida como englobando a omissão em termos da adopção das medidas razoáveis e apropriadas, no sentido de impedir que os funcionários ou representantes se envolvam

em actividades ilegais em nome da pessoa colectiva. As referidas medidas razoáveis e apropriadas poderão ser determinadas por diversos factores, tais como o tipo de empresa, a sua dimensão, as normas aplicáveis ou as boas práticas em vigor, etc. Tal não deverá, pois, ser interpretado como exigindo a implementação de um regime geral de vigilância sobre as comunicações dos funcionários (consultar também o parágrafo 54). Um fornecedor de serviços não incorrerá em quaisquer responsabilidades pelo facto de um cliente, um utilizador ou um terceiro, ter cometido uma infracção no seu sistema, dado que a expressão "agindo sob a sua autoridade" se aplica exclusivamente a funcionários e representantes que actuem no quadro das suas competências.

126. De acordo com este artigo, a responsabilidade poderá ser de natureza criminal, civil ou administrativa. Cada Parte dispõe da flexibilidade necessária para decidir estipular todas ou quaisquer destas formas de responsabilidade, de acordo com os seus princípios jurídicos, desde que satisfaçam os critérios descritos no Artigo 13º, parágrafo 2, no sentido de a sanção ou medida aplicável ser "eficaz, proporcional e dissuasiva" e abranger sanções de cariz monetário.

127. O parágrafo 4 especifica que a responsabilidade corporativa não exclui a responsabilidade individual.

Sanções e medidas (Artigo 13º)

128. Este artigo possui uma estreita ligação com os Artigos 2º a 11º, os quais definem os vários crimes informáticos ou crimes relacionados com computadores que devem ser punidos ao abrigo da lei penal. De acordo com as obrigações decorrentes destes artigos, a presente disposição obriga as Partes contratantes a estipular as consequências resultantes da natureza grave das referidas infracções, ao prever as sanções penais aplicáveis que deverão ser "eficazes, proporcionais e dissuasivas" e, no caso das pessoas físicas, incluir penas de prisão.

129. As pessoas colectivas cuja responsabilidade deva ser definida em conformidade com o Artigo 12º deverão ficar sujeitas à aplicação de sanções "eficazes, proporcionais e dissuasivas" que poderão ser de natureza criminal, administrativa ou civil. Assim, as Partes contratantes obrigar-se-ão, em virtude do disposto no parágrafo 2, a regulamentar a possibilidade de aplicação de sanções pecuniárias a pessoas colectivas.

130. Este artigo deixa em aberto a possibilidade de outras sanções ou medidas que reflictam a gravidade das infracções, tais como medidas que incluam

a ordem de interdição ou confiscação. Caberá às Partes, no exercício do seu poder discricionário, criar um sistema de infracções penais e sanções que seja compatível com os sistemas jurídicos existentes ao nível nacional.

Secção 2 – Direito Processual

131. Os artigos da presente Secção descrevem determinadas medidas processuais a serem empreendidas ao nível nacional, para efeitos de investigação criminal relativamente às infracções definidas na Secção 1, a outras infracções penais cometidas por meio de um sistema informático e à recolha de provas, sob a forma electrónica, de uma infracção penal. De acordo com o prescrito pelo Artigo 39º, parágrafo 3, não consta da Convenção nenhuma disposição que obrigue ou convide as Partes a estipular outros poderes ou procedimentos que não aqueles contemplados pela presente Convenção, nem que obste a que uma Parte o possa fazer.

132. A revolução tecnológica, que engloba a "auto-estrada da informação electrónica", na qual se encontram interrelacionadas e interligadas inúmeras formas de comunicação e serviços através da partilha de meios e suportes de transmissão comuns, veio introduzir algumas alterações na esfera do direito penal e do processo penal. A rede de comunicações, em constante expansão, abre novas perspectivas à criminalidade, quer em termos das clássicas infracções quer a nível de crimes inerentes às novas tecnologias. Não só as disposições do direito penal substantivo deverão acompanhar estas novas formas abusivas, como também o código de processo penal e as técnicas de investigação. Do mesmo modo, as salvaguardas também deverão ser adaptadas ou desenvolvidas a fim de se manterem a par com o novo meio tecnológico e os novos poderes processuais.

133. Um dos maiores desafios que se colocam, no contexto do combate ao crime praticado no seio de redes informáticas, é a dificuldade de identificação do infractor, bem como de avaliação da extensão e do impacto dessa mesma infracção. Um outro problema prende-se com a volatilidade dos dados electrónicos, uma vez que estes são passíveis de serem alterados, transferidos ou eliminados apenas em alguns segundos. Temos, por exemplo, o caso de um utilizador que efectua o controlo dos dados e que poderá utilizar o sistema informático para apagar os dados que constituem o objecto de uma dada investigação criminal, destruindo assim as provas existentes. A rapidez e, por vezes, o sigilo representam frequentemente factores cruciais para o êxito de uma investigação.

134. A Convenção adapta certas medidas processuais clássicas, tal como a busca e a apreensão, ao novo ambiente tecnológico. Paralelamente, foram criadas novas medidas, tais como a preservação expedita de dados, de forma a assegurar que as tradicionais medidas de recolha, como a busca e a apreensão, mantêm a sua eficácia num meio tecnológico que se caracteriza pela volatilidade. Visto que os dados, inseridos no novo ambiente tecnológico, nem sempre são estáticos mas poderão circular ao longo do processo de comunicação, procedeu-se igualmente à adaptação de outros procedimentos de recolha tradicionais relativos às telecomunicações, tais como a recolha de dados de tráfego e a intercepção de dados de conteúdo em tempo real, a fim de permitir efectuar a recolha de dados electrónicos durante o processo de comunicação. Algumas de entre estas medidas encontram-se definidas pela Recomendação Nº R (95) 13, do Conselho da Europa, relativa aos problemas de direito processual penal relacionados com as tecnologias da informação.

135. Todas as disposições a que faz referência a presente Secção, têm como objectivo viabilizar a obtenção ou a recolha de dados para fins de investigações criminais ou acções penais específicas. Os redactores da presente Convenção debateram a questão de saber se a Convenção deveria impor, aos fornecedores de serviços, a obrigação de recolher e conservar regularmente os dados de tráfego, por um período de tempo determinado, não tendo no entanto procedido à inclusão de uma tal obrigação por motivos de inexistência de consenso sobre este assunto.

136. De um modo geral, os procedimentos referem-se a todos os tipos de dados, incluindo três tipos específicos de dados informatizados (dados de tráfego, dados de conteúdo e dados relativos aos subscritores), os quais podem existir sob duas formas (armazenados ou presentes no processo de comunicação). As definições de alguns destes termos são apresentadas nos Artigos 1º e 18º. A aplicabilidade de um procedimento a um tipo ou a uma forma de dados electrónicos, em particular, depende da natureza e formato dos dados bem como da natureza do procedimento, tal como especificamente mencionado em cada artigo.

137. Ao adaptar as leis processuais clássicas ao novo meio tecnológico, surge a questão da terminologia apropriada, no âmbito das disposições da presente secção. As opções resumiam-se a manter a linguagem tradicional ("busca" e "apreensão"), utilizar novos termos informáticos mais orientados para o domínio tecnológico ("acesso" e "cópia") –como adoptados nos textos de outras instâncias internacionais relativas a este assunto (tal como o Subgrupo do G8 especializado em crime de alta tecnologia) – ou adoptar uma solução de

compromisso em que a linguagem seria mista ("a investigação, ou de forma semelhante, o acesso" e "a apreensão, ou de forma semelhante, a guarda"). Uma vez reconhecida a importância de que o meio electrónico reflicta a evolução dos conceitos, identificando e mantendo as suas raízes tradicionais, foi seguida uma abordagem flexível que consiste em permitir que os Estados utilizem quer as antigas noções de "busca e apreensão" quer as novas noções de "acesso e cópia".

138. Todos os artigos incluídos na presente Secção fazem referência às "autoridades competentes" e aos respectivos poderes de que deverão ser investidas para fins de investigações criminais ou acções penais específicas. Em determinados países, somente os juizes dispõem de poderes para ordenar ou autorizar a recolha ou a produção de provas, enquanto que, noutros países, os promotores de justiça ou outras entidades que zelam pela aplicação da lei encontram-se investidos de poderes idênticos ou semelhantes. De onde se conclui que a expressão "autoridade competente" se refere, assim, a toda e qualquer autoridade judicial, administrativa ou outra que zele pela aplicação da lei e que se encontre, ao abrigo da legislação nacional, investida dos poderes necessários para ordenar, autorizar ou executar as medidas processuais cujo objecto seja a recolha ou a produção de provas relativamente a investigações criminais ou acções penais específicas.

Título 1 – Disposições comuns

139. A Secção começa com duas disposições de âmbito geral que se aplicam a todos os artigos relacionados com o direito processual.

Âmbito das disposições processuais (Artigo 14º)

140. Cada Estado Parte obrigar-se-á a adoptar as medidas do foro legislativo e outras que se revelem necessárias, de acordo com as leis vigentes internamente e com o contexto jurídico, de modo a estipular os poderes e procedimentos descritos na presente Secção para fins de "investigações criminais ou acções penais específicas".

141. Encontrando-se sujeita a duas excepções, cada Parte deverá aplicar os poderes e procedimentos descritos em conformidade com a presente Secção a: (i) infracções penais definidas de acordo com a Secção 1 da Convenção; (ii) outras infracções penais cometidas por meio de um sistema informático; e (iii) à recolha de provas sob a forma electrónica relativamente a uma infracção penal. Assim, para efeitos de investigações criminais ou acções penais

específicas, os poderes e procedimentos referidos nesta Secção deverão ser aplicados às infracções definidas de acordo com a Convenção, a outras infracções penais cometidas por meio de um sistema informático, e à recolha de provas sob a forma electrónica relativamente a uma infracção penal. Fica, deste modo, assegurada a obtenção ou recolha de provas sob a forma electrónica relativamente a uma infracção penal, em virtude da aplicação dos poderes e procedimentos estabelecidos na presente Secção. Garante-se, ainda, uma capacidade equivalente ou paralela de obtenção ou recolha de dados informatizados, tal como se verifica ao nível dos poderes e procedimentos tradicionais relativos a dados não electrónicos. A Convenção especifica que as Partes podem incluir nas suas legislações internas a possibilidade de a informação contida em formato digital ou outro formato electrónico poder ser utilizada como prova, no contexto de acções penais em Tribunal, independentemente da natureza da infracção penal que está a ser julgada.

142. Existem, pois, duas excepções a este âmbito de aplicação. Primeiramente, o Artigo 21º estabelece que o poder de intercepção de dados de conteúdo deverá ser limitado a um conjunto de infracções graves a ser determinado pela legislação nacional. Muitos Estados limitam o poder de intercepção de telecomunicações ou comunicações verbais a uma série de infracções graves, pelo facto de reconhecerem o carácter privado das telecomunicações ou comunicações verbais, bem como o carácter de intrusão desta medida de investigação. Da mesma forma, a presente Convenção apenas exige que as Partes definam os poderes e procedimentos de intercepção relativamente a dados de conteúdo de comunicações informáticas específicas, no que concerne a um conjunto de infracções graves a ser determinado pela legislação nacional.

143. Em segundo lugar, uma Parte poderá reservar-se o direito de aplicar as medidas prescritas pelo Artigo 20º (recolha de dados de tráfego em tempo real) somente às infracções ou categorias de infracções especificadas na reserva formulada, desde que o conjunto das referidas infracções ou categorias de infracções não seja mais restrito do que o conjunto das infracções às quais se aplicam as medidas de intercepção mencionadas no Artigo 21º. Alguns Estados consideram a recolha de dados de tráfego como sendo equivalente à recolha de dados de conteúdo, em termos de privacidade e de intrusão. O direito à formulação de reserva permitiria a estes Estados limitarem a aplicação das medidas de recolha de dados de tráfego, em tempo real, ao mesmo conjunto de infracções ao qual aplicam os poderes e procedimentos de intercepção de dados de conteúdo em tempo real. Contudo, muitos Estados não consideram

a intercepção de dados de conteúdo e a recolha de dados de tráfego como sendo equivalentes em termos dos interesses de privacidade e do grau de intrusão que lhes são inerentes, uma vez que a recolha de dados de tráfego, por si só, não recolhe nem divulga o conteúdo da comunicação. Visto que a recolha de dados de tráfego em tempo real poderá revestir-se grande importância no que respeita à localização da origem e do destino das comunicações efectuadas por meio de sistemas informáticos (contribuindo assim para a identificação dos infractores), a Convenção convida as Partes que exercem o seu direito de reserva a limitarem a mesma, de forma a permitir a aplicação, tão alargada quanto possível, dos poderes e procedimentos definidos para a recolha, em tempo real, de dados de tráfego.

144. O parágrafo (b) prevê a possibilidade de formulação de reserva no caso de países que, devido a limitações existentes na sua legislação interna, não reúnem as condições necessárias para proceder à intercepção de comunicações efectuadas através de sistemas informáticos que são operados para benefício de um grupo fechado de utilizadores, e que não recorrem a redes públicas de comunicações nem se encontram conectados a outros sistemas informáticos. A expressão "grupo fechado de utilizadores" refere-se, por exemplo, a um número limitado de utilizadores pelo facto de estes se encontrarem associados a um fornecedor de serviços, como por exemplo os funcionários de uma empresa aos quais é conferida a possibilidade de comunicarem entre si através de uma rede informática. A expressão "não conectados a outros sistemas informáticos" significa que, aquando da emissão de uma ordem, tal como prevista pelos Artigos 20º ou 21º, o sistema através do qual as comunicações são transmitidas não possui uma ligação física ou lógica com outro sistema informático. A expressão "não recorre a redes públicas de comunicações" exclui os sistemas que utilizam redes informáticas públicas (incluindo a Internet), redes telefónicas públicas ou outros meios de telecomunicações públicos na transmissão das suas comunicações, quer a referida utilização seja ou não do conhecimento dos utilizadores.

Condições e salvaguardas (Artigo 15º)

145. A definição, implementação e aplicação dos poderes e procedimentos mencionados na presente Secção da Convenção deverão ficar sujeitas às condições e salvaguardas previstas nos termos da legislação interna de cada Parte. Embora as Partes fiquem obrigadas a introduzir certas disposições de direito processual na sua legislação nacional, as modalidades de definição e implementação destes poderes e procedimentos no quadro do seu sistema

jurídico, e a aplicação dos referidos poderes e procedimentos a casos específicos, serão da competência da legislação nacional e dos procedimentos internos de cada Parte. A dita legislação nacional e os procedimentos internos, tal como se descreve abaixo de forma mais pormenorizada, deverão incluir condições ou salvaguardas, as quais poderão ser instituídas de forma constitucional, legislativa, judicial ou outra. As modalidades deverão englobar a adição de certos elementos enquanto condições ou salvaguardas que permitam atingir um equilíbrio entre os requisitos de aplicação da lei e a protecção dos direitos e liberdades fundamentais do Homem. 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. As Partes deverão certificar-se de que as referidas condições e salvaguardas contemplam uma adequada protecção das liberdades e direitos do ser humano. Existem algumas normas comuns ou salvaguardas mínimas, às quais as Partes contratantes da Convenção deverão aderir, a saber, normas ou salvaguardas mínimas decorrentes das obrigações assumidas por uma Parte ao abrigo dos instrumentos internacionais aplicáveis, relativos aos direitos do Homem. Entre os referidos instrumentos contam-se, nomeadamente, a Convenção do Conselho da Europa para a Protecção dos Direitos do Homem e das Liberdades Fundamentais dos Cidadãos, datada de 1950, e os seus Protocolos Adicionais números 1, 4, 6, 7 e 12 (STE nº 005[4], 009, 046, 114, 117 e 177), no que respeita aos Estados europeus que são Partes contratantes dos mesmos. Citamos ainda outros instrumentos internacionais relativos aos Direitos do Homem, aplicáveis aos Estados de outras regiões do mundo (por exemplo, a Convenção Americana sobre os Direitos do Homem, datada de 1969, e a Carta Africana dos Direitos do Homem e dos Povos, datada de 1981), que são Partes nestes instrumentos, bem como o Pacto Internacional relativo aos Direitos Civis e Políticos, celebrado em 1966 e ratificado por um elevado número de Estados a nível mundial. Adicionalmente, são de sublinhar

4. O texto da Convenção foi modificado de acordo com as disposições constantes do Protocolo Nº 3 (STE nº 45), o qual entrou em vigor a 21 de Setembro de 1970, do Protocolo Nº 5 (STE nº 55), o qual entrou em vigor a 20 de Dezembro de 1971 e do Protocolo Nº 8 (STE nº 118), o qual entrou em vigor a 1 de Janeiro de 1990, e incluía igualmente o texto do Protocolo Nº 2 (STE nº 44), o qual, em conformidade com o Artigo 5º, parágrafo 3, fez parte integrante da Convenção desde a sua entrada em vigor à data de 21 de Setembro de 1970. Todas as disposições alvo de modificações ou aditamentos por meio dos referidos Protocolos foram substituídas pelo Protocolo Nº 11 (STE nº 155), a contar da sua entrada em vigor a 1 de Novembro de 1998. A partir dessa data, o Protocolo Nº 9 (STE nº 140), o qual entrou em vigor a 1 de Outubro de 1994, foi declarado nulo e o Protocolo Nº 10 (STE nº 146) cessou o seu objecto.

as protecções análogas previstas ao abrigo das legislações vigentes na grande maioria dos Estados.

146. Uma outra salvaguarda que consta da Convenção é a de que os poderes e procedimentos deverão "integrar o princípio da proporcionalidade". A proporcionalidade deverá ser implementada por cada uma das Partes, em conformidade com os princípios relevantes da sua legislação nacional. No que diz respeito aos países Europeus, decorrerá dos princípios estabelecidos em virtude da Convenção do Conselho da Europa para a Protecção dos Direitos do Homem e das Liberdades Fundamentais dos Cidadãos, datada de 1950, assim como da sua jurisprudência aplicável e da legislação e jurisprudência nacionais, que os poderes e os procedimentos deverão ser proporcionais à natureza e às circunstâncias da infracção. Outros Estados aplicarão princípios análogos da sua legislação, tais como as limitações relativas às ordens de produção e as exigências de fundamentação, aplicáveis às buscas e apreensões. Da mesma maneira, também a limitação que figura explicitamente no Artigo 21º, de que as obrigações relativas às medidas de intercepção sejam, no que se refere a uma série de infracções graves, determinadas pela legislação nacional, constitui um exemplo concreto da aplicação do princípio da proporcionalidade.

147. Sem limitar os tipos de condições e de salvaguardas eventualmente aplicáveis, a Convenção requer especificamente que tais condições e salvaguardas incluam, em função da natureza do poder ou do procedimento, uma supervisão por parte de um órgão judicial ou outro independente, os fundamentos justificativos da aplicação do poder ou do procedimento, e a limitação relativa ao âmbito ou à duração dos mesmos. Caberá às legislações nacionais determinar, aquando da aplicação das obrigações internacionais vinculatórias para a Parte e dos princípios estabelecidos internamente, quais os poderes e procedimentos que, pelo seu grau de intrusão, podem implicar a implementação de condições e salvaguardas particulares. Tal como mencionado no parágrafo 215, as partes deverão aplicar também, claramente, condições e salvaguardas particulares no que respeita à intercepção, por questões que se prendem, mais uma vez, com o seu grau de intrusão. Paralelamente, as referidas salvaguardas não necessitam, por exemplo, de ser igualmente aplicadas à preservação. Entre outras salvaguardas que devem ser tratadas pela legislação nacional, contam-se o direito contra a auto-acusação, bem como os privilégios legais e a especificidade das características dos indivíduos ou dos locais objecto de aplicação da medida.

148. No que respeita às questões tratadas no parágrafo 3, deverá ser atribuída uma importância considerável ao "interesse público", em especial no

que toca aos interesses relativos a uma "sólida e correcta administração da justiça". Na medida em que tal se mostre coerente com o interesse público, as Partes deverão considerar outros factores, tais como o impacto do poder ou do procedimento sobre "os direitos, responsabilidades e interesses legítimos" de terceiros, incluindo de fornecedores de serviços, em resultado das medidas coercivas, devendo ainda, ponderar quais os meios apropriados a utilizar no sentido de minimizar tal impacto. Em suma, é necessário primeiramente levar em consideração a sólida e correcta administração da justiça e também outros interesses públicos (por exemplo, a segurança pública e a saúde pública a par com outros interesses, incluindo os interesses de vítimas e o respeito pela vida privada). Na medida em que tal se afigure compatível com o interesse público, deverão ainda ser levados em conta outros aspectos: redução das perturbações dos serviços prestados ao consumidor, protecção contra a responsabilidade imputável por divulgação de dados ou pela contribuição na divulgação dos mesmos, ao abrigo do disposto no presente Capítulo, ou protecção dos interesses patrimoniais.

Título 2 – Preservação expedita de dados informatizados armazenados

149. As medidas previstas nos Artigos 16º e 17º aplicam-se a dados armazenados que foram já recolhidos e arquivados pelos detentores de dados, tais como os fornecedores de serviços. As referidas medidas não se aplicam, pois, à recolha em tempo real nem à conservação de futuros dados de tráfego ou ao acesso em tempo real ao conteúdo das comunicações. Estas questões são abordadas no Título 5.

150. As medidas descritas nos referidos artigos apenas serão aplicáveis no caso de dados informatizados já existentes e em curso de armazenamento. Por diversas razões, os dados informatizados com um interesse relevante para efeitos de investigações criminais poderão não existir ou não se encontrar arquivados. Por exemplo, poderão não se recolher nem se conservar dados exactos, ou caso tenham sido recolhidos não se ter procedido à sua conservação. As leis relativas à protecção de dados poderão ter exigido a destruição de dados importantes antes de se ter tomado consciência da sua relevância para fins de acções penais. Por vezes, poderá não existir qualquer motivo profissional que justifique a recolha e o arquivo de dados, tal como no caso em que os clientes pagam uma tarifa fixa por determinados serviços ou em que estes últimos são prestados gratuitamente. Os Artigos 16º e 17º não tratam, pois, destas questões.

151. Dever-se-á distinguir entre "Preservação de dados" e "Arquivo de dados". Embora com conotações semelhantes na linguagem comum, os seus significados são distintos quando se trata de terminologia informática. Preservar dados significa manter dados quando estes já existem e se encontram armazenados, estando assim protegidos de tudo quanto seja passível de causar a alteração ou deterioração da qualidade ou do estado actual. Arquivar dados significa guardar e manter na sua posse, para o futuro, dados cuja produção está em curso. O arquivo de dados implica a acumulação de dados no presente e a guarda ou a posse dos mesmos visando um período de tempo futuro, pelo que o referido arquivo de dados constitui o processo de armazenamento de dados. A preservação de dados, por outro lado, consiste na actividade que permite conservar intactos e seguros os referidos dados armazenados.

152. Os Artigos 16º e 17º referem-se somente à preservação de dados e não ao arquivo de dados. Estes artigos não prescrevem a recolha e o arquivo da totalidade, ou mesmo de uma parte, dos dados recolhidos por um fornecedor de serviços ou por uma outra entidade durante a realização das suas actividades. As medidas de preservação aplicam-se, assim, a dados informatizados que "foram armazenados por meio de um sistema informático", o que pressupõe que os dados já existiam, foram previamente recolhidos e são, então, armazenados. Além disso, tal como indicado no Artigo 14º, todos os poderes e procedimentos cuja definição está prevista na Secção 2 da Convenção destinam-se a "investigações criminais ou acções penais específicas", o que limita a aplicação das medidas a uma investigação de um caso particular. Adicionalmente, quando uma Parte executa as medidas de preservação mediante a emissão de uma ordem, esta ordem refere-se a "dados específicos informatizados e armazenados, que se encontrem na posse ou sob o controlo de uma pessoa" (parágrafo 2 do Artigo 16º). Os referidos artigos apenas determinam, portanto, o poder de requerer a preservação de dados previamente existentes e armazenados, durante o período de tempo que decorre até à sua divulgação em conformidade com outros poderes do sistema jurídico e relativamente a investigações criminais ou acções penais específicas.

153. A obrigação de assegurar a preservação dos dados não acarreta para as Partes a obrigatoriedade de limitar o fornecimento ou a utilização de serviços que não impliquem a recolha e o arquivo sistemáticos de certos tipos de dados, tais como os dados relativos ao tráfego ou aos subscritores, enquanto parte integrante das suas práticas comerciais legítimas. A referida obrigação não impõe igualmente às Partes a implementação de novas competências técnicas, por exemplo, no sentido de preservar dados efémeros, que poderão

estar presentes no sistema por um período de tempo de tal forma breve que não possibilitaria a sua razoável preservação em resposta a uma solicitação ou ordem.

154. A legislação vigente em alguns Estados impõe que certos tipos de dados, tais como os dados de carácter pessoal, que se encontrem na posse de determinados tipos de detentores de dados, não sejam arquivados mas sim apagados, caso não exista um objectivo comercial que justifique o arquivo dos dados. Na União Europeia, o princípio geral foi implementado pelas disposições constantes da Directiva 95/46/CE e, no contexto particular do sector das telecomunicações, pela Directiva 97/66/CE. As referidas directivas determinam a obrigação de proceder à eliminação dos dados logo que o armazenamento dos mesmos não se afigure necessário. Todavia, os Estados-membros poderão adoptar leis que prevejam as necessárias excepções para fins da prevenção, investigação ou da instauração de processos relativamente a infracções penais. Estas directivas não impedem os Estados-membros da União Europeia de definir poderes e procedimentos, ao abrigo da sua legislação nacional, a fim de preservar os dados especificados relativos a investigações específicas.

155. Para a maioria dos países, a preservação de dados representa um poder ou procedimento jurídico totalmente novo ao abrigo da sua legislação interna. A preservação é, pois, uma ferramenta de investigação importante no âmbito da abordagem ao crime informático e ao crime relacionado com computadores, em especial no que diz respeito a infracções cometidas através da Internet. Isto, em primeiro lugar porque, devido à volatilidade dos dados informatizados, estes são facilmente sujeitos a manipulações ou alterações. Assim sendo, as valiosas provas de um crime poderão ser facilmente perdidas em resultado de práticas de tratamento e armazenamento descuidadas, de manipulação ou eliminação intencionais com a finalidade de destruir as provas existentes, ou ainda de uma eliminação de rotina dos dados cujo arquivo já não é necessário. Para as autoridades competentes, um dos métodos de preservar a integridade dos dados consiste em efectuar uma busca ou, de forma semelhante, aceder e apreender ou, de forma semelhante, guardar os referidos dados. No entanto, nos casos em que o administrador dos dados seja uma pessoa idónea e digna de confiança, tal como uma empresa de renome, a integridade dos dados poderá ser garantida mais rapidamente, mediante a emissão de uma ordem de preservação dos dados. Para uma empresa de renome, uma ordem de preservação dos dados causará certamente menores transtornos ao decurso normal das suas actividades e será menos prejudicial para a sua reputação no mercado, do que a execução de uma operação de busca e apreensão nas

suas instalações. Em segundo lugar, porque os crimes informáticos e os crimes relacionados com computadores são praticados, em larga medida, em resultado da transmissão de comunicações por meio do sistema informático. Ora, a estas comunicações poderá estar inerente um conteúdo ilegal, tal como pornografia infantil, vírus de computadores ou outras instruções susceptíveis de interferir com os dados ou o adequado funcionamento do sistema informático, ou ainda, provas que apontem para a prática de outros crimes, tal como no caso de fraude ou tráfico de drogas. Determinar a origem ou o destino de comunicações efectuadas anteriormente no tempo, poderá contribuir para apurar a identidade dos autores destas infracções. De modo a identificar a origem ou o destino das referidas comunicações, é necessário dispor de dados de tráfego relativos às mesmas (consultar a explicação dada acerca da importância dos dados de tráfego, mais adiante, no artigo 17º). Em terceiro lugar, nos casos em que a estas comunicações estão associados conteúdos ilegais ou provas de actos criminosos, e as cópias de tais comunicações são conservadas pelos fornecedores de serviços, tais como as de correio electrónico, a preservação das ditas comunicações torna-se importante no sentido de assegurar que as provas consideradas relevantes não são perdidas. Assim, a obtenção de cópias de comunicações anteriormente efectuadas (por exemplo, mensagens de correio electrónico armazenadas, na pasta de envio ou de recepção) poderá constituir uma prova reveladora de um crime.

156. O poder relativo à preservação expedita de dados informatizados tem por objectivo regulamentar e fazer face a estas questões. As Partes obrigar-se-ão, portanto, a instituir um poder que permita emitir uma ordem de preservação dos dados informatizados especificados enquanto medida provisória, sendo que os dados serão preservados durante um período de tempo tão prolongado quanto o necessário, até ao prazo máximo de 90 dias. A Parte poderá agir de forma a que a referida ordem possa ser subsequentemente renovada. Tal não significa que, durante o período da preservação, os dados sejam automaticamente divulgados junto das autoridades competentes para a aplicação da lei. Para que tal se concretize, deverá ser dada uma ordem de busca ou tomada uma medida de divulgação adicional. No que respeita à divulgação dos dados preservados junto das autoridades competentes para a aplicação da lei, deverão ser consultados os parágrafos 152 e 160.

157. É igualmente importante que as medidas de preservação se encontrem contempladas ao nível da legislação nacional, de modo a permitir que as Partes possam apoiar-se umas às outras no plano internacional, através da preservação expedita dos dados armazenados, que estejam localizados no

seio do seu território. Tal ajudará a garantir que não se perdem os dados mais importantes no decorrer dos tradicionais procedimentos de assistência jurídica mútua, muitas vezes morosos mas necessários para que a Parte requerida possa efectivamente obter os dados e divulgá-los à Parte requerente.

Preservação expedita de dados informatizados armazenados (Artigo 16º)

158. O objectivo das disposições contidas no Artigo 16º é o de assegurar que as autoridades competentes, ao nível nacional, dispõem da capacidade necessária para emitir uma ordem ou, de forma semelhante, obter a preservação expedita dos dados informatizados armazenados, especificados, relativamente a uma investigação criminal ou acção penal específica.

159. O termo "preservação" implica que os dados, já existentes sob a forma armazenada, sejam protegidos de tudo quanto seja susceptível de provocar a alteração ou deterioração da sua qualidade ou do seu estado actual, pelo que os dados terão que ser mantidos a salvo de toda e qualquer modificação, danificação ou eliminação. A preservação não implica forçosamente que os dados sejam "congelados" (isto é, tornados inacessíveis) e que esses dados, ou as cópias dos mesmos, não possam ser usados pelos seus utilizadores legítimos. A pessoa à qual a ordem é dirigida poderá continuar a aceder aos dados, ficando tal acesso dependente das especificações exactas que figurem na referida ordem. O artigo não especifica a forma segundo a qual os dados deverão ser preservados, pelo que caberá a cada Parte estipular a forma mais adequada de preservação e, nalguns casos particulares, determinar se a preservação dos dados deverá ou não implicar o seu "congelamento".

160. A referência a "ordenar ou, de forma semelhante, obter" visa permitir a aplicação de outros meios jurídicos de concretizar a preservação, que não apenas através de uma ordem judicial ou administrativa ou de uma instrução oficial (da polícia ou do magistrado do Ministério Público). Nalguns Estados, as ordens de preservação não se encontram contempladas na sua legislação processual, pelo que os dados apenas poderão ser preservados e obtidos por meio de busca e apreensão ou ordem de produção. A noção de flexibilidade encontra-se implícita na expressão "ou, de outra forma, obter" a fim de permitir aos Estados implementar este artigo, através do recurso aos referidos meios. Todavia, recomenda-se que os Estados considerem a definição de poderes e procedimentos que efectivamente permitam requerer do destinatário da ordem a preservação dos dados, visto que uma intervenção rápida por parte do mesmo poderá, em determinados casos, ter como resultado uma implementação mais agilizada das medidas de preservação aplicáveis.

161. O poder de ordenar ou, de forma semelhante, obter a preservação expedita dos dados informatizados especificados, aplica-se a qualquer tipo de dados informatizados armazenados. Tal poderá incluir todo e qualquer tipo de dados que seja especificado na ordem de preservação, como por exemplo, registos comerciais, médicos, pessoais ou outros. A aplicação das medidas deverá ser definida pelas Partes "em especial nos casos em que existam motivos para crer que os dados sejam particularmente vulneráveis a perdas ou modificações." Isto poderá abranger situações em que os dados se encontram sujeitos a um curto período de conservação, tal como quando estamos perante uma política empresarial de eliminação de dados após decorrido um certo período de tempo, ou nos casos em que os dados são normalmente apagados pelo facto de o suporte de armazenamento ser igualmente usado para o registo de outros dados. Poderá também dizer respeito à natureza do administrador dos dados ou à forma pouco segura sob a qual os dados são armazenados. No entanto, se o administrador dos dados não for digno de confiança, será mais seguro proceder à preservação por meio de uma operação de busca e apreensão, do que através de uma ordem cujo cumprimento poderá não se verificar. No parágrafo 1, faz-se expressamente referência aos "dados de tráfego" a fim de indicar a aplicabilidade particular destas disposições a este tipo de dados que, se recolhidos e arquivados por um fornecedor de serviços, serão geralmente mantidos apenas por um curto período de tempo. A menção aos "dados de tráfego" estabelece igualmente uma ligação entre as medidas citadas nos Artigos 16º e 17º.

162. O parágrafo 2 especifica que, nos casos em que uma Parte aplique as medidas de preservação por meio da emissão de uma ordem, esta ordem tem por objecto os "dados específicos informatizados e armazenados, que se encontrem na posse ou sob o controlo de uma pessoa". Assim, os dados armazenados poderão, na realidade, encontrar-se na posse da referida pessoa ou estar armazenados num outro local mas sob o controlo da mesma. A pessoa à qual é dirigida a ordem fica obrigada a "conservar e manter a integridade de tais dados informatizados por um período de tempo tão prolongado quanto o necessário, até um prazo máximo de 90 dias, de modo a permitir às autoridades competentes obter a sua divulgação." A legislação interna adoptada por uma Parte deverá conter indicações concretas relativamente a um período de tempo máximo durante o qual os dados, alvo de uma ordem de preservação, deverão ser conservados, sendo que na ordem deverá ser indicado o prazo exacto de preservação dos dados especificados. O período de tempo deverá ser tão prolongado quanto o necessário, até um prazo máximo de 90 dias, de modo a permitir às autoridades competentes a aplicação de outras medidas

do foro jurídico, tais como operações de busca e apreensão, ou o acesso ou a guarda semelhantes, e a emissão de uma ordem de produção, a fim de obter a divulgação dos dados. A Parte poderá agir de forma a que a referida ordem possa ser subsequentemente renovada. Neste contexto, devemos remeter-nos ao Artigo 29º, no qual são abordados os pedidos de assistência mútua que visam a preservação expedita dos dados armazenados por meio de um sistema informático. O referido Artigo determina que a preservação efectuada em resposta a um pedido de assistência mútua "deverá ter lugar por um período não inferior a 60 dias, a fim de permitir à Parte requerente apresentar um pedido para fins de busca ou acesso semelhante, apreensão ou guarda semelhante, ou divulgação dos dados."

163. O parágrafo 3 impõe, ao administrador dos dados a serem preservados ou à pessoa à qual é dirigida a ordem para preservar os dados, uma obrigação de confidencialidade relativamente à execução dos procedimentos de preservação, pelo período de tempo estipulado ao abrigo da legislação aplicável a nível nacional. Tal exige que as Partes procedam à introdução de medidas de confidencialidade relativas à preservação expedita de dados armazenados, bem como de um prazo limite relativo ao período durante o qual se requer a confidencialidade. Esta medida leva, assim, em linha de conta as necessidades inerentes à aplicação da lei de maneira a que o suspeito, alvo da investigação em causa, não tome conhecimento da mesma. A medida contempla, ainda, o direito das pessoas singulares à vida privada. Do ponto de vista das autoridades competentes para a aplicação da lei, a preservação expedita dos dados faz parte integrante das investigações iniciais, pelo que, nesta fase, poderá ser importante a manutenção do sigilo. A preservação constitui uma medida preliminar a ser tomada enquanto se aguarda a execução de outras medidas jurídicas no sentido da obtenção dos dados ou da divulgação dos mesmos. A confidencialidade é exigida para que não haja lugar a tentativas, por parte de terceiros, de manipulação ou de eliminação dos dados. Para a pessoa à qual é dirigida a ordem, a pessoa visada ou outras pessoas susceptíveis de serem citadas ou identificadas pelos dados em questão, é claramente indicado o período de tempo limite de aplicação da medida. A dupla obrigatoriedade que consiste em conservar os dados protegidos e seguros e manter confidencial o facto de que foi empreendida uma medida de preservação, contribui para a defesa do direito à privacidade que assiste à pessoa visada ou a outras pessoas susceptíveis de serem citadas ou identificadas pelos dados em questão.

164. Para além das limitações acima enumeradas, os poderes e procedimentos referidos no Artigo 16º encontram-se igualmente sujeitos às condições e salvaguardas previstas nos Artigos 14º e 15º.

Preservação expedita e divulgação parcial de dados de tráfego (artigo 17º)

165. O presente artigo define obrigações específicas relativamente à preservação de dados de tráfego ao abrigo do disposto no Artigo 16º e prevê a divulgação expedita de determinados dados de tráfego, a fim de detectar se estiveram envolvidos outros fornecedores de serviços na transmissão das comunicações especificadas. O termo "dados de tráfego" encontra-se definido no Artigo 1º.

166. A obtenção de dados de tráfego armazenados, que estejam associados a comunicações anteriormente efectuadas, poderá ser importante em termos da determinação da origem ou do destino de uma dada comunicação, revelando-se, assim, vital para a identificação das pessoas que, por exemplo, distribuíram produtos de pornografia infantil, difundiram falsas declarações no contexto de uma operação fraudulenta, participaram na propagação de vírus informáticos, tentaram aceder ou acederam ilicitamente a sistemas informáticos, ou transmitiram comunicações a um sistema informático, provocando interferências quer nos dados do sistema quer no correcto funcionamento do próprio sistema. No entanto, estes dados são geralmente armazenados por curtos períodos de tempo, visto que as leis destinadas a proteger a privacidade poderão proibir, ou os intervenientes do mercado poderão desencorajar, o armazenamento de longa duração destes dados. Assim sendo, é importante que sejam tomadas medidas de preservação no sentido de assegurar a integridade dos referidos dados (consultar acima os pontos discutidos em relação à preservação).

167. É frequente constatar-se a participação de mais do que um fornecedor de serviços na transmissão de uma comunicação. Cada fornecedor de serviços poderá deter alguns dados de tráfego relacionados com a transmissão da comunicação especificada, os quais foram gerados e arquivados pelo dito fornecedor de serviços aquando da passagem da comunicação através do seu sistema, ou foram veiculados por outros fornecedores de serviços. Por vezes, os dados de tráfego ou, pelo menos, alguns tipos de dados de tráfego, são partilhados entre os fornecedores de serviços envolvidos na transmissão da comunicação, para fins comerciais, técnicos ou de segurança. Nesse caso, qualquer um dos fornecedores de serviços implicados poderá possuir os dados

de tráfego considerados fundamentais para determinar a origem ou o destino da comunicação. Contudo, na maioria dos casos, nenhum dos fornecedores de serviços detém individualmente os dados de tráfego fundamentais, em número suficiente, para possibilitar a identificação da verdadeira origem ou destino da comunicação. Cada um deles tem em sua posse uma parte do puzzle, e cada uma destas partes necessita de ser examinada de forma a detectar-se a sua origem ou o seu destino.

168. O Artigo 17º zela para que, nas situações em que se constate estarem envolvidos vários fornecedores de serviços na transmissão de uma comunicação, se possa proceder a uma preservação expedita dos dados de tráfego junto de cada um dos referidos fornecedores de serviços. Este Artigo não especifica os meios através dos quais tal deverá ser efectuado, cabendo assim à legislação nacional das Partes, a determinação do meio que se afigure mais pertinente em função do sistema económico e jurídico vigente. Para as autoridades competentes, um meio de alcançar a preservação expedita dos dados seria a emissão, com efeitos imediatos, de uma ordem de preservação a ser dirigida a cada um dos fornecedores de serviços. Todavia, a obtenção de um conjunto de ordens separadas poderá ser um processo desnecessariamente moroso. Uma alternativa mais favorável seria a de obter uma única ordem, cujo âmbito se aplicaria, no entanto, a todos os fornecedores de serviços identificados subsequentemente como estando envolvidos na transmissão da comunicação especificada. Esta ordem global poderia ser notificada sequencialmente a cada um dos fornecedores de serviços identificados. Outras alternativas possíveis consistem, por exemplo, em solicitar a participação dos fornecedores de serviços, isto é, requerer a um fornecedor de serviços que tenha sido notificado de uma tal ordem, que proceda à notificação do fornecedor de serviços seguinte na cadeia da comunicação, acerca da existência e do teor da ordem de preservação emitida. Esta notificação poderia, consoante as disposições constantes da legislação interna, produzir os seus efeitos quer no sentido de autorizar o segundo fornecedor a preservar voluntariamente os dados de tráfego relevantes, não obstante quaisquer obrigações previamente existentes de eliminação dos mesmos, quer no sentido de conferir um carácter vinculatório à preservação supracitada. De igual forma, o segundo fornecedor de serviços ocupar-se-ia da notificação do fornecedor de serviços seguinte na cadeia.

169. Uma vez que os dados de tráfego não são divulgados junto das autoridades competentes para a aplicação da lei, aquando da notificação de uma ordem de preservação a um fornecedor de serviços (mas apenas obtidos ou

divulgados a posteriori mediante a tomada de outras medidas legais), as referidas autoridades não poderão, nesta fase, ter conhecimento de aspectos, tais como, se o fornecedor de serviços possui todos os dados de tráfego cruciais ou se existem outros fornecedores de serviços envolvidos na cadeia de transmissão da comunicação. Portanto, este Artigo exige que o fornecedor de serviços que recebe a notificação de uma ordem de preservação ou de uma acção similar, proceda de imediato à divulgação, junto das autoridades competentes, ou de outra entidade designada para esse efeito, de uma quantidade suficiente de dados de tráfego de forma a permitir que as referidas autoridades possam identificar quaisquer outros fornecedores de serviços, bem como o caminho através do qual a comunicação foi transmitida. As autoridades competentes deverão especificar claramente o tipo de dados de tráfego que necessitará de ser divulgado. A obtenção desta informação permitirá às autoridades competentes determinar se deverão, ou não, ser tomadas medidas de preservação relativas aos outros fornecedores de serviços. Deste modo, as entidades responsáveis pela investigação poderão localizar a comunicação, quanto à sua origem ou ao seu destino, e identificar o autor ou os autores da infracção objecto de investigação. As medidas constantes do presente Artigo encontram-se igualmente sujeitas às limitações, condições e salvaguardas prescritas pelos Artigos 14º e 15º.

Título 3 – Ordem de Produção

Ordem de produção (Artigo 18º)

170. O parágrafo 1 do presente Artigo convida as Partes a investir as suas autoridades competentes dos poderes necessários para obrigar uma pessoa que se encontre no seu território a fornecer os dados armazenados especificados, ou um fornecedor de serviços que ofereça os seus serviços no território da Parte, a prestar informações relativas aos subscritores. Tratam-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. Em vez de se exigir que os Estados apliquem sistematicamente medidas coercivas em relação a terceiros, tais como a busca e apreensão de dados, é essencial que os Estados disponham, ao abrigo da sua legislação nacional, de poderes de investigação alternativos que permitam o recurso a meios menos intrusivos de obter informações relevantes no contexto das investigações criminais realizadas.

171. Uma "ordem de produção" representa uma medida flexível que poderá ser aplicada pelas respectivas autoridades em muitos casos, em especial, como alternativa a medidas que impliquem uma maior intrusão ou que se mostrem

mais dispendiosas. A implementação de um tal mecanismo processual revelar-se-á igualmente benéfico para terceiros, administradores de dados, tais como os fornecedores de serviços da Internet (ISP) que, muitas vezes, estão dispostos a colaborar voluntariamente com as autoridades competentes para a aplicação da lei, fornecendo os dados que se encontram sob o seu controlo mas manifestando a sua preferência pela adopção de uma base jurídica relativa a esta assistência, de modo a ficarem isentos de quaisquer responsabilidades contratuais ou não contratuais eventualmente decorrentes desta divulgação.

172. As ordens de produção dizem respeito a dados informatizados ou a informações relativas aos subscritores que se encontrem na posse ou sob o controlo de uma pessoa singular ou de um fornecedor de serviços. Esta medida é aplicável somente nas situações em que se constate a manutenção, por parte da referida pessoa ou do fornecedor de serviços, de tais dados ou informações. Alguns fornecedores de serviços, por exemplo, não mantêm normalmente quaisquer registos relativos aos subscritores dos seus serviços.

173. Em virtude do disposto no parágrafo 1(a), uma Parte deverá certificar-se de que as suas autoridades competentes para a aplicação da lei são investidas dos poderes necessários para ordenar a uma pessoa, que esteja no seu território, a apresentação de dados específicos armazenados num sistema informático ou num suporte de armazenamento de dados, que se encontrem na sua posse ou sob o seu controlo. A expressão "posse ou controlo" refere-se à posse física dos dados em questão no seio do território da Parte que emite a ordem, bem como a situações em que os dados a serem produzidos não se encontram na posse física da pessoa mas sendo possível, contudo, a esta última exercer livremente o seu controlo sobre a produção dos dados a partir do território da Parte emissora da ordem (por exemplo, sob reserva dos privilégios aplicáveis, toda e qualquer pessoa que receba uma ordem de produção relativa à informação armazenada, por sua conta, por meio de um serviço de armazenamento à distância on-line, ficará obrigada a reproduzir a referida informação). Por outro lado, a simples capacidade técnica de aceder a dados armazenados à distância (por exemplo, a capacidade de um utilizador para aceder, através de uma ligação da rede, a dados armazenados à distância que não se encontrem legalmente sob o seu controlo), não constitui necessariamente um "controlo" nos termos a que se refere a presente disposição. Nalguns Estados, o conceito denominado por "posse", de acordo com a lei, cobre a noção de posse física e construtiva, com uma amplitude suficiente para satisfazer este requisito de "posse ou controlo".

Em conformidade com o disposto no parágrafo 1(b), uma Parte deverá igualmente instituir o poder de requerer de um fornecedor de serviços, que ofereça os seus serviços no seu território, a "apresentação de informação relativa aos subscritores de tais serviços e que se encontre na posse ou sob o controlo do referido fornecedor de serviços". Tal como no parágrafo 1(a), a expressão "posse ou controlo" refere-se à informação relativa aos subscritores que se encontre na posse física do fornecedor de serviços, bem como à informação relativa aos subscritores armazenada à distância mas sob o controlo do fornecedor de serviços (por exemplo, numa unidade de armazenamento de dados à distância fornecida por outra empresa). A expressão "relativamente a tais serviços" significa que o poder deverá destinar-se a fins de obtenção de informações relativas aos subscritores dos serviços oferecidos no seio do território da Parte emissora da ordem supracitada.

174. As condições e salvaguardas referidas no parágrafo 2 deste Artigo poderão, dependendo das disposições constantes da legislação interna, excluir os dados confidenciais ou as informações protegidas pelo segredo profissional. Uma Parte poderá optar pela prescrição de diferentes termos, autoridades competentes e salvaguardas no que diz respeito à apresentação de determinados tipos de dados informatizados ou de informações relativas aos subscritores, detidos por categorias específicas de pessoas ou fornecedores de serviços. Por exemplo, no que concerne a certos tipos de dados, tais como as informações relativas aos subscritores e disponíveis ao público, uma Parte poderá autorizar os agentes responsáveis pela aplicação da lei a emitir uma tal ordem, enquanto que noutras situações poderia ser exigido um despacho do Tribunal. Por outro lado, em determinadas situações, uma Parte poderá requerer, ou ver-se obrigada pelas salvaguardas decorrentes dos direitos do Homem a requerer, que uma ordem de produção seja emitida apenas por autoridades judiciais de forma a poder obter certos tipos de dados. As Partes poderão limitar a divulgação destes dados, para efeitos de aplicação da lei no contexto da luta contra a criminalidade, às situações em que tenha havido lugar, por parte das autoridades judiciais, à emissão de uma ordem de produção para fins de divulgação da dita informação. O princípio da proporcionalidade também permite uma certa flexibilidade relativamente à aplicação da medida, como, por exemplo, em muitos países nos quais se exclui a sua aplicação a casos menores ou sem gravidade.

175. As Partes poderão igualmente considerar a possibilidade de introdução de medidas relativas à confidencialidade. A referida disposição não contém referências específicas à confidencialidade, de modo a manter o paralelismo

com o mundo não electrónico, no qual a confidencialidade não é imposta em geral no que respeita às ordens de produção. No entanto, no mundo electrónico, em particular no mundo virtual on-line, uma ordem de produção poderá, por vezes, ser utilizada como uma medida preliminar no quadro de uma investigação, que precede outras medidas tais como a busca e apreensão ou a intercepção em tempo real de outros dados. A confidencialidade poderá, pois, ser a chave do sucesso de uma investigação.

176. No que diz respeito às modalidades de produção, as Partes poderão estipular a obrigatoriedade de produção dos dados informatizados ou da informação relativa aos subscritores, segundo a forma especificada na respectiva ordem. Tal poderá incluir a referência a um período de tempo durante o qual a divulgação deverá ocorrer, ou ainda, referir-se à forma sob a qual devem ser divulgados os dados ou as informações, por exemplo, sob a forma de texto "claro", on-line, impresso ou em disquete.

177. O termo "informação relativa ao subscritor" encontra-se definido no parágrafo 3. Em princípio, abrange toda e qualquer informação detida pela administração de um fornecedor de serviços relativamente a um subscritor dos seus serviços. A informação relativa ao subscritor poderá apresentar-se sob a forma de dados informatizados ou qualquer outra forma, tal como um documento em suporte papel. Sendo que a informação relativa ao subscritor nem sempre se apresenta sob a forma de dados informatizados, foi incluída no presente artigo uma disposição especial cujo objectivo é regulamentar este tipo de informação. O termo "subscritor" pressupõe-se englobar um vasto leque de clientes de fornecedores de serviços, desde aqueles que pagam uma tarifa fixa de assinatura, aos que pagam os serviços à medida que os vão utilizando, até aos que usufruem de serviços gratuitos. O referido termo cobre igualmente toda a informação referente a pessoas que se encontram habilitadas a utilizar a conta do subscritor.

178. No decorrer de uma investigação criminal, a informação relativa ao subscritor poderá revelar-se necessária, basicamente, em duas situações que passamos a descrever: a primeira, quando há que identificar quais os serviços, e as medidas técnicas a eles associadas, que foram utilizados ou estão a ser utilizados por um subscritor, tal como o tipo de serviço telefónico utilizado (por ex.: móvel), o tipo de outros serviços conexos utilizados (por ex.: reencaminhamento de chamadas, voice-mail, etc.). o número de telefone ou outro endereço técnico (por ex.: endereço de e-mail). A segunda, nos casos em que é conhecido um endereço técnico, a informação relativa ao subscritor é necessária como forma de ajudar a identificar a pessoa visada. Outras

informações relativas ao subscritor, tal como informação comercial sobre facturação e registos de pagamento do subscritor, poderão igualmente ser de alguma utilidade no contexto de investigações criminais, nomeadamente quando o crime que está a ser alvo de investigação envolve uma situação de fraude informática ou outras infracções de natureza económica.

179. Assim sendo, a informação relativa ao subscritor abrange vários tipos de informação acerca da utilização de um serviço e do utilizador desse serviço. No que concerne à utilização do serviço, o termo designa toda e qualquer informação, exceptuando os dados de tráfego ou de conteúdo, através da qual poderá ser determinado o tipo do serviço de comunicação utilizado, as medidas técnicas relacionadas e o período de tempo durante o qual a pessoa subscreveu o serviço. A expressão "medidas técnicas" inclui todas as medidas tomadas no sentido de permitir a um subscritor usufruir do serviço de comunicação oferecido. As referidas medidas abrangem a atribuição e reserva de um número ou endereço técnico (número de telefone, endereço de uma página Web ou nome de domínio, endereço de correio electrónico, etc.), bem como o fornecimento e o registo do equipamento de comunicação utilizado pelo subscritor, tal como aparelhos telefónicos, centrais de atendimento de chamadas ou LAN's (redes locais).

180. A informação relativa ao subscritor não se limita à informação directamente relacionada com a utilização do serviço de comunicação. Designa igualmente toda e qualquer informação, exceptuando os dados de tráfego ou de conteúdo, através da qual poderá ser determinada a identidade do utilizador, o seu endereço postal ou geográfico, o número de telefone ou outro número de acesso, bem como informação sobre facturação e pagamentos, a qual é disponibilizada com base no acordo ou contrato de prestação de serviços firmado entre o subscritor e o fornecedor de serviços. Refere-se ainda a toda e qualquer informação, exceptuando os dados de tráfego ou de conteúdo, relativamente ao local onde se encontra instalado o equipamento de comunicação e que é disponibilizada com base no acordo ou contrato de serviços celebrado. Esta última informação poderá ser relevante, em termos práticos, apenas nos casos em que não se trate de equipamento portátil, mas o conhecimento acerca da portabilidade ou da alegada localização do equipamento (com base na informação prestada em conformidade com os termos e condições do acordo ou do contrato de serviços) poderá ser útil no quadro de uma investigação.

181. Todavia, o presente Artigo não deverá ser interpretado como impondo, aos fornecedores de serviços, a obrigação de manter registos sobre os seus subscritores nem como exigindo dos mesmos a garantia da exactidão de

tais informações. Assim, um fornecedor de serviços não é obrigado a registar informação sobre a identidade dos utilizadores dos chamados cartões de pré-pagamento para acesso a serviços telefónicos móveis, nem será obrigado a verificar a identidade dos subscritores ou a opor-se à utilização de pseudónimos por parte dos utilizadores dos seus serviços.

182. Dado que os poderes e procedimentos, objecto da presente Secção, são instituídos para fins de investigações criminais ou acções penais específicas (Artigo 14º), as ordens de produção destinam-se a ser aplicadas a casos individuais que, em geral, dizem respeito a um subscritor em particular. Por exemplo, tendo por base a menção de um dado nome na ordem de produção, poderá ser solicitado um dado número de telefone ou um endereço de correio electrónico que lhe esteja associado. Da mesma maneira, tendo por base um determinado número de telefone ou endereço de correio electrónico, poderá ser solicitado o nome e a morada do respectivo subscritor. A disposição não autoriza as Partes a emitirem uma ordem jurídica para efeitos da divulgação não selectiva de informações relativas ao subscritor detidas pelo fornecedor de serviços, no que respeita a grupos de subscritores, por exemplo, para fins de exploração aprofundada e extracção de dados.

183. A expressão "acordo ou contrato de serviços" deverá ser interpretada num sentido lato, incluindo qualquer tipo de relação com base na qual um cliente utilize os serviços prestados pelo fornecedor.

Título 4 – Busca e apreensão de dados informatizados armazenados

Busca e apreensão de dados informatizados armazenados (Artigo 19º)

184. O presente Artigo visa a modernização e a harmonização das legislações nacionais relativamente à busca e apreensão de dados informatizados armazenados, para fins de obtenção de provas relacionadas com investigações criminais ou acções penais específicas. Qualquer legislação interna em matéria de direito processual penal, contempla os poderes relativos à busca e apreensão de objectos tangíveis. Contudo, em muitos Estados ou jurisdições, os dados informatizados armazenados, por si só, não serão considerados como algo tangível, pelo que não poderão ser adquiridos a título de investigações criminais e acções penais da mesma forma que os bens corpóreos, a não ser através da obtenção do suporte no qual se encontram armazenados os dados. O objectivo do Artigo 19º da presente Convenção é o de estabelecer um poder equivalente relativo aos dados armazenados.

185. No quadro de uma busca operada segundo os clássicos trâmites aplicáveis a documentos ou pastas, a busca implica a compilação de provas anteriormente registadas ou inscritas sob uma forma tangível, tal como aquelas em foi utilizada tinta sobre papel. Os investigadores examinam ou pesquisam tais dados registados e apreendem ou extraem os registos tangíveis levando-os consigo. A compilação de dados tem lugar durante o período de realização da busca ou investigação, focalizando-se apenas nos dados existentes até ao momento. A condição previamente necessária à obtenção da autorização legal para efeitos de realização de uma operação de busca, traduz-se pela existência de motivos que levem a crer, tal como prescrito ao abrigo da legislação nacional e das disposições relativas à defesa dos direitos do Homem, que tais dados têm a sua existência material num determinado local e são passíveis de fornecer provas de uma infracção penal específica.

186. No que se refere à investigação de provas, em especial em se tratando de dados informatizados, muitas são as características da investigação tradicional que perduram no novo meio tecnológico. Por exemplo, a compilação dos dados ocorre durante o período de realização da busca ou investigação, focalizando-se nos dados existentes até ao momento. Os pré-requisitos a serem preenchidos no sentido de obter a autorização legal para realizar uma busca permanecem inalterados. O grau de convicção ou conhecimento exigido para obter uma autorização legal de busca não difere consoante se trate de dados sob a forma tangível ou sob a forma electrónica. Da mesma maneira, a convicção e a busca dizem respeito a dados já existentes e que permitirão reunir provas acerca de uma dada infracção.

187. Todavia, no que se refere à investigação de dados informatizados, são necessárias disposições processuais complementares, a fim de assegurar que os dados informatizados podem ser obtidos com a mesma eficácia de uma operação de busca e apreensão de suportes de dados tangíveis. Existem diversas razões para este facto: em primeiro lugar, os dados são intangíveis, como é o caso dos dados sob a forma electromagnética. Em segundo lugar, enquanto que os dados podem lidos através da utilização de um equipamento informático, o mesmo não se passa relativamente à apreensão e transporte desses mesmos dados, tal como acontece com um documento em suporte papel. O suporte físico no qual se encontram armazenados os dados intangíveis (por exemplo, o disco rígido de um computador ou uma disquete) deverá ser apreendido e retirado do local, ou deverá ser efectuada uma cópia dos dados, quer sob uma forma tangível (por exemplo, uma impressão feita a partir de um computador) quer sob uma forma intangível, num suporte físico (por

exemplo, uma disquete), antes que o suporte tangível que contém a cópia possa ser apreendido e transportado para fora do local. Nos dois últimos casos enunciados, em que são efectuadas cópias dos dados, permanecerá no sistema informático ou na unidade de armazenamento uma cópia dos dados. A legislação nacional deverá instituir o poder relativo à realização das ditas cópias. Em terceiro lugar, devido à conectividade dos sistemas informáticos, os dados poderão não se encontrar armazenados no computador alvo de busca, podendo ser facilmente acessíveis a partir desse mesmo sistema. Os dados poderão ser armazenados numa unidade de armazenamento de dados associada, que se encontre directamente ligada ao computador, ou indirectamente ligada ao mesmo através do recurso a sistemas de comunicação, tais como a Internet. Tal poderá requerer ou não a implementação de novas leis no sentido de alargar a extensão da busca ao sistema no qual os dados se encontrem efectivamente armazenados (ou da extracção dos dados do local em questão para o computador alvo de busca), ou de maneira a permitir a utilização dos tradicionais poderes de investigação, com uma maior rapidez e uma melhor coordenação, em ambos os locais.

188. As disposições constantes do parágrafo 1 requerem que as Partes deleguem, nas autoridades competentes para a aplicação da lei, os poderes necessários para o acesso e a investigação de dados informatizados, contidos quer num sistema informático quer numa parte deste (tal como um dispositivo de armazenamento de dados a ele conectado), ou num suporte de armazenamento de dados independente (tal como um CD-ROM ou uma disquete). Uma vez que a definição de "sistema informático" que figura no Artigo 1º, designa "todo e qualquer dispositivo ou grupo de dispositivos relacionados ou interligados", o parágrafo 1 refere-se à investigação de um sistema informático e dos seus componentes relacionados que podem ser considerados como constituindo, no seu todo, um sistema informático distinto (por exemplo, um computador pessoal em conjunto com uma impressora e outros dispositivos de armazenamento, ou uma rede de área local). Por vezes, os dados que se encontram fisicamente armazenados noutro sistema ou dispositivo de armazenamento, poderão ser acedidos legalmente através do sistema informático alvo de busca, bastando para esse efeito estabelecer uma ligação a outros sistemas informáticos distintos. Esta situação, envolvendo ligações a outros sistemas informáticos por meio de redes de telecomunicações no seio do mesmo território (por exemplo, rede de área alargada ou Internet), é abordada no parágrafo 2.

189. Embora a operação de busca e apreensão de um "suporte de armazenamento informático onde possam estar armazenados dados informatizados" (parágrafo 1(b)) seja susceptível de ser executada mediante a utilização dos poderes de busca tradicionais, são frequentes os casos em que tal operação exige tanto a investigação do sistema informático como a de qualquer suporte de armazenamento de dados informatizados (por exemplo, disquetes) que se encontre nas proximidades do sistema. Devido a esta relação, o parágrafo 1 prevê a implementação de uma autoridade jurídica global para lidar com ambas as situações.

190. O Artigo 19º é consagrado aos dados informatizados armazenados. A este respeito, é colocada a questão que incide sobre o facto de se uma mensagem de correio electrónico não aberta, em espera na caixa de correio de um fornecedor de serviços de Internet, até que o respectivo destinatário efectue o descarregamento para o seu sistema informático, deverá ser considerada como constituindo dados armazenados ou dados em curso de transferência. Ao abrigo da legislação adoptada por algumas Partes, a referida mensagem de correio electrónico faz parte integrante de uma comunicação, pelo que o seu conteúdo apenas poderá ser conhecido mediante a aplicação do poder de intercepção, enquanto que, segundo outros sistemas jurídicos, a dita mensagem se considera pertencer ao domínio dos dados armazenados aos quais se refere o Artigo 19º. Assim, as Partes deverão proceder a uma revisão das suas leis relativas a esta matéria, por forma a determinar qual é a visão mais adequada no âmbito dos seus sistemas jurídicos internos.

191. Neste parágrafo, faz-se referência à expressão "a busca ou, de forma semelhante, o acesso". A utilização do termo tradicional de "busca" traduz a ideia de exercício do poder coercivo por parte do Estado, e indica que o poder mencionado no presente artigo é análogo à busca clássica. "Busca" significa procurar, ler, inspeccionar ou rever dados. Inclui a noção de pesquisa de dados e de análise de dados. Por outro lado, a palavra "acesso" encerra um significado neutro mas reflecte com maior exactidão a terminologia informática. Ambos os termos são utilizados de forma a conciliar os conceitos tradicionais com a terminologia moderna.

192. A referência a "no seio do seu território" serve para realçar o facto de que a presente disposição, bem como todos os artigos da Convenção, se aplicam apenas a medidas a serem empreendidas ao nível nacional.

193. O parágrafo 2 autoriza as autoridades responsáveis pela investigação a alargarem as suas operações de busca, ou de forma semelhante, o acesso a um

outro sistema informático ou a uma parte do mesmo, caso existam motivos para crer que os dados procurados se encontram armazenados nesse outro sistema informático. No entanto, também neste caso, o referido sistema ou a parte deste, deverá encontrar-se "no seio do seu território".

194. A Convenção não prescreve a forma como deverá ser levado a cabo ou autorizado um tal alargamento da operação de busca, cabendo pois às Partes deliberar sobre essa matéria ao abrigo da sua legislação interna. Citamos alguns exemplos de condições possíveis: investir a entidade judiciária ou outra responsável pela autorização da operação de busca relativa a um sistema informático específico, dos poderes necessários para autorizar a extensão ou alargamento da busca, ou de forma semelhante, o acesso a um sistema que a ele esteja conectado, caso tal entidade apresente fundamentos que levem a crer (na medida exigida pela legislação nacional e pelas disposições relativas à defesa dos direitos do Homem) que o sistema informático conectado poderá conter os dados específicos objecto de busca; delegar os necessários poderes nas autoridades responsáveis pela investigação, de forma a que estas últimas possam alargar uma busca, ou de forma semelhante, um acesso autorizado de um sistema informático específico a um sistema que a ele se encontre conectado, caso existam, mais uma vez, motivos para crer que neste último sistema informático referido poderão estar armazenados os dados específicos objecto de busca; ou exercer os poderes de busca, ou de forma semelhante, de acesso a ambos os locais e de uma forma coordenada e expedita. Em qualquer das situações, impõe-se que os dados objecto de busca sejam legalmente acessíveis a partir do sistema informático inicial ou disponibilizados a este.

195. O presente artigo não aborda a "busca e apreensão transfronteiriça" que confere aos Estados a possibilidade de busca e apreensão de dados no seio do território de outras Partes, sem que seja necessário recorrer às modalidades tradicionais de assistência jurídica mútua. Esta questão será, pois, debatida mais adiante no Capítulo sobre cooperação internacional.

196. O parágrafo 3 trata as questões relacionadas com a delegação de poderes às autoridades competentes de modo a que estas possam apreender ou, de forma semelhante, adquirir e guardar os dados informatizados alvo de busca, ou de forma semelhante, alvo de acesso, de acordo com as disposições constantes dos parágrafos 1 ou 2. As medidas previstas englobam o poder de apreensão de material informático e de suportes de armazenamento de dados informatizados. Em certos casos, por exemplo quando os dados se encontram armazenados num sistema operativo cuja especificidade não permite efectuar uma cópia dos dados, não resta outra solução senão a de proceder à apreensão

do próprio suporte de dados. Tal poderá revelar-se igualmente necessário nos casos em que o suporte de dados tenha que ser sujeito a uma análise no sentido de extrair do mesmo os antigos dados a que foram sobrepostos outros dados, mas dos quais, ainda assim, é possível detectar alguns vestígios no suporte de dados.

197. No contexto da presente Convenção, o termo "apreender" significa transportar para fora do local em questão, o suporte físico no qual foram registados os dados ou as informações, ou efectuar e guardar uma cópia de tais dados ou informações. O termo "apreender" inclui, ainda, a utilização ou apreensão de programas necessários para aceder aos dados objecto de busca e investigação. Ao mesmo tempo que se utiliza o termo clássico de "apreensão", introduz-se a expressão "ou de forma semelhante, a guarda" de maneira a abarcar outros meios através dos quais é possível remover e tornar inacessíveis os dados intangíveis, ou de outro modo assumir o controlo destes últimos no meio informático. Uma vez que as medidas instituídas se referem aos dados intangíveis armazenados, torna-se necessário que as autoridades competentes adoptem medidas complementares no sentido da aquisição e guarda dos dados, isto é, de maneira a "preservar a integridade dos dados", ou manter a "cadeia de posse" dos dados, o que significa que os dados copiados ou removidos são conservados no estado em que foram encontrados aquando da apreensão, mantendo-se inalterados no período durante o qual é intentada a acção penal. A expressão remete-nos, pois, para um assumir do controlo dos dados ou para a remoção dos mesmos do local em questão.

198. A inacessibilidade dos dados poderá estar relacionada com a sua codificação (por exemplo, através da encriptação) ou com o bloqueio, por qualquer outro meio tecnológico, do acesso aos mesmos. Esta medida poderia ser aplicada, e revestir-se de alguma utilidade, nas situações que implicam perigos ou efeitos nocivos para a sociedade, tal como os provocados, por exemplo, por programas de vírus ou instruções sobre como criar vírus ou fabricar bombas, ou nos casos em que o conteúdo dos dados é ilegal, tal como na pornografia infantil. O termo "remoção" pretende exprimir a ideia de que os dados ao serem removidos ou tornados inacessíveis, não são destruídos, continuando assim a existir. Deste modo, o suspeito fica temporariamente privado dos dados, mas estes poderão ser-lhe devolvidos após o final da investigação criminal ou acção penal.

199. Isto posto, podemos afirmar que a apreensão, ou de forma semelhante, a guarda de dados tem duas funções: 1) reunir provas, por meio da realização de cópias dos dados, ou 2) confiscar dados, efectuando cópias dos mesmos

e, subsequentemente, bloqueando o acesso à versão original dos dados ou removendo-os. A apreensão não implica uma eliminação definitiva dos dados apreendidos.

200. O parágrafo 4 introduz uma medida coerciva cujo objectivo é o de facilitar a busca e apreensão de dados informatizados. Trata-se aqui, em termos práticos, da dificuldade de acesso aos dados investigados e da sua identificação enquanto elementos constituintes de prova, devido à quantidade de dados passíveis de processamento e armazenamento, ao desenvolvimento de medidas de segurança, bem como à natureza das operações informáticas. Reconhecendo a possibilidade de ser necessário consultar os administradores de sistema - em virtude dos conhecimentos particulares que estes possuem acerca do sistema informático - relativamente à melhor forma de conduzir o processo de investigação em termos das modalidades técnicas existentes, a presente disposição autoriza as entidades competentes a obrigar um administrador de sistema a prestar o seu contributo, da forma que se afigure razoável, no quadro da operação de busca e apreensão.

201. O referido poder não é apenas vantajoso para as autoridades responsáveis pela investigação. Sem uma tal cooperação, as autoridades responsáveis pela investigação poderiam permanecer nas instalações alvo da operação de busca e impedir o acesso ao sistema informático, por longos períodos de tempo, enquanto estivesse a decorrer a investigação. Tal poderia representar uma sobrecarga, em termos económicos, para as empresas com actividades legais ou para os clientes e subscritores aos quais seria vedado o acesso aos dados durante esse período. Contando com a colaboração de pessoas devidamente qualificadas, as investigações tornam-se mais eficazes e mais rentáveis, quer sob o ponto de vista da aplicação da lei quer em termos das pessoas singulares afectadas. Ao obrigar um administrador de sistemas a cooperar, nos termos da lei, estar-se-á igualmente a isentá-lo de quaisquer obrigações contratuais ou outras de não divulgação dos dados.

202. A informação cujo fornecimento é passível de ser solicitado, consiste na informação necessária à execução das operações de busca e apreensão, ou de forma semelhante, acesso e guarda. No entanto, a prestação desta informação é pois limitada à que se considere ser "razoável". Em determinadas circunstâncias, a prestação da informação dentro de tais limites razoáveis, inclui a divulgação de uma password ou de outra medida de segurança junto das autoridades competentes. Todavia, noutras circunstâncias, tal poderá não ser considerado razoável, por exemplo, nas situações em que a divulgação de uma password ou de outra medida de segurança constitua, desnecessariamente,

uma ameaça à privacidade de outros utilizadores ou ao carácter confidencial de outros dados para os quais não exista uma autorização de busca. Neste caso, a prestação da "informação necessária" poderia residir na divulgação, sob uma forma inteligível e legível, dos dados que são efectivamente objecto de investigação por parte das autoridades competentes.

203. Em virtude do disposto no parágrafo 5 do presente artigo, as medidas encontram-se sujeitas às condições e salvaguardas previstas pela legislação nacional, com base no Artigo 15º da presente Convenção. As referidas condições poderão incluir disposições relativas ao recrutamento e à remuneração de testemunhas e de peritos.

204. No contexto do parágrafo 5, os redactores da presente Convenção estudaram a questão que se prende com o facto de se as partes interessadas deverão ser notificadas acerca da execução de uma operação de busca. No mundo virtual, poderá ser menos notória a realização de uma busca e apreensão (cópia) dos dados do que no mundo não virtual, visto que, neste último caso, os objectos apreendidos passam a estar fisicamente ausentes. A legislação adoptada por algumas das Partes não prevê a obrigação de notificação no caso do clássico procedimento de busca. Por esse motivo, se ao abrigo da Convenção se impusesse a obrigação de notificar, estar-se-ia a criar uma discrepância nos termos da legislação das referidas Partes. Por outro lado, algumas Partes poderão considerar a notificação como sendo um elemento essencial desta medida, o qual permitiria estabelecer a distinção entre a investigação de dados armazenados, no quadro de uma operação de busca (a qual não se pressupõe ser uma medida tomada de maneira sub-reptícia), e a intercepção de dados em curso de transmissão (sendo esta uma medida sub-reptícia; consultar os artigos 20º e 21º). A questão da notificação é assim remetida à deliberação das Partes, devendo ser analisada à luz das suas legislações nacionais. Caso as Partes ponderem a adopção de um sistema de notificação obrigatória das pessoas visadas, deverá ser tido em consideração o facto de que tal notificação é susceptível de prejudicar a investigação. Uma vez cientes da existência de tal risco, as Partes deverão considerar a possibilidade de adiamento da emissão da notificação.

Título 5 – Recolha de dados informatizados em tempo real

205. Os Artigos 20º e 21º tratam da recolha em tempo real de dados de tráfego e da intercepção em tempo real de dados de conteúdo, associados a comunicações específicas transmitidas por meio de um sistema informático. As disposições contidas nos referidos Artigos abordam a questão da recolha

e da intercepção, em tempo real, de tais dados por parte das autoridades competentes, assim como a recolha e intercepção desses mesmos dados pelos fornecedores de serviços. Prevê-se, ainda, ao abrigo destes Artigos, uma obrigação de confidencialidade.

206. A intercepção de telecomunicações refere-se, normalmente, às redes de telecomunicações tradicionais. Estas redes podem incluir infra-estruturas por cabo, quer de cabo metálico quer de fibras ópticas, bem como interligações com redes sem fio, incluindo sistemas telefónicos móveis e sistemas de transmissão por microondas. Nos dias de hoje, também as comunicações móveis se encontram facilitadas por um sistema de redes de satélite especiais. As redes informáticas consistem igualmente numa infra-estrutura por cabos fixa e independente, mas são mais frequentemente operadas como uma rede virtual através de ligações efectuadas por meio de infra-estruturas de telecomunicação, permitindo assim a criação de redes informáticas ou a ligação de redes de dimensão global. Em resultado da convergência das tecnologias da informação e das telecomunicações, torna-se pouco nítida a distinção existente entre as telecomunicações e as comunicações informáticas, bem como a especificidade das suas infra-estruturas. Assim, a definição de "sistema informático" constante do Artigo 1º não limita a forma segundo a qual os dispositivos ou o grupo de dispositivos devem estar interligados. Os Artigos 20º e 21º aplicam-se, portanto, a comunicações específicas transmitidas por meio de um sistema informático, nelas se incluindo a transmissão de uma comunicação através de redes de telecomunicação antes de ser recebida por um outro sistema informático.

207. Os Artigos 20º e 21º não estabelecem uma distinção entre um sistema de telecomunicação ou um sistema informático público ou privado, nem se referem à utilização de sistemas e serviços de comunicação pelo público ou por grupos fechados de utilizadores ou particulares. A definição de "fornecedor de serviços" que figura no Artigo 1º, diz respeito a entidades públicas e privadas que oferecem aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático.

208. O presente Título regulamenta a recolha de provas contidas nas comunicações em curso de produção, sendo que a dita recolha tem lugar aquando da transmissão da comunicação (isto é, em tempo real). Os dados apresentam-se sob a forma intangível (por exemplo, sob a forma de transmissões de voz ou de impulsos electrónicos). A recolha não interfere significativamente na circulação dos dados, pelo que a comunicação chega ao seu destinatário. Em vez de uma apreensão física dos dados, é efectuado um registo (isto é, uma

cópia) dos dados que estão a ser comunicados. A recolha destas provas ocorre durante um determinado período de tempo. A autorização legal mediante a qual é possível efectuar a recolha é sempre solicitada relativamente a um acontecimento futuro (isto é, uma futura transmissão de dados).

209. Existem dois tipos de dados passíveis de serem recolhidos, a saber, os dados de tráfego e os dados de conteúdo. O termo "dados de tráfego" encontra-se definido no Artigo 1º e designa qualquer dado informatizado, relacionado com uma comunicação efectuada por meio de um sistema informático, gerado pelo sistema informático e que faz parte integrante da cadeia de comunicação, através do qual se indicam os aspectos da comunicação, tais como a sua origem, o destino, o caminho, a hora, a data, a dimensão, a duração ou o tipo do serviço subjacente à mesma. O termo "dados de conteúdo" não se encontra definido na presente Convenção mas designa o conteúdo informativo da comunicação, ou seja, o significado ou o teor da comunicação, ou a mensagem ou informação veiculada pela comunicação (que não a relativa aos dados de tráfego).

210. São vários os Estados que estabelecem uma distinção entre a intercepção em tempo real de dados de conteúdo e a recolha em tempo real de dados de tráfego, tanto no que respeita aos pré-requisitos exigidos por lei para autorizar a aplicação de uma tal medida de investigação, como em termos das infracções relativamente às quais esta medida poderá ser aplicada. Embora reconhecendo que, a ambos os tipos de dados poderão estar associados interesses de cariz privado, muitos Estados consideram que os referidos interesses se revestem de uma maior importância ou são superiores em se tratando dos dados de conteúdo, devido à natureza do conteúdo ou da mensagem veiculada pela comunicação. Deste modo, poderão ser impostas maiores restrições à recolha em tempo real de dados de conteúdo do que à dos dados de tráfego. Para melhor salientar esta distinção estabelecida por alguns Estados, e partindo da constatação de que, no plano operacional, os dados são recolhidos e registados em ambas as situações, a Convenção refere-se, no plano normativo, nos títulos dos artigos, à recolha de dados de tráfego como "recolha em tempo real" e à recolha de dados de conteúdo como "intercepção em tempo real".

211. Nalguns Estados, a legislação em vigor não traça qualquer distinção entre a recolha de dados de tráfego e a intercepção de dados de conteúdo. Tal poderá ficar a dever-se quer ao facto de não ter sido estabelecida, nos termos da lei, a diferença associada aos interesses de natureza privada, quer ao facto de as técnicas de recolha aplicáveis a ambas as medidas serem muito

semelhantes. Assim, os pré-requisitos exigidos por lei para a autorização de aplicação das referidas medidas, bem como as infracções relativamente às quais é possível recorrer a estas medidas, são basicamente os mesmos nos dois casos. Esta situação também se encontra contemplada pela Convenção, sendo, pois, utilizada a expressão "recolher ou registar" no texto de ambos os Artigos 20º e 21º.

212. No que concerne à intercepção em tempo real de dados de conteúdo, em muitos casos, a lei prescreve que apenas se deve recorrer a esta medida quando se trate da investigação de infracções graves ou de categorias de infracções graves. As referidas infracções são identificadas como graves, a este título e, ao abrigo das legislações nacionais, sendo incluídas numa lista descritiva das infracções às quais a medida é passível de ser aplicada, ou sendo englobadas nesta categoria com base numa determinada pena máxima de prisão, aplicável a estas infracções. Assim, quanto à intercepção de dados de conteúdo, o Artigo 21º especifica que as Partes apenas deverão instituir esta medida "no que se refere a uma série de infracções graves a serem definidas ao abrigo da legislação nacional".

213. Por outro lado, o Artigo 20º cujas disposições se referem à recolha de dados de tráfego, não apresenta as mesmas limitações e aplica-se, em princípio, a qualquer infracção penal abrangida pela Convenção. Todavia, o parágrafo 3 do Artigo 14º estipula que as Partes poderão reservar-se o direito de aplicar a medida apenas no caso de infracções ou categorias de infracções especificadas na declaração de reserva, desde que o conjunto de tais infracções ou categorias de infracções não seja mais restrito do que o conjunto de infracções às quais se aplica a medida de intercepção de dados de conteúdo. Não obstante este aspecto, nos casos em que seja formulada uma tal reserva, as Partes deverão considerar a restrição da mesma de modo a permitir a aplicação, tão alargada quanto possível, da medida de recolha de dados de tráfego.

214. Para alguns Estados, as infracções definidas pela Convenção não são, em geral, consideradas suficientemente graves para permitir a intercepção dos dados de conteúdo e, em certos casos, até mesmo a recolha de dados de tráfego. Contudo, na maioria dos casos, estas técnicas são cruciais para a investigação de algumas das infracções definidas pela Convenção, tais como as que envolvem o acesso ilícito a sistemas informáticos, a propagação de vírus informáticos ou a distribuição de pornografia infantil. A origem da intrusão ou da distribuição, por exemplo, nem sempre poderá ser detectada sem que se proceda a uma recolha em tempo real dos dados de tráfego. Da mesma maneira, nalguns casos, a natureza da comunicação não poderá ser descoberta

sem que se proceda a uma intercepção em tempo real dos dados de conteúdo. As referidas infracções, devido ao seu carácter ou ao meio de transmissão utilizado, implicam pois o recurso às tecnologias informáticas. Assim, poderá ser permitido o uso de meios tecnológicos no quadro da investigação destas infracções. No entanto, devido ao carácter delicado de que se reveste esta questão da intercepção de dados de conteúdo, a Convenção prevê que o âmbito desta medida deverá ser determinado de acordo com as disposições da legislação nacional das Partes. Visto que alguns países equiparam juridicamente a recolha de dados de tráfego e a intercepção de dados de conteúdo, foi concedida a possibilidade de formulação de uma reserva a fim de limitar a aplicabilidade da primeira, desde que tal aplicabilidade não seja limitada numa medida superior aquela adoptada, pelas Partes, relativamente à intercepção em tempo real de dados de conteúdo. No entanto, as Partes deverão considerar a aplicação das duas medidas às infracções definidas pela Convenção, na Secção 1, de modo a proporcionar um meio eficaz de investigação destes crimes informáticos e infracções relacionadas com computadores.

215. As condições e salvaguardas relativas aos poderes e procedimentos aplicáveis à intercepção em tempo real de dados de conteúdo e à recolha em tempo real de dados de tráfego, encontram-se sujeitas às disposições constantes dos Artigos 14º e 15º. Uma vez que a intercepção de dados de conteúdo representa uma medida com elevado grau de intrusão na vida privada, torna-se necessária a implementação de salvaguardas rigorosas de modo a garantir um equilíbrio adequado entre os interesses da justiça e os direitos fundamentais do Homem. No domínio da intercepção, a presente Convenção não prevê salvaguardas específicas, para além de limitar a autorização de intercepção de dados de conteúdo às investigações relativas a infracções penais graves, de acordo com as disposições da legislação nacional. Todavia, as condições e salvaguardas importantes neste domínio, e aplicáveis em conformidade com a legislação nacional, são as seguintes: supervisão por parte de um órgão judiciário ou outro independente; especificidade das comunicações ou das pessoas alvo de intercepção; necessidade, subsidiariedade e proporcionalidade (por exemplo, condições jurídicas justificativas da aplicação da medida; ineficácia de outras medidas com menor grau de intrusão); limitação do período de duração da intercepção; direito de recurso. Muitas destas salvaguardas reflectem o espírito da Convenção Europeia dos Direitos do Homem e a sua subsequente jurisprudência (consultar as sentenças proferidas pelo Tribunal Europeu dos Direitos do Homem

nos casos Klass[5], Kruslin[6], Huvig[7], Malone[8], Halford[9], Lambert[10]). Algumas das salvaguardas anteriormente mencionadas são também aplicáveis à recolha de dados de tráfego em tempo real.

Recolha de dados de tráfego em tempo real (Artigo 20º)

216. É frequente dar-se o caso de os dados de tráfego iniciais já não estarem disponíveis ou não serem relevantes, devido ao facto de o intruso ter alterado o caminho da comunicação. Por esse motivo, a recolha em tempo real dos dados de tráfego constitui uma medida de investigação de extrema importância. O Artigo 20º aborda a temática da recolha e registo de dados de tráfego, em tempo real, para fins de investigações criminais ou acções penais específicas.

217. A recolha de dados de tráfego relativamente às telecomunicações (por exemplo, nas conversas telefónicas) desde sempre se afigurou como sendo um instrumento de investigação útil, na medida em que permite a identificação da origem ou destino (por exemplo, os números de telefone) e dos dados conexos (por exemplo, a hora, data e duração) sobre vários tipos de comunicações ilegais (por exemplo, no caso de ameaças de crimes e assédio, conspiração de índole criminosa, declarações falsas) e sobre comunicações que forneçam provas de crimes passados ou futuros (por exemplo, tráfico de estupefacientes, homicídio, infracções de cariz económico, etc.).

218. As comunicações através de computadores podem constituir ou servir de prova dos mesmos tipos de actos criminosos. No entanto, visto que a tecnologia informática permite transmitir grandes quantidades de dados, incluindo texto, imagens e sons, existe também um maior potencial para a prática de crimes que envolvam a distribuição de conteúdos ilegais (por exemplo, pornografia infantil). Da mesma maneira, uma vez que os computadores têm capacidade de armazenamento de vastas quantidades de dados, os quais são frequentemente de natureza privada, tal significa que o risco de efeitos negativos pode ser substancial, quer a nível económico, social ou pessoal, caso se assista a uma interferência na integridade dos dados. Além disso, como a ciência da tecnologia informática se baseia no tratamento de dados, quer sejam estes um produto final ou um elemento da sua função operacional (por exemplo,

5. Sentença do TEDH no caso Klass e outros vs. Alemanha, A28, 06/09/1978
6. Sentença do TEDH no caso Kruslin vs. França, 176-A, 24/04/1990
7. Sentença do TEDH no caso Huvig vs. França, 176-B, 24/04/1990
8. Sentença do TEDH no caso Malone vs. Reino Unido, A82, 02/08/1984
9. Sentença do TEDH no caso Halford vs. Reino Unido, Relatórios 1997 – III, 25/06/1997
10. Sentença do TEDH no caso Lambert vs. França, Relatórios 1998 – V, 24/08/1998

execução de programas de computador), toda e qualquer interferência nestes dados poderá ter resultados desastrosos no que respeita ao funcionamento dos sistemas informáticos. Nos casos de distribuição de pornografia infantil, acesso ilícito a um sistema informático ou interferência no correcto funcionamento do sistema informático ou na integridade dos dados, e em particular quando estas infracções são cometidas à distância, por exemplo via Internet, torna-se não só necessário mas vital detectar o caminho das comunicações entre a vítima e o autor da infracção. Assim sendo, a capacidade de recolher dados de tráfego relativos a comunicações informáticas é tão ou mais importante do que essa mesma capacidade relativamente às tradicionais telecomunicações. Esta técnica de investigação permite relacionar a hora, a data, a origem e o destino das comunicações efectuadas pelo suspeito com a hora da intrusão no sistema da vítima, possibilitando a identificação de outras vítimas ou revelando ligações com cúmplices.

219. Ao abrigo do disposto no presente Artigo, os dados de tráfego visados deverão estar associados a comunicações específicas, efectuadas no seio do território da Parte em causa. Fala-se de "comunicações" específicas, no plural, uma vez que poderá ser necessário recolher dados de tráfego relativos a várias comunicações, a fim de determinar a origem ou o destino humano (por exemplo, no caso de uma família em que vários dos seus membros utilizam os mesmos meios de telecomunicações, poderá ser necessário estabelecer uma relação entre as várias comunicações efectuadas e a possibilidade de cada um desses membros fazer uso do sistema informático). Deverão, pois ser especificadas as comunicações relativamente às quais os dados de tráfego poderão ser recolhidos ou registados. Assim, a Convenção não exige nem autoriza a vigilância ou a recolha, geral ou indiscriminada, de grandes quantidades de dados de tráfego. Do mesmo modo, a Convenção não permite a realização de "missões de exploração" através das quais se espera descobrir actividades de índole criminosa, sendo estas situações muito diferentes das investigações levadas a cabo relativamente a casos específicos de criminalidade. Por este motivo, a ordem judicial ou outra que autorize a recolha deverá indicar expressamente quais as comunicações cujos dados de tráfego deverão ser recolhidos.

220. Sem prejuízo do disposto no parágrafo 2, as Partes obrigar-se-ão, ao abrigo do parágrafo 1(a) a assegurar que as suas autoridades competentes se encontram investidas dos poderes necessários para proceder à recolha ou ao registo de dados de tráfego, recorrendo a meios técnicos. O Artigo

não especifica os meios tecnológicos através dos quais a recolha deverá ser realizada, não sendo definidas quaisquer obrigações em termos técnicos.

221. Adicionalmente, em virtude do disposto no parágrafo 1(b), as Partes comprometem-se a assegurar que as suas autoridades competentes se encontram investidas do poder para obrigar um fornecedor de serviços a recolher ou registar dados de tráfego ou para exigir que este último colabore e apoie as autoridades competentes ao nível da recolha ou registo de tais dados. Esta obrigação que recai sobre os fornecedores de serviços é aplicável apenas na medida em que tal recolha ou registo e colaboração ou apoio se encontrem no âmbito da real capacidade técnica do fornecedor de serviços. É de notar que o Artigo não obriga os fornecedores de serviços a garantirem a existência de uma tal capacidade técnica necessária à realização da recolha ou registo, ou à prestação da colaboração e apoio. Não se exige, dos fornecedores de serviços, a aquisição ou o desenvolvimento de novos equipamentos, a contratação de assistência técnica especializada ou a reconfiguração onerosa dos seus sistemas. No entanto, caso os seus sistemas e o pessoal responsável possuam a referida capacidade técnica para efeitos de recolha, registo, colaboração ou apoio, o Artigo obriga a que sejam tomadas as medidas necessárias nesse sentido. Por exemplo, mesmo que a tal não se recorra no decurso normal das actividades levadas a cabo pelo fornecedor de serviços, o sistema poderia ser reconfigurado de forma a permitir a execução destas medidas ou o fornecedor de serviços poderia dispor já dos programas informáticos necessários à execução das mesmas. Nesse caso, o Artigo exigiria que o fornecedor de serviços procedesse à aplicação ou à colocação em funcionamento das soluções supracitadas, em conformidade com os termos da lei.

222. Uma vez que se trata de uma medida a ser empreendida a nível nacional, as medidas são aplicáveis à recolha ou ao registo relativamente a comunicações específicas, efectuadas no seio do território da respectiva Parte. Assim, em termos práticos, as obrigações serão geralmente aplicáveis às situações em que o fornecedor de serviços disponha, nesse território, de alguma infra-estrutura ou equipamento passível de permitir a execução das medidas acima mencionadas, não sendo necessário que a sua sede ou estabelecimento de actividade principal se situe nesse mesmo território. Para os fins a que se propõe a presente Convenção, considera-se que uma comunicação é efectuada no seio do território de uma Parte, caso uma das partes intervenientes na comunicação (seres humanos ou computadores) esteja situada nesse território ou caso o equipamento informático ou de telecomunicação através do qual é transmitida a comunicação, esteja localizado no referido território.

223. De um modo geral, as duas possibilidades de recolha de dados de tráfego mencionadas no parágrafo 1(a) e (b) não constituem alternativas, pelo que não se excluem mutuamente. Salvo no caso previsto no parágrafo 2, as Partes deverão certificar-se de que ambas as medidas poderão ser empreendidas. Este aspecto é indispensável, pois no caso de um fornecedor de serviços não dispor da capacidade técnica necessária para levar a cabo a operação de recolha ou registo de dados de tráfego (1(b)), as autoridades competentes para a aplicação da lei, da respectiva Parte, deverão ter a possibilidade de tomar a seu cargo a execução de tal operação (1(a)). De forma análoga, também a obrigação, assumida em virtude do parágrafo 1 (b)(ii), de prestação de apoio e colaboração com as autoridades competentes no âmbito da recolha ou registo de dados de tráfego, perderá todo o sentido caso as autoridades competentes não se encontrem, elas próprias, investidas dos poderes necessários para proceder à recolha ou registo dos dados de tráfego. Além disso, no caso de algumas redes de área local (LAN), em que não existe a participação de um fornecedor de serviços, a única forma de efectuar a recolha ou o registo dos dados seria incumbir dessa tarefa as autoridades responsáveis pela investigação. As duas medidas referidas no parágrafo 1 (a) e (b) não terão, pois, que ser aplicadas em todas as situações, mas o Artigo requer a existência e disponibilidade de ambos os métodos.

224. Todavia, esta dupla obrigação coloca algumas dificuldades a certos Estados, nos quais as autoridades competentes para a aplicação da lei apenas dispõem da possibilidade de interceptar dados em sistemas de telecomunicações com a intervenção de um fornecedor de serviços, ou pelo menos, de forma velada, não sem o conhecimento do fornecedor de serviços. Assim sendo, o parágrafo 2 contempla este tipo de situações. Nos casos em que a Parte, por motivos que se prendem com os "princípios estabelecidos pelo seu sistema jurídico nacional", não reuna as condições necessárias para adoptar as medidas descritas no parágrafo 1 (a), poderá adoptar uma outra abordagem, no sentido, por exemplo, de obrigar os fornecedores de serviços a fornecerem apenas os meios técnicos necessários para que as autoridades competentes possam assegurar a recolha dos dados de tráfego em tempo real. Nesse caso, serão ainda aplicáveis as restantes limitações relativas ao território, à especificidade das comunicações e à utilização de meios técnicos.

225. Tal como verificado relativamente à intercepção em tempo real de dados de conteúdo, também a recolha em tempo real de dados de tráfego apenas será eficaz se for realizada sem o conhecimento das pessoas que são objecto da investigação. A intercepção é uma operação, por natureza, sub-reptícia e deverá ser executada de forma a que as partes intervenientes na comunicação,

dela não se apercebam. Sobre os fornecedores de serviços e seus colaboradores, que tenham conhecimento da intercepção, recairá a obrigação de manter o sigilo por forma a que a operação seja bem sucedida.

226. O parágrafo 3 obriga as partes a adoptar as medidas do foro legislativo e outras que se afigurem pertinentes no sentido de obrigar um fornecedor de serviços a manter confidenciais quaisquer informações, ou factos com estas relacionados, acerca da execução de qualquer uma das medidas referidas no presente Artigo, no que toca à recolha em tempo real de dados de tráfego. Esta disposição não apenas garante a confidencialidade da investigação, como também isenta o fornecedor de serviços de quaisquer obrigações contratuais ou outras, previstas pelo sistema jurídico vigente, de notificação dos subscritores acerca dos quais estão a ser recolhidos os dados. A aplicação do disposto no parágrafo 3 poderá ter lugar através da implementação de obrigações explícitas de acordo com os termos da lei. Por outro lado, uma Parte deverá poder assegurar a confidencialidade da medida com base noutras disposições existentes no quadro da legislação nacional, tais como o poder de instauração de processo penal por obstrução à justiça, face a todos aqueles que colaborem com os infractores ao fornecerem a informação de que estão a ser alvo de investigação. Embora um requisito específico de confidencialidade (com uma sanção eficaz em caso de incumprimento) constitua o procedimento preferível, o estabelecimento de infracções por obstrução à justiça poderá constituir um meio alternativo de impedir a divulgação inadequada e, assim, ser suficiente para efeitos da aplicação do disposto no presente parágrafo. No caso de serem instituídas obrigações explícitas de confidencialidade, estas deverão ficar sujeitas às condições e salvaguardas prescritas pelos Artigos 14º e 15º. Dada a natureza sub-reptícia da medida de investigação em causa, as referidas condições ou salvaguardas deverão fixar um prazo máximo de duração da obrigação.

227. Tal como mencionado anteriormente, o interesse de cariz privado é, em geral, considerado menor quando se relaciona com a recolha de dados de tráfego do que com a intercepção de dados de conteúdo. A recolha dos dados de tráfego no que diz respeito à hora, duração e dimensão da comunicação, revela pouca ou nenhuma informação de carácter pessoal acerca de um indivíduo e da sua forma de pensar. Contudo, poderá existir uma componente de cariz privado mais forte em dados relativos à origem ou ao destino de uma comunicação (por exemplo, as páginas Web visitadas). A recolha destes dados poderá, pois, nalgumas circunstâncias, permitir a elaboração de um perfil dos interesses da pessoa em questão, bem como das pessoas a ela associadas e

do meio social em que vive. Assim, as Partes deverão ter em conta estes factores ao estipularem as salvaguardas apropriadas e os pré-requisitos legais de aplicação destas medidas, em conformidade com as disposições contidas nos Artigos 14º e 15º.

Intercepção de dados de conteúdo (Artigo 21º)

228. A recolha de dados relativamente ao conteúdo das telecomunicações (por exemplo, nas conversas telefónicas) desde sempre tem demonstrado ser uma ferramenta de investigação útil para determinar se a comunicação se reveste de um carácter ilegal (por exemplo, quando a comunicação constitui uma ameaça de crime ou assédio, uma conspiração de índole criminosa ou declarações falsas), bem como para reunir provas sobre infracções passadas ou futuras (por exemplo, tráfico de estupefacientes, homicídio, infracções de cariz económico, etc.). As comunicações através de computadores podem constituir ou servir de prova dos mesmos tipos de actos criminosos. No entanto, visto que a tecnologia informática permite transmitir grandes quantidades de dados, incluindo texto, imagens e sons, existe também um maior potencial para a prática de crimes que envolvam a distribuição de conteúdos ilegais (por exemplo, pornografia infantil). A prática de muitos dos crimes informáticos conhecidos, implica a transmissão ou a comunicação de dados, como é o caso, por exemplo, das comunicações efectuadas para aceder ilicitamente a um sistema informático ou para propagar vírus informáticos. Não é, pois, possível determinar, em tempo real, a natureza ilegal e nociva destas comunicações sem que se proceda à intercepção do conteúdo da mensagem. Não existindo a possibilidade de determinar e impedir a ocorrência de criminalidade, apenas restaria às autoridades competentes a investigação dos crimes cometidos no passado, cujos efeitos prejudiciais já não podem ser travados. Assim sendo, a intercepção em tempo real de dados de conteúdo relativos a comunicações informáticas é tão ou mais importante do que a intercepção em tempo real de telecomunicações.

229. O termo "dados de conteúdo" refere-se ao conteúdo informativo da comunicação, isto é, o significado ou o teor da comunicação, ou a mensagem ou informação transmitida pela comunicação. Designa, assim, todos os elementos transmitidos como parte da comunicação mas que não constituam dados de tráfego.

230. A maioria dos aspectos deste Artigo é idêntica aos do Artigo 20º. Portanto, os comentários, acima, relativamente à recolha ou registo de dados de tráfego, às obrigações de colaboração e prestação de apoio, bem como às obrigações

de confidencialidade, são igualmente aplicáveis à intercepção de dados de conteúdo. Devido ao facto de ser mais elevado o interesse de cariz privado, quando associado aos dados de conteúdo, a medida de investigação é, pois, limitada a "um conjunto de infracções graves a ser determinado pela legislação nacional".

231. Do mesmo modo, tal como indicado acima, nos comentários relativos às disposições contidas no Artigo 20º, as condições e salvaguardas aplicáveis à intercepção em tempo real de dados de conteúdo poderão ser mais rigorosas do que aquelas aplicáveis à recolha em tempo real de dados de tráfego, ou à busca e apreensão ou, de forma semelhante, ao acesso ou guarda de dados armazenados.

Secção 3 - Jurisdição

Jurisdição (Artigo 22º)

232. O presente Artigo define uma série de critérios segundo os quais as Partes contratantes ficam obrigadas a estipular a sua jurisdição relativamente às infracções penais enumeradas nos Artigos 2º a 11º da Convenção.

233. O disposto na alínea a. do parágrafo 1 assenta no princípio da territorialidade. Cada Parte ficará obrigada a punir a prática dos crimes definidos pela presente Convenção, quando estes sejam cometidos no seu território. Assim, por exemplo, uma Parte deverá considerar ser da sua jurisdição territorial um caso em que tanto a pessoa responsável pela invasão de um sistema informático como o sistema alvo dessa invasão se encontrem no seu território, o mesmo se aplicando às situações em que o sistema alvo de invasão esteja localizado no seu território e a pessoa responsável não esteja.

234. Foi ainda analisada a possibilidade de incluir uma disposição que exigisse de cada Parte a definição da sua jurisdição relativamente às infracções que envolvessem satélites registados em seu nome. Todavia, os redactores da presente Convenção decidiram que uma tal disposição seria desnecessária uma vez que as comunicações ilegais efectuadas por meio de satélites apenas poderão ser provenientes da Terra e/ou ser recebidas na Terra. Assim, seria aplicável uma das bases da jurisdição de uma Parte, tal como definidas no parágrafo 1(a) – (c), no caso de a transmissão ter o seu início ou o seu fim num dos locais especificados. Além disso, na medida em que a infracção que envolve uma comunicação via satélite é cometida por um cidadão de uma das Partes, sem pertencer à jurisdição territorial de qualquer Estado, a alínea d. do parágrafo 1 estabelece então uma base jurisdicional. Por último, os redactores

interrogaram-se sobre se o registo constituiria um fundamento apropriado para a definição da jurisdição penal, dado que, em muitos casos, não haveria qualquer relação efectiva entre a infracção cometida e o Estado de registo, pois um satélite não é mais do que um simples meio de transmissão.

235. As alíneas b. e c. do parágrafo 1 baseiam-se numa variante do princípio da territorialidade. De acordo com o disposto nas referidas alíneas, cada Parte deverá estipular uma jurisdição penal relativamente a infracções cometidas a bordo de um navio que ostente a sua bandeira ou de um avião registado ao abrigo das suas respectivas leis. Esta obrigação vigora já em virtude da legislação adoptada por inúmeros Estados, dado que os referidos navios e aviões são frequentemente considerados como sendo uma extensão do território de um Estado. Este tipo de jurisdição reveste-se de grande utilidade nos casos em que o navio ou o avião em causa não se encontram localizados no seu território aquando do cometimento da infracção, pelo que o disposto na alínea a. do parágrafo 1 não seria aplicável em termos de definição da jurisdição. No caso de a infracção ser cometida a bordo de um navio ou de um avião que se encontre fora do território da Parte correspondente à bandeira ostentada ou ao registo, nenhum outro Estado poderia exercer a sua jurisdição se não existisse uma tal regra. Além disso, no caso de uma infracção cometida a bordo de um navio ou de um avião que apenas estivesse de passagem nas águas ou no espaço aéreo de outro Estado, este último teria de fazer face a entraves significativos ao exercício da sua jurisdição, revelando-se assim muito útil o facto de o Estado de registo também ser considerado competente nesta matéria.

236. A alínea d. do parágrafo 1 tem por base o princípio da nacionalidade. A teoria da nacionalidade é mais frequentemente invocada pelos Estados que aplicam o direito civil. Em conformidade com o referido princípio, os cidadãos de um Estado obrigar-se-ão a respeitar a legislação nacional, mesmo encontrando-se fora do seu território. Em virtude do disposto na alínea d., nos casos em que um cidadão nacional cometa uma infracção no estrangeiro, a respectiva Parte é obrigada a dispor da capacidade necessária à instauração de um processo penal, se o comportamento em causa for igualmente punível ao abrigo da legislação adoptada pelo Estado no qual a infracção foi cometida, ou se a mesma tiver tido lugar fora da jurisdição territorial de qualquer Estado.

237. O parágrafo 2 autoriza as Partes a formularem uma reserva relativamente às bases de jurisdição descritas no parágrafo 1, alíneas b., c., e d. No entanto, não será permitida qualquer reserva no diz respeito à definição da jurisdição territorial, tal como prescrita pela alínea a., ou à obrigação de estipular a

jurisdição nos casos abrangidos pelo princípio de "aut dedere aut judicare" (extraditar ou instaurar processo penal) ao abrigo do disposto no parágrafo 3, nos casos em que a Parte recuse proceder à extradição do presumível autor da infracção, devido à sua nacionalidade, quando este se encontre no seu território. A jurisdição estabelecida com base no disposto no parágrafo 3, mostra-se necessária a fim de assegurar que uma Parte que recusa a extradição de um cidadão, dispõe de meios legais para levar a cabo as investigações e instaurar o processo penal no seio do seu território, caso tal lhe seja solicitado pela Parte que fez o pedido de extradição em consonância com os requisitos constantes do parágrafo 6 do Artigo 24º sobre Extradição, da presente Convenção.

238. As bases de jurisdição descritas no parágrafo 1 não são exclusivas. O disposto no parágrafo 4 do presente Artigo autoriza as Partes a definirem também, em conformidade com a sua legislação interna, outros tipos de jurisdição penal.

239. No caso de infracções cometidas por meio da utilização de sistemas informáticos, haverá situações em que pertence a mais do que uma Parte a jurisdição sobre alguns ou todos os intervenientes numa dada infracção. Por exemplo, muitos dos casos de propagação de vírus informáticos, cometimento de fraudes e violação de direitos de autor, através da utilização da Internet, têm como alvo vítimas que se encontram espalhadas por vários países. A fim de evitar a duplicação de esforços, incómodos desnecessários para as testemunhas ou a concorrência entre os serviços competentes para a aplicação da lei, dos vários Estados envolvidos, ou, por outro lado, a fim de reforçar a eficácia ou equidade dos processos, as respectivas Partes deverão proceder a uma consulta de modo a determinar qual a jurisdição mais apropriada para intentar a acção. Nalguns casos, por motivos que se prendem com a eficácia, os Estados terão todo o interesse em escolher apenas uma única jurisdição, ao passo que, noutros casos será preferível que um Estado se ocupe de uns intervenientes enquanto outro Estado, ou vários outros Estados, se ocupam de outros intervenientes. Neste parágrafo encontram-se, assim, previstas ambas as soluções. Por fim, a obrigação de consultar não é absoluta, devendo ser aplicável "sempre que tal se mostre adequado". Assim, por exemplo, se uma das Partes tem conhecimento de que a consulta não é necessária (por exemplo, no caso de ter recebido a confirmação de que a outra Parte não tenciona instaurar um processo), ou se a Parte é da opinião de que a consulta é susceptível de prejudicar a sua investigação ou o processo penal instaurado, poderá então optar por adiar a consulta ou recusá-la.

Capítulo III – Cooperação internacional

240. O Capítulo III contém diversas disposições relativas à extradição e à assistência jurídica mútua entre as Partes.

Secção 1 – Princípios gerais

Título 1 – Princípios gerais relativos à cooperação internacional

Princípios gerais relativos à cooperação internacional (Artigo 23º)

241. O Artigo 23º enuncia três princípios gerais no que respeita à cooperação internacional prevista no Capítulo III.

242. Primeiramente, o Artigo especifica que a cooperação internacional deverá ter lugar entre as Partes "no âmbito mais alargado possível". Este princípio requer que as Partes cooperem amplamente umas com as outras, envidando todos os seus esforços no sentido da minoração dos obstáculos que eventualmente se coloquem a um fluxo, rápido e regular, da informação e das provas ao nível internacional.

243. Em seguida, o Artigo 23º define o âmbito geral da obrigação de cooperação: a cooperação deverá estender-se a todas as infracções penais relacionadas com sistemas informáticos e dados informatizados (isto é, as infracções incluídas no Artigo 14º, parágrafo 2, alíneas a e b.), bem como à recolha de provas sob a forma electrónica de uma dada infracção penal. Tal significa que, tanto nos casos de infracções cometidas por meio da utilização de um sistema informático, como nos casos de infracções comuns não cometidas através da utilização de um sistema informático (por exemplo, um homicídio) mas que envolvam provas sob a forma electrónica, serão pois aplicáveis os termos constantes do Capítulo III. Todavia, deverá salientar-se o facto de que os Artigos 24º (Extradição), 33º (Assistência Mútua relativamente à recolha de dados de tráfego em tempo real) e 34º (Assistência Mútua relativamente à intercepção de dados de conteúdo) autorizam as Partes a introduzir modificações ao campo de aplicação destas medidas.

244. Por fim, afirma-se que esta cooperação deverá ter lugar "em conformidade com as disposições contidas no presente Capítulo", e "através da aplicação dos respectivos instrumentos internacionais no que diz respeito à cooperação internacional em matéria penal, de acordos celebrados com base numa legislação uniforme e recíproca, bem como da implementação das leis nacionais."

A última cláusula estabelece o princípio geral de que as disposições contidas no Capítulo III não anulam nem substituem as disposições dos instrumentos internacionais relativos a assistência jurídica mútua e extradição, dos acordos recíprocos celebrados entre as Partes no que respeita a esta matéria (descritos mais pormenorizadamente na análise do Artigo 27º, mais adiante), ou as respectivas disposições da legislação nacional relativamente à cooperação internacional. Este princípio de base é explicitamente reforçado pelo disposto nos Artigos 24º (Extradição), 25º (Princípios gerais relativos à assistência mútua), 26º (Informação espontânea), 27º (Procedimentos relativos a pedidos de assistência mútua em caso de inexistência de acordos internacionais aplicáveis), 28º (Confidencialidade e limitação de utilização), 31º (Assistência mútua relativamente ao acesso a dados informatizados armazenados), 33º (Assistência Mútua relativamente à recolha de dados de tráfego em tempo real) e 34º (Assistência Mútua relativamente à intercepção de dados de conteúdo).

Título 2 – Princípios relativos à extradição

Extradição (Artigo 24º)

245. O parágrafo 1 especifica que a obrigação de extradição somente será aplicável às infracções definidas em conformidade com o disposto nos Artigos 2º a 11º da Convenção, que sejam passíveis de punição em virtude da legislação adoptada por ambas as Partes envolvidas, por meio da privação da liberdade por um período máximo de, pelo menos, um ano ou através da aplicação de uma pena mais grave. Os redactores decidiram introduzir um limite de pena mínima pois, ao abrigo da Convenção, as Partes poderão punir algumas das infracções mediante a aplicação de uma pena máxima de prisão relativamente curta (por exemplo, nos casos expostos nos Artigos 2º - acesso ilícito e 4º - interferência nos dados). Por este motivo, os redactores não julgaram conveniente estabelecer que cada uma das infracções definidas nos Artigos 2º a 11º fossem consideradas, per se, susceptíveis de ocasionar a extradição. Foi assim alcançado o consenso, tendo sido estipulado, como requisito geral, que uma infracção deverá ser considerada susceptível de ocasionar a extradição se – tal como prescrito pelo Artigo 2º da Convenção Europeia de Extradição (STE nº 24) – a pena máxima aplicável à infracção, relativamente ao autor da qual se efectuou um pedido de extradição, for de pelo menos um ano de prisão. A determinação de se a infracção pode ou não ocasionar a extradição, não depende da pena efectivamente imposta a cada caso concreto, mas sim do período máximo que, nos termos da lei, for aplicável no caso da infracção alvo de um pedido de extradição.

246. Por outro lado, em virtude do princípio geral de que a cooperação internacional prevista no Capítulo III deverá ter a sua aplicação em consonância com os instrumentos adoptados e em vigor entre as Partes, o parágrafo 1 prevê igualmente que, nos casos em que exista um tratado sobre extradição ou um acordo firmado com base numa legislação uniforme ou reciproca entre duas ou mais Partes (consultar a descrição deste termo nos comentários ao Artigo 27º abaixo) e cujo texto estipule uma pena mínima diferente para que haja lugar à extradição, será aplicável a referida pena mínima estipulada ao abrigo de tal tratado ou acordo. Assim, por exemplo, muitos tratados de extradição celebrados entre países europeus e países não europeus estabelecem que, uma infracção apenas será susceptível de ocasionar a extradição, caso a pena máxima imposta seja superior a um ano de prisão ou se aplique uma pena mais grave. Nestas circunstâncias, os especialistas em extradição, ao nível internacional, continuarão a aplicar a pena mínima normalmente prevista pela sua prática convencional a fim de determinar se uma infracção é ou não susceptível de ocasionar a extradição. Mesmo ao abrigo das disposições constantes da Convenção Europeia de Extradição (STE nº 24), as reservas formuladas poderão indicar uma pena mínima diferente para a extradição. Entre as Partes contratantes da referida Convenção, sempre que uma Parte que tenha formulado uma tal reserva, receba um pedido de extradição, a pena prevista na declaração de reserva deverá constituir a base para a determinação de se a infracção em causa é ou não passível de dar lugar à extradição.

247. O parágrafo 2 estipula que as infracções descritas no parágrafo 1 deverão ser consideradas como sendo infracções passíveis de extradição ao abrigo de todo e qualquer tratado de extradição existente ou a ser celebrado entre as Partes, devendo ainda ser incluídas em futuros acordos que sejam negociados entre as referidas Partes. Tal não significa que a extradição deva ser aplicável sempre que for apresentado um pedido nesse sentido, mas que deverá existir a possibilidade de recorrer à extradição das pessoas responsáveis pelas ditas infracções. Em virtude do parágrafo 5, as Partes poderão definir outros requisitos aplicáveis à extradição.

248. Em virtude do parágrafo 3, uma Parte que não reuna as condições necessárias para conceder a extradição, quer devido à inexistência de um tratado de extradição com a Parte requerente, quer porque os tratados existentes não cobrem um pedido apresentado relativamente às infracções definidas em conformidade com a presente Convenção, poderá aplicar a própria Convenção como base jurídica para entregar a pessoa cuja extradição foi pedida, embora nada obrigue a que proceda desta forma.

249. O parágrafo 4 prevê que, nos casos em que uma Parte utilize um sistema regulamentar geral para levar a cabo a extradição, em vez de se basear num tratado de extradição existente, deverá a Parte ficar obrigada a incluir as infracções descritas no parágrafo 1 no conjunto das infracções para as quais é possível recorrer à extradição.

250. O parágrafo 5 determina que a Parte requerida não será obrigada a proceder à extradição caso considere que não foram satisfeitos os termos e condições previstos no tratado ou na legislação aplicável. Trata-se, pois, de mais um exemplo do princípio segundo o qual a cooperação internacional deverá ser levada a cabo em conformidade com os termos dos instrumentos internacionais aplicáveis e em vigor entre as Partes, os acordos recíprocos existentes ou a legislação adoptada a nível nacional. Assim, as condições e limitações prescritas pela Convenção Europeia de Extradição (STE nº 24) e pelos seus Protocolos Adicionais (STE nº 86 e STE nº 98) aplicar-se-ão às Partes intervenientes nos referidos instrumentos, e a extradição poderá ser recusada com base nos mesmos (por exemplo, o Artigo 3º da Convenção Europeia de Extradição prevê que a extradição deverá ser recusada caso se considere que a infracção se reveste de um carácter político, ou caso se julgue que o pedido foi apresentado para fins de instauração de processo penal ou punição relativamente a uma dada pessoa, por motivos que se prendem, inter alia, com questões de raça, religião, nacionalidade ou opinião política).

251. O parágrafo 6 aplica o princípio de "aut dedere aut judicare" (extraditar ou instaurar processo penal). Uma vez que muitos Estados recusam a extradição dos seus cidadãos, os infractores, que são encontrados no seio do território da Parte cuja nacionalidade possuem, poderão evitar de responder por um crime cometido no território de outra Parte, a menos que as autoridades locais sejam obrigadas a intervir. Em virtude do disposto no parágrafo 6, se uma outra Parte pediu a extradição do autor da infracção e a referida extradição foi recusada devido ao facto de o autor da infracção ser um cidadão da Parte requerida, esta última deverá, mediante solicitação da Parte requerente, remeter o caso às autoridades competentes para fins de instauração de processo penal. Se a Parte cujo pedido de extradição foi recusado não solicitar que o caso seja submetido, a nível local, a uma investigação e instauração de processo penal, não recairá sobre a Parte requerida qualquer obrigação de intervir. Além do mais, caso não tenha sido efectuado qualquer pedido de extradição ou se a extradição tiver sido recusada com base noutros aspectos que não a nacionalidade do infractor, o presente parágrafo não obriga a que a Parte requerida submeta o caso às autoridades nacionais para fins de instauração de processo

penal. Adicionalmente, o parágrafo 6 determina que a investigação e o processo penal sejam tratados, a nível local, de forma célere, devendo estes ser levados a cabo com o mesmo rigor aplicável a "qualquer outra infracção de natureza comparável" de acordo com a legislação adoptada pela Parte que submete o caso. A referida Parte deverá comunicar o resultado da investigação e do processo à Parte responsável pela emissão do pedido.

252. De modo a que cada Parte saiba a quem dirigir os seus requerimentos de prisão preventiva ou extradição, o parágrafo 7 determina que, na ausência de um tratado aplicável, as Partes deverão comunicar ao Secretário Geral do Conselho da Europa, o nome e morada das suas respectivas autoridades responsáveis pela emissão e recepção dos pedidos de extradição ou de prisão preventiva. Esta disposição limita-se, pois, às situações em que não vigore entre as Partes um tratado de extradição, visto que em caso de existência de um tal tratado de extradição, bilateral ou multilateral, entre as Partes (tal como a STE nº 24), estas últimas saberão a quem dirigir os seus pedidos de extradição e de prisão preventiva, sem que seja necessário obter um registo das respectivas autoridades. A comunicação ao Secretário Geral deverá ter lugar no acto da assinatura ou aquando do depósito dos instrumentos de ratificação, aceitação, aprovação ou adesão das Partes. É de salientar que a nomeação de uma autoridade não exclui a possibilidade de recurso à via diplomática.

Título 3 – Princípios gerais relativos à assistência mútua

Princípios gerais relativos à assistência mútua (Artigo 25º)

253. Os princípios gerais que regem a obrigação de prestação de assistência mútua encontram-se descritos no parágrafo 1. A cooperação deverá ser levada a cabo "no âmbito mais alargado possível". Assim, tal como prescrito pelo Artigo 23º ("Princípios gerais relativos à cooperação internacional"), a assistência mútua deverá, por princípio, ser alargada e as barreiras à mesma serem estritamente limitadas. Em segundo lugar, e igualmente como disposto no Artigo 23º, a obrigação de cooperação aplicar-se-á, em princípio, tanto às infracções penais relacionadas com sistemas informáticos e dados informatizados (isto é, as infracções contempladas pelo Artigo 14º, parágrafo 2, alíneas a e b), como à recolha de provas sob a forma electrónica de uma dada infracção penal. Foi decidido impor uma obrigação de cooperação relativamente a esta vasta categoria de infracções, pois que, em ambos os domínios se sente a necessidade de racionalização dos mecanismos da cooperação internacional. Contudo, os

Artigos 34º e 35º conferem às Partes a possibilidade de modificação do campo de aplicação destas medidas.

254. Outras disposições do presente Capítulo apontam claramente para que a obrigação de prestação de assistência mútua deverá ser cumprida, de um modo geral, em conformidade com os termos dos acordos, legislações e tratados de assistência jurídica mútua aplicáveis. Em virtude do parágrafo 2, cada Parte deverá dispor da base jurídica necessária para levar a cabo as modalidades específicas de cooperação descritas nas restantes disposições contidas neste Capítulo, caso os seus referidos tratados, legislações e acordos não incluam já tais directrizes. A disponibilidade destes mecanismos, em especial os mencionados nos Artigos 29º a 35º (Disposições específicas – Títulos 1, 2, 3), é vital para a implementação de uma cooperação eficaz no que respeita aos casos de infracções penais relacionadas com computadores.

255. Algumas das Partes não necessitarão de adoptar quaisquer medidas específicas, do foro legislativo, de modo a proceder à aplicação do disposto no parágrafo 2, visto considerar-se que as disposições contidas nos tratados internacionais, que regulamentam detalhadamente os regimes de assistência mútua, adquirem automaticamente a força de lei. Parte-se, assim, do princípio de que as Partes poderão tratar estas disposições como possuindo força de lei, ou terão a flexibilidade suficiente, ao abrigo da legislação existente sobre assistência mútua, para proceder à execução das medidas citadas no presente capítulo, ou ainda, de que poderão rapidamente adoptar as leis necessárias para esse efeito.

256. Os dados informatizados são altamente voláteis. Bastará um simples premir de teclas ou a execução de programas automáticos para os apagar, tornando assim impossível chegar até ao autor da infracção ou destruindo as provas da sua culpabilidade. Alguns tipos de dados informatizados são armazenados apenas por curtos períodos de tempo antes de serem eliminados. Noutros casos, se as provas não forem recolhidas rapidamente, tal poderá causar prejuízos significativos a pessoas e bens. Em casos urgentes como estes, tanto o pedido como a resposta deverão caracterizar-se pela maior celeridade possível. O objectivo do parágrafo 3 é, portanto, o de facilitar a aceleração do processo de obtenção de assistência mútua, de modo a que não sejam perdidas provas ou informações importantes pelo facto de os dados serem eliminados, antes de o pedido de assistência mútua ser elaborado, transmitido e respondido. O parágrafo 3 prevê, assim, duas formas de atingir o referido objectivo: (1) investir as Partes dos poderes necessários para que estas emitam pedidos urgentes de cooperação através do recurso

a meios de comunicação expeditos, em vez da utilização dos tradicionais e muito mais lentos processos de transmissão de documentos escritos, em sobrescrito fechado e selado, por via da mala diplomática ou dos serviços de correio postal; e (2) solicitar às Partes requeridas que utilizem meios expeditos de resposta aos pedidos apresentados nas referidas circunstâncias. Cada Parte deverá dispor da capacidade para aplicar esta medida, caso esta não se encontre já prevista no âmbito dos seus respectivos tratados, legislações ou acordos de assistência mútua. O fax e o correio electrónico são mencionados a título meramente indicativo, dado que poderão ser igualmente utilizados quaisquer outros meios de comunicação expeditos e adequados às circunstâncias do caso concreto. Os avanços tecnológicos poderão ainda proporcionar outros meios de comunicação expeditos, os quais poderão ser utilizados para efectuar um pedido de assistência mútua. No que diz respeito às condições de autenticidade e de segurança citadas neste parágrafo, as Partes poderão decidir, entre si, qual a forma de assegurar a autenticidade das comunicações, bem como determinar a necessidade de protecções especiais de segurança (incluindo a encriptação) relativamente a casos particularmente delicados. Por fim, o parágrafo confere ainda à Parte requerida a possibilidade de, se assim o entender, solicitar uma confirmação formal a ser enviada pelas tradicionais vias após a transmissão expedita.

257. O parágrafo 4 enuncia o princípio segundo o qual a assistência mútua se encontra sujeita aos termos e condições estabelecidos pelas legislações internas e pelos tratados de assistência mútua aplicáveis. Estes regimes prevêem salvaguardas relativamente aos direitos de pessoas que se encontrem no território da Parte requerida e que possam ser objecto de um pedido de assistência mútua. Assim, por exemplo, uma medida intrusiva tal como uma operação de busca e apreensão, não será executada em nome de uma Parte requerente, salvo se tiverem sido satisfeitos os requisitos fundamentais da Parte requerida para que a medida possa ser aplicável no âmbito de um caso interno. As Partes poderão igualmente garantir a protecção dos direitos das pessoas em relação aos objectos apreendidos e fornecidos através da assistência jurídica mútua.

258. Contudo, o disposto no parágrafo 4 não será aplicável se existirem "indicações expressas em contrário no presente Capítulo". Esta cláusula tem por finalidade sublinhar o facto de que a Convenção contém várias excepções significativas ao princípio geral. A primeira das referidas excepções decorre do disposto no parágrafo 2 deste Artigo, em virtude do qual cada Parte fica obrigada a levar a cabo as formas de cooperação descritas nos restantes artigos

deste Capítulo (tais como a preservação, a recolha de dados em tempo real, a busca e apreensão, e a manutenção de uma rede 24/7), independentemente de estas medidas se encontrarem já inscritas nos seus tratados de assistência jurídica mútua, legislações ou acordos equivalentes nesta matéria. Outra das referidas excepções é a que figura no Artigo 27º, a qual deverá ser sempre aplicada à execução dos pedidos em vez de uma disposição da legislação interna da Parte requerida, que regulamente a cooperação internacional na ausência de um tratado de assistência mútua ou de um acordo equivalente entre a Parte requerente e a Parte requerida. O Artigo 27º apresenta um sistema de condições e de motivos de recusa. Uma outra excepção, especificamente prevista neste parágrafo, consiste no facto de que a cooperação não poderá ser recusada, pelo menos no que se refere às infracções definidas ao abrigo dos Artigos 2º a 11º da Convenção, por ser considerado, pela Parte requerida, que o pedido diz respeito a infracções de natureza "fiscal". Finalmente, o disposto no Artigo 29º constitui uma outra excepção, sendo que a preservação não poderá ser recusada por razões que se prendam com a questão da criminalidade dupla, apesar de ser possível formular uma reserva a este respeito.

259. O parágrafo 5 é, essencialmente, uma definição do conceito de criminalidade dupla para efeitos da assistência mútua a ser prestada ao abrigo das disposições contidas neste Capítulo. Nos casos em que a Parte requerida esteja autorizada a exigir a dupla criminalidade como condição necessária à prestação de assistência (por exemplo, quando a Parte requerida se reserve o direito de exigir a dupla criminalidade relativamente à preservação de dados prevista pelo parágrafo 4 do Artigo 29º, intitulado "Preservação expedita de dados informatizados armazenados"), deverá considerar-se que tal requisito foi preenchido caso a conduta subjacente à infracção para a qual é pedida a assistência mútua seja igualmente classificada como infracção penal à luz da legislação interna da Parte requerida, mesmo que tal legislação inclua a dita infracção numa categoria diferente de infracções 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 criminalidade dupla. Tendo em conta as diferenças verificadas ao nível dos sistemas jurídicos nacionais, é inevitável a constatação das variações existentes no plano da terminologia e da categorização dos comportamentos de índole criminosa. Se a conduta em causa constituir uma infracção 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.

Informação espontânea (Artigo 26º)

260. O presente Artigo teve por base as disposições contidas em instrumentos anteriores do Conselho da Europa, tais como as do Artigo 10º da Convenção relativa ao Branqueamento, Detecção, Apreensão e Confisco dos Produtos do Crime (STE nº 141) e do Artigo 28º da Convenção de Direito Penal sobre a Corrupção (STE nº 173). É cada vez mais frequente dar-se o caso de uma Parte dispor de informação importante e estar convicta de que a mesma poderá ter interesse no contexto das investigações e das acções penais levadas a cabo por uma outra Parte que, por sua vez, não tem conhecimento da existência de tal informação. Em casos como este, não será apresentado qualquer pedido de assistência mútua. O parágrafo 1 autoriza o Estado que está de posse da informação a comunicá-la a um outro Estado, sem que haja lugar a um requerimento prévio. Esta disposição reveste-se de alguma utilidade, na medida em que, em conformidade com as leis vigentes nalguns Estados, é necessário que se conceda uma tal autoridade a fim de poder prestar assistência mútua na ausência de um pedido. Uma Parte não ficará, contudo, obrigada a proceder espontaneamente ao envio de informação para outra Parte, podendo assim exercer o seu poder discricionário de acordo com as circunstâncias do caso concreto. Além disso, a divulgação espontânea de informação não isenta a Parte responsável pela divulgação, caso lhe pertença a jurisdição, da investigação e da instauração de processos relativamente aos factos divulgados.

261. O parágrafo 2 aborda a questão de que, em determinadas circunstâncias, uma Parte apenas procederá ao envio espontâneo da informação, se as informações de cariz mais delicado forem mantidas confidenciais ou se a utilização dessas informações for sujeita a outras condicionantes. Nomeadamente, a confidencialidade representa um factor de relevo quando se trata de casos em que a divulgação ao público de tais informações seja passível de comprometer interesses importantes do Estado responsável pela divulgação, por exemplo, quando é necessário manter secreto o método de recolha da informação ou o facto de que um grupo de criminosos se encontra sob investigação. Caso se saiba, de antemão, que a Parte receptora não poderá respeitar uma condição apresentada pela Parte emissora relativamente à utilização das informações (por exemplo, quando não lhe for possível cumprir um requisito de confidencialidade devido ao facto de a informação em causa ser necessária como prova num julgamento público), a referida Parte receptora deverá alertar

para esse aspecto a Parte emissora que, por sua vez, poderá optar por não divulgar a informação. Todavia, se a Parte receptora concordar em satisfazer essa condição deverá, pois, honrar o seu compromisso. Prevê-se, assim, que as condições impostas pelo presente Artigo seriam compatíveis com as que poderiam ser impostas pela Parte emissora na sequência de um pedido de assistência mútua efectuado pela Parte receptora.

Título 4 - Procedimentos relativos a pedidos de assistência mútua em caso de inexistência de acordos internacionais aplicáveis

Procedimentos relativos a pedidos de assistência mútua em caso de inexistência de acordos internacionais aplicáveis (Artigo 27º)

262. O Artigo 27º vincula as Partes à aplicação de certos procedimentos e condições relativamente a pedidos de assistência mútua, sempre que não exista qualquer tratado ou acordo de assistência mútua, com base em legislação uniforme ou recíproca, vigente entre as Partes requerente e requerida. Assim, o Artigo reforça o princípio geral de que a assistência mútua deverá ter lugar através da aplicação dos respectivos tratados ou acordos semelhantes de assistência mútua. Os redactores da presente Convenção declinaram a possibilidade de criação de um regime geral distinto de assistência mútua ao qual se recorreria em alternativa a outros acordos e instrumentos aplicáveis, tendo então considerado que seria mais conveniente remeter-se, de uma maneira geral, aos regimes fixados pelos tratados de assistência jurídica mútua em vigor, permitindo assim aos especialistas nesta matéria procederem à utilização dos instrumentos e acordos com os quais se encontram mais familiarizados e evitar o risco de confusão eventualmente resultante da implementação de regimes concorrentes. Tal como mencionado anteriormente, os mecanismos cuja necessidade se faz particularmente sentir no contexto de uma cooperação rápida e eficaz em matéria de criminalidade informática, tal como os previstos nos Artigos 29º a 35º (Disposições específicas – Títulos 1, 2, 3), são os únicos para os quais cada Parte será obrigada a estabelecer uma base jurídica, a fim de permitir a execução de tais modalidades de cooperação, caso os tratados, acordos ou legislações já existentes não contenham disposições nesse sentido.

263. Do acima exposto decorre que a maioria das modalidades de assistência mútua previstas no presente Capítulo, continuará a ser levada a cabo em conformidade com as disposições constantes da Convenção Europeia sobre Assistência Mútua em Matéria Penal (STE nº 30) e do seu Protocolo (STE nº 99), entre as Partes contratantes dos referidos instrumentos. Alternativamente, as

Partes na presente Convenção que tenham firmado entre si quaisquer tratados bilaterais de assistência jurídica mútua ou outros acordos multilaterais através dos quais seja regulamentada a assistência mútua em matéria penal (tal como entre os Estados-membros da União Europeia), deverão, pois, continuar a aplicar os seus respectivos termos, complementados pelos mecanismos especificamente aplicáveis ao crime informático ou ao crime relacionado com computadores, descritos nos restantes Artigos do Capítulo III, salvo em caso de ser acordada a aplicação, integral ou parcial, das disposições contidas no presente Artigo. A assistência mútua poderá ainda ter por base acordos celebrados ao abrigo de legislação uniforme ou recíproca em vigor, 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 (parágrafo 4 do Artigo 25º), e entre os membros da Commonwealth. Por fim, a referência aos acordos ou tratados de assistência mútua com base em legislação uniforme ou recíproca não se limita apenas aos instrumentos já existentes à data de entrada em vigor da presente Convenção, pelo que se encontram também abrangidos os instrumentos passíveis de serem adoptados no futuro.

264. Os parágrafos 2 a 10 do Artigo 27º (Procedimentos relativos a pedidos de assistência mútua em caso de inexistência de acordos internacionais aplicáveis) prevêem um conjunto de normas referentes à prestação de assistência mútua na ausência de um tratado ou acordo de assistência jurídica mútua, firmado com base em legislação uniforme ou recíproca, entre as quais se contam a constituição de autoridades centrais, a imposição de condições, a definição de fundamentos e procedimentos em casos de adiamento ou recusa, a confidencialidade dos pedidos e as comunicações directas. No que respeita a estes aspectos expressamente abordados, e perante a inexistência de um tratado ou acordo de assistência jurídica mútua baseado em legislação uniforme ou recíproca, serão aplicáveis as disposições contidas no presente Artigo em vez das disposições da legislação interna que normalmente regem as questões relacionadas com a assistência mútua. Paralelamente, o Artigo 27º não define normas relativas a outras matérias tradicionalmente tratadas pela legislação nacional em relação à assistência mútua na cena internacional. Por exemplo, não existem quaisquer disposições respeitantes à forma e ao conteúdo dos pedidos, à recolha dos depoimentos das testemunhas no território das Partes requerente ou requerida, à elaboração de registos negociais ou oficiais, à transferência de testemunhas prisioneiras, ou à assistência em matéria de confisco. No que respeita a estas questões, resulta do disposto no parágrafo 4 do Artigo 25º que, na ausência de uma disposição específica contida no

presente Capítulo, deverá a legislação da Parte requerida regulamentar as modalidades de prestação deste tipo de assistência.

265. O parágrafo 2 obriga à constituição de uma ou mais autoridades centrais responsáveis pelo envio de, e pela resposta a, pedidos de assistência. A instituição de autoridades centrais é uma característica comum aos actuais instrumentos de assistência mútua em matéria penal, sendo especialmente útil quando se trata de assegurar o tipo de reacção rápida que tão importante se afigura no contexto do combate à criminalidade informática ou relacionada com computadores. Em primeiro lugar, uma transmissão directa entre as referidas autoridades revela-se mais rápida e eficaz do que a transmissão efectuada pela via diplomática. Adicionalmente, a criação de uma autoridade central activa desempenha um papel relevante em termos de assegurar que tanto os pedidos recebidos como os pedidos emitidos são tratados de forma célere, que é prestado o necessário aconselhamento às entidades homólogas estrangeiras responsáveis pela aplicação da lei, no que concerne à melhor forma de satisfazer os requisitos legais vigentes no território da Parte requerida e, ainda, que todos os pedidos particularmente delicados ou urgentes são tratados em conformidade.

266. As Partes são convidadas, por razões de eficácia, a designar uma única autoridade central para os fins da prestação de assistência mútua. De um modo geral, o ideal seria que a autoridade nomeada para este efeito, em virtude do disposto num tratado de assistência jurídica mútua ou da legislação interna de uma Parte, representasse igualmente a autoridade central para os fins da aplicação do presente Artigo. No entanto, as Partes dispõem de uma flexibilidade que lhes permite designar mais do que uma autoridade central, sempre que tal se mostre apropriado ao abrigo do seu sistema de assistência mútua. Em caso de constituição de mais do que uma autoridade central, a Parte em questão deverá certificar-se de que a interpretação, atribuída por cada uma das referidas autoridades às disposições constantes da presente Convenção, segue a mesma linha de pensamento, bem como assegurar que tanto os pedidos recebidos como os emitidos são objecto de um tratamento rápido e eficaz. Caberá a cada uma das Partes informar o Secretário Geral do Conselho da Europa acerca dos nomes e dados de contacto (incluindo números de fax e endereços de correio electrónico) da(s) autoridade(s) designada(s) para tratar da recepção e da resposta a pedidos de assistência mútua ao abrigo das disposições do presente Artigo, obrigando-se as Partes a zelar pela actualização constante dos referidos elementos.

267. Um dos principais objectivos inerentes a um pedido de assistência mútua, por parte de um Estado, consiste em garantir o cumprimento da sua legislação interna relativamente à admissibilidade das provas, o que lhe permitirá usar as ditas provas em tribunal. De modo a assegurar que os requisitos probatórios são efectivamente satisfeitos, o parágrafo 3 incumbe a Parte requerida de proceder à execução dos pedidos em conformidade com os procedimentos especificados pela Parte requerente, salvo nos casos em que tal se mostre incompatível com a sua legislação. Note-se, pois, que este parágrafo somente se refere à obrigação de respeitar os requisitos processuais técnicos e não às garantias processuais fundamentais. Assim, por exemplo, a Parte requerente não poderá solicitar à Parte requerida a execução de uma operação de busca e apreensão, se esta não satisfizer os requisitos fundamentais prescritos pelo sistema jurídico da Parte requerida, relativamente a esta medida. Tendo em conta a natureza limitada da obrigação, foi decidido que o simples facto de o sistema jurídico da Parte requerida não contemplar tal procedimento não será considerado fundamento suficiente para recusar a aplicação do procedimento indicado pela Parte requerente, pelo que, para esse efeito, o referido procedimento teria que se revelar incompatível com os princípios jurídicos da Parte requerida. Por exemplo, a lei da Parte requerente poderá estabelecer como requisito processual que o depoimento de uma testemunha seja dado sob juramento. Isto posto, mesmo que a Parte requerida não estabeleça, ao nível da sua legislação interna, o requisito segundo o qual um depoimento terá que ser apresentado sob juramento, deverá pois satisfazer o pedido da Parte requerente.

268. O parágrafo 4 prevê a possibilidade de recusar a execução dos pedidos de assistência mútua apresentados em virtude do presente Artigo. A assistência poderá ser recusada com base nos motivos enumerados no parágrafo 4 do Artigo 25º (isto é, os fundamentos prescritos pela lei da Parte requerida), dos quais citamos o prejuízo causado à soberania do Estado, à segurança, à ordem pública ou a outros interesses essenciais, bem como os casos em que a infracção é considerada, pela Parte requerida, como sendo uma infracção de natureza política ou uma infracção, por sua vez, relacionada com uma infracção de natureza política. Em nome do princípio prevalecente que consiste em implementar a cooperação, de forma tão alargada quanto possível (consultar os Artigos 23º e 25º), os fundamentos de recusa definidos por uma Parte requerida deverão ser restritos e invocados com moderação. Os referidos fundamentos não deverão, assim, revestir-se de uma amplitude tal que seja passível de conduzir a situações de recusa categórica de cooperação ou de

prestação de cooperação mediante condições demasiado rígidas, relativamente a vastas categorias de provas ou informações.

269. Em consonância com esta abordagem, considerou-se que para além dos fundamentos descritos no Artigo 28º, a recusa de prestação de assistência, por motivos de protecção de dados, apenas poderá ser invocada em casos excepcionais. Uma tal situação poderá surgir se, após terem sido ponderados os interesses importantes envolvidos num caso em particular (por um lado, os interesses públicos, incluindo a correcta e sólida administração da justiça e, por outro lado, os interesses ligados à vida privada), o fornecimento dos dados específicos, procurados pela Parte requerente, colocar dificuldades de tão amplas repercussões que levaria a que fossem consideradas, pela Parte requerida, como afectando os interesses essenciais que constituem fundamento de recusa. Assim, não será pois permitida uma aplicação vasta, categórica ou sistemática dos princípios relativos à protecção de dados no sentido de recusar a cooperação. Deste modo, o facto de as Partes envolvidas possuírem sistemas distintos de protecção do cariz privado dos dados (tal como, por exemplo, a Parte requerente não dispor do equivalente a uma autoridade especializada em matéria de protecção de dados), ou utilizarem meios diferentes de protecção de dados pessoais (tal como a Parte requerente recorrer a outros meios que não o processo de eliminação para proteger a privacidade ou a exactidão dos dados pessoais recebidos pelas autoridades competentes para a aplicação da lei), não constitui, por si só, um fundamento justificativo de recusa. Ao invés de invocar os "interesses essenciais" enquanto uma base de recusa de cooperação, a Parte requerida deverá procurar proporcionar as condições necessárias à transferência dos dados. (consultar o parágrafo 6 do Artigo 27º e o parágrafo 271 do presente relatório).

270. O parágrafo 5 autoriza a Parte requerida a adiar, e não a recusar, a assistência nos casos em que a execução imediata do pedido se mostre prejudicial para as investigações ou acções penais levadas a cabo pelas suas autoridades. Assim, por exemplo, se a Parte requerente solicitar a comunicação de provas ou a apresentação do depoimento de uma testemunha para fins de investigação ou julgamento, e as referidas provas ou testemunhas forem necessárias para integrar um julgamento em fase inicial no território da Parte requerida, esta última disporá, pois, de um argumento válido para adiar a concessão de assistência.

271. O parágrafo 6 prevê que nos casos em que a Parte requerida seria normalmente levada a recusar ou adiar a assistência pedida, poderá alternativamente prestar a sua cooperação subordinando-a a determinadas condições.

Se as referidas condições não forem aceitáveis do ponto de vista da Parte requerente, a Parte requerida poderá então modificá-las ou exercer o seu direito de recusa ou adiamento da prestação de assistência. Uma vez que à Parte requerida cabe a obrigação de prestar a sua cooperação, de forma tão alargada quanto possível, foi acordado que tanto os direitos de recusa como os de imposição de condições deveriam ser exercidos moderadamente.

272. O parágrafo 7 obriga a Parte requerida a manter a Parte requerente informada acerca do seguimento dado ao pedido, e exige que sejam expostos os motivos em caso de recusa ou adiamento da prestação de assistência. A apresentação dos motivos poderá, entre outros aspectos, ajudar a Parte requerente a compreender a forma como a Parte requerida interpreta os requisitos decorrentes do presente Artigo, proporcionar uma base de consulta de modo a reforçar a eficácia de futuras prestações de assistência mútua, e fornecer à Parte requerente informações factuais anteriormente desconhecidas acerca da disponibilidade ou situação das testemunhas ou das provas.

273. Por vezes, poderá acontecer que uma Parte emita um pedido em relação a um caso particularmente delicado, ou a um caso em que as consequências de se tornarem públicos, prematuramente, os factos subjacentes ao pedido seriam desastrosas. Assim, o parágrafo 8 autoriza a Parte requerente a solicitar a manutenção da confidencialidade relativamente ao facto e ao conteúdo do pedido. No entanto, a confidencialidade apenas poderá ser solicitada na medida em que não impeça a Parte requerida de obter as provas ou as informações visadas; por exemplo, nos casos em que a divulgação das informações em questão é indispensável para obter um despacho do tribunal, necessário para a execução do pedido de assistência, ou nos casos em que seja preciso notificar determinadas pessoas singulares que estejam de posse das provas, acerca do pedido, de modo a que execução do mesmo possa ser bem sucedida. Se a Parte requerida não reunir as condições necessárias para poder cumprir o requisito de confidencialidade, deverá informar desse facto a Parte requerente, a qual poderá então optar por retirar ou modificar o pedido.

274. As autoridades centrais designadas em conformidade com o disposto no parágrafo 2, deverão comunicar directamente entre si. Todavia, em caso de urgência, os pedidos de assistência jurídica mútua poderão ser enviados directamente pelos juizes e promotores de justiça da Parte requerente aos seus homólogos da Parte requerida. O juiz ou promotor de justiça que aplicar este procedimento deverá igualmente enviar uma cópia do pedido à autoridade central do seu país para que esta última a transmita, por sua vez, à autoridade central da Parte requerida. Em virtude do prescrito na alínea b., os

pedidos poderão ser transmitidos por intermédio da Interpol. As autoridades da Parte requerida que recebam um pedido cujo foro de competência não lhe pertença, deverão, ao abrigo da alínea c. do referido parágrafo, honrar uma dupla obrigação. Em primeiro lugar, remeter o pedido às autoridades competentes da Parte requerida e, em segundo lugar, informar de tal facto as autoridades da Parte requerente. De acordo com a alínea d., os pedidos poderão ainda ser transmitidos directamente, sem a intervenção das autoridades centrais mesmo que não se revistam de um carácter urgente, desde que a autoridade da Parte requerida disponha das condições necessárias para satisfazer o pedido sem fazer uso de acções coercivas. Por fim, a alínea e. determina que uma Parte deverá, por intermédio do Secretário Geral do Conselho da Europa, informar as outras Partes de que, por razões de eficácia, as comunicações deverão ser enviadas directamente à respectiva autoridade central.

Confidencialidade e limitação de utilização (Artigo 28º)

275. Esta disposição prevê expressamente as limitações aplicáveis à utilização de informação ou de material, de modo a permitir que a Parte requerida possa, nos casos em que tais informações ou materiais sejam especialmente delicados, assegurar que a sua utilização é limitada ao estritamente necessário à concessão da assistência, ou garantir que a sua divulgação apenas se concretiza junto das entidades competentes para a aplicação da lei no território da Parte requerente. Estas limitações constituem salvaguardas e garantias que são, inter alia, aplicáveis para fins de protecção de dados.

276. Tal como para o Artigo 27º, também o Artigo 28º se aplicará 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. No caso de se encontrar em vigor um tal tratado ou acordo, as suas disposições relativas à confidencialidade e à limitação de utilização deverão prevalecer sobre as disposições do presente Artigo, salvo em caso de acordo firmado em contrário pelas Partes intervenientes. Tal evitará uma sobreposição relativamente aos tratados de assistência jurídica mútua, bilaterais e multilaterais, e a acordos análogos existentes, permitindo assim aos especialistas nesta matéria continuarem a aplicar o regime habitual em vez de tentarem aplicar dois instrumentos concorrentes e, eventualmente, contraditórios.

277. O parágrafo 2 permite que a Parte requerida, ao responder a um pedido de assistência mútua, possa impor dois tipos de condições. Primeiro, a Parte

requerida poderá solicitar que a informação ou o material fornecido seja mantido confidencial nos casos em que o referido pedido não possa ser satisfeito na ausência de tal condição, como por exemplo, quando se trata da identidade de um informante secreto. Não será, pois, apropriado exigir uma confidencialidade absoluta nos casos em que a Parte requerida seja obrigada a prestar a assistência pedida, uma vez que tal comprometeria, em muitas situações, o êxito da Parte requerente no contexto das suas investigações e acções penais, como por exemplo, impedindo-a de utilizar as provas num julgamento público (incluindo a divulgação obrigatória).

278. Segundo, a Parte requerida poderá fazer depender o fornecimento da informação ou do material, da condição de que os mesmos não sejam utilizados para outras investigações ou acções penais que não as referidas no pedido. Para que tal condição se aplique, é necessário que a Parte requerida o indique expressamente; caso contrário, não existirão quaisquer limitações de utilização que a Parte requerida deva observar. Nos casos de indicação expressa da referida condição, tal constituirá uma garantia de que a informação e o material em causa somente serão utilizados para os fins previstos no pedido, impossibilitando, assim, a sua utilização para outros fins sem o prévio consentimento da Parte requerida. Os negociadores previram duas excepções à capacidade de limitação de utilização das informações, encontrando-se as referidas excepções implícitas nos termos do presente parágrafo. Primeiramente, ao abrigo dos princípios jurídicos fundamentais de muitos Estados, se o material fornecido constituir um elemento de prova da inocência de um acusado, deverá o mesmo ser divulgado junto de uma autoridade judicial ou da defesa. Além disso, a maior parte dos materiais fornecidos em virtude da aplicação dos regimes de assistência mútua, destina-se a ser utilizada em tribunal, normalmente no contexto de julgamentos públicos (incluindo a divulgação obrigatória). Uma vez realizada esta divulgação, entende-se que o material passou a ser, essencialmente, do domínio público. Em situações como esta que acabamos de descrever, não será possível garantir a confidencialidade da investigação ou da acção penal relativamente à qual foi pedida a assistência mútua.

279. O parágrafo 3 determina que, caso a Parte para a qual a informação é enviada, não disponha da capacidade necessária para cumprir a condição imposta, deverá desde logo notificar a Parte emissora, a qual poderá então optar por não fornecer a informação. Contudo, se a Parte destinatária aceitar a referida condição, ficará vinculada ao cumprimento da mesma.

280. O parágrafo 4 prevê a possibilidade de solicitar à Parte requerente uma explicação acerca do uso que foi dado à informação ou ao material recebido

segundo as condições descritas no parágrafo 2, por forma a que a Parte requerida possa certificar-se de que a referida condição foi efectivamente cumprida. Mais se decidiu que, a Parte requerida não poderá pois exigir a comunicação de demasiados pormenores, como por exemplo, a indicação de todas as vezes que as informações ou materiais fornecidos foram consultados.

Secção 2 – Disposições específicas

281. O objectivo da presente Secção é o de instituir mecanismos específicos que permitam levar a cabo uma acção concertada e eficaz, no plano internacional, relativamente a casos que envolvam infracções relacionadas com computadores e provas sob a forma electrónica.

Título 1 – Assistência Mútua relativamente a medidas provisórias

Preservação expedita de dados informatizados armazenados (Artigo 29º)

282. O presente Artigo institui um mecanismo de âmbito internacional equivalente ao previsto no Artigo 16º para utilização a nível nacional. Assim, o parágrafo 1 deste Artigo autoriza as Partes a requerer, e o parágrafo 3 impõe que as Partes disponham da capacidade jurídica para obter, a preservação expedita dos dados armazenados no território da Parte requerida através de um sistema informático, de modo a que os dados não sejam alterados, removidos ou eliminados durante o período de tempo necessário à preparação, transmissão e execução de um pedido de assistência mútua para fins de obtenção dos dados. A preservação dos dados constitui uma medida provisória, de carácter limitado e que se destina a ser implementada com muito maior rapidez do que uma prestação de assistência mútua tradicional. Tal como anteriormente mencionado, os dados informatizados são altamente voláteis. Com um simples premir de teclas ou mediante a execução de programas automáticos, estes poderão ser apagados, alterados ou movidos, tornando impossível a identificação do autor do crime ou destruindo as provas incriminatórias. Alguns tipos de dados informatizados são armazenados apenas por curtos períodos de tempo antes de serem eliminados. Assim, concluiu-se ser necessário criar um mecanismo que permitisse assegurar a disponibilidade dos referidos dados durante o desenrolar do longo e complexo processo de execução de um pedido formal de assistência mútua, o qual poderá demorar semanas ou meses.

283. Sendo mais rápida do que o clássico processo de assistência mútua, esta medida é simultaneamente menos intrusiva. Não é, pois, exigido aos responsáveis pela prestação de assistência mútua da Parte requerida, que obtenham a posse dos dados junto do seu administrador. O método preferencial, para a Parte requerida, consiste em assegurar que o referido administrador (tratando-se frequentemente de um fornecedor de serviços ou de outros terceiros) procede à preservação dos dados (isto é, não os apaga) durante o período que decorre até que seja ordenada a sua posterior entrega aos serviços competentes para a aplicação da lei. Este procedimento tem como vantagens ser rápido e respeitar os direitos da pessoa visada no que concerne à sua vida privada, uma vez que os respectivos dados não serão divulgados nem examinados por qualquer entidade governamental até que sejam cumpridos todos os critérios aplicáveis à divulgação integral, em conformidade com os normais regimes de assistência mútua. Ao mesmo tempo, a Parte requerida encontra-se autorizada a seguir outros procedimentos no sentido de assegurar a rápida preservação dos dados, entre os quais se contam a emissão e execução expeditas de uma ordem de produção ou um mandado de busca relativamente aos dados. O factor chave consiste em poder accionar um processo extremamente rápido, a fim de evitar que os dados sejam irremediavelmente perdidos.

284. O parágrafo 2 descreve o conteúdo de um requerimento de preservação em conformidade com as disposições do presente Artigo. Tendo em conta que se trata de uma medida provisória e que o requerimento deverá ser preparado e transmitido rapidamente, a informação fornecida terá que ser sumária e incluir somente a informação mínima requerida de modo a permitir a preservação dos dados. Para além de especificar qual a autoridade que requer a preservação e qual a infracção que está na origem de um tal requerimento, aquele deverá conter outros elementos, tais como: uma síntese dos factos, informações suficientes para identificar os dados a serem preservados e a sua respectiva localização, uma exposição demonstrativa da necessidade de preservação, bem como da importância dos dados para a investigação ou acção penal relativa à infracção em causa. Por fim, a Parte requerente deverá comprometer-se a apresentar, posteriormente, um pedido de assistência mútua com a finalidade de obter a produção dos dados.

285. O parágrafo 3 define o princípio segundo o qual a criminalidade dupla não deverá ser exigida como condição prévia à preservação. De um modo geral, a aplicação do princípio da criminalidade dupla é contraproducente no contexto da preservação. Primeiramente, do ponto de vista das actuais práticas da assistência mútua, verifica-se uma tendência para eliminar o requisito da

criminalidade dupla no que respeita a todas as medidas processuais excepto as mais intrusivas, tais como a busca e apreensão ou a intercepção. Todavia, a preservação, tal como é encarada pelos redactores, não é uma medida particularmente intrusiva, uma vez que o administrador se limita a manter a posse dos dados que, nos termos da lei, já se encontravam na sua posse e que os dados não são divulgados aos responsáveis da Parte requerida nem examinados por estes últimos, antes da execução de um pedido oficial de assistência mútua com vista à divulgação dos referidos dados. Em segundo lugar, a prática dita-nos que o tempo necessário para obter os devidos esclarecimentos, de forma a constatar irrefutavelmente a existência da criminalidade dupla, é por vezes tão prolongado que poderá entretanto haver lugar à eliminação, remoção ou alteração dos dados. Por exemplo, na fase inicial de uma investigação, a Parte requerente poderá estar ciente de que ocorreu uma intrusão num computador situado no seu território, mas apenas tomar conhecimento da natureza e da extensão dos danos causados numa fase posterior. Se a Parte requerida tivesse que adiar a preservação dos dados de tráfego que iriam permitir detectar a fonte da intrusão, até que se concluísse da existência de criminalidade dupla, os dados decisivos seriam eliminados pelos fornecedores de serviços que, geralmente, apenas os conservam durante algumas horas ou alguns dias após a transmissão da comunicação. Assim, mesmo que a Parte requerente pudesse posteriormente constatar a existência de criminalidade dupla, os dados de tráfego considerados cruciais seriam já irrecuperáveis e o autor do crime não poderia já ser identificado por este meio.

286. Consequentemente, as Partes deverão, como regra geral, abster-se de requerer a criminalidade dupla para fins de preservação. No entanto, o parágrafo 4 prevê a possibilidade de formulação de uma reserva limitada, a qual passamos a descrever: se uma Parte requerer a criminalidade dupla como condição para responder a um pedido de assistência mútua relativamente à produção de dados, e caso tenha motivos para crer que, aquando da divulgação, o requisito da criminalidade dupla não terá sido satisfeito, a Parte poderá reservar-se o direito de requerer a criminalidade dupla como condição prévia à preservação. No que diz respeito às infracções definidas em conformidade com os Artigos 2º a 11º, parte-se do princípio de que o requisito da criminalidade dupla será automaticamente preenchido entre as Partes, salvo em caso de disposições contrárias que figurem nas reservas previstas pela Convenção e formuladas pelas Partes relativamente às referidas infracções. As Partes apenas poderão, portanto, impor esta condição no que se refere a outras infracções que não as definidas na presente Convenção.

287. Por outro lado, em virtude do disposto no parágrafo 5, a Parte requerida apenas poderá recusar um requerimento de preservação nos casos em que a sua execução seja passível de prejudicar a sua soberania, segurança, ordem pública ou outros interesses essenciais, ou caso considere tratar-se de uma infracção de natureza política ou uma infracção que, por sua vez, esteja relacionada com uma infracção de natureza política. Visto entender-se esta medida como sendo algo indispensável à eficácia da investigação e do processo penal instaurado relativamente a crimes informáticos ou relacionados com computadores, foi decidida a exclusão da possibilidade de adopção de qualquer outra base de recusa face a um requerimento de preservação.

288. Por vezes, a Parte requerida aperceber-se-á da probabilidade de o administrador dos dados agir de uma maneira que comprometa a confidencialidade ou, de algum modo, prejudique a investigação levada a cabo pela Parte requerente (por exemplo, quando os dados a serem preservados são detidos por um fornecedor de serviços controlado por um grupo de crime organizado ou pela própria pessoa alvo da investigação). Nestas situações, e em virtude do disposto no parágrafo 6, a Parte requerente deverá ser imediatamente notificada a esse respeito, de forma a poder avaliar se deverá sujeitar-se ao risco inerente à execução do requerimento de preservação ou procurar aplicar um método mais intrusivo, mas mais seguro, de concessão de assistência mútua, tal como a produção de dados ou a busca e apreensão.

289. Finalmente, o parágrafo 7 obriga a que cada uma das Partes assegure que os dados preservados de acordo com as disposições contidas no presente Artigo, serão mantidos por um período de, pelo menos, 60 dias enquanto se aguarda a recepção de um pedido formal de assistência mútua com vista à divulgação dos dados, devendo os mesmos continuar a ser conservados após a recepção do pedido.

Divulgação expedita dos dados de tráfego preservados (Artigo 30º)

290. O presente Artigo estabelece, no plano internacional, o equivalente ao poder instituído para aplicação ao nível nacional, pelo Artigo 17º. Frequentemente, e mediante solicitação de uma Parte no território da qual foi cometida uma infracção, a Parte requerida irá proceder à preservação dos dados de tráfego relativos a uma comunicação transmitida através dos seus computadores, a fim de detectar a origem da comunicação e identificar o autor da infracção ou localizar provas decisivas. Ao fazê-lo, a Parte requerida poderá descobrir que os dados de tráfego encontrados no seu território revelam que a comunicação foi encaminhada por um fornecedor de serviços situado num terceiro Estado,

ou até mesmo por um fornecedor no país da própria Parte requerente. Neste caso, a Parte requerida obrigar-se-á a fornecer à Parte requerente, nos mais breves prazos, os dados de tráfego suficientes para permitir a identificação do fornecedor de serviços no outro Estado e o caminho por ele utilizado para a transmissão da comunicação. No caso de a transmissão provir de um terceiro Estado, esta informação permitirá então à Parte requerente proceder à emissão de um requerimento de preservação e de um pedido de assistência mútua expedita, junto desse outro Estado, a fim de localizar a transmissão a partir da sua verdadeira origem. No caso de a comunicação ter sido reencaminhada através da Parte requerente, esta última poderá obter a preservação e divulgação de novos dados de tráfego por meio dos procedimentos internos aplicáveis.

291. Ao abrigo do disposto no parágrafo 2, a Parte requerida somente poderá recusar a divulgação dos dados de tráfego, nos casos em que tal seja susceptível de prejudicar a sua soberania, segurança, ordem pública ou outros interesses essenciais, ou nos casos em que considere tratar-se de uma infracção de natureza política ou uma infracção que, por sua vez, esteja relacionada com uma infracção de natureza política. Tal como para o Artigo 29º (Preservação expedita de dados informatizados armazenados), e dado que este tipo de informação é vital para a identificação dos autores dos crimes abrangidos pela presente Convenção ou para a localização de provas decisivas, os fundamentos de recusa deverão ser estritamente limitados, tendo sido estipulado que a adopção de qualquer outra base de recusa de assistência ficaria assim excluída.

Título 2 – Assistência mútua relativamente a poderes de investigação

Assistência mútua relativamente ao acesso a dados informatizados armazenados (Artigo 31º)

292. Cada Parte deverá dispor da capacidade de, em benefício de uma outra Parte, investigar ou, de forma semelhante, aceder, apreender ou, de forma semelhante, guardar e divulgar dados armazenados por meio de um sistema informático situado no seu território – tal como deverá, nos termos do Artigo 19º (Busca e apreensão de dados informatizados armazenados), dispor da capacidade de o fazer para fins de âmbito nacional. O parágrafo 1 autoriza as Partes a requererem este tipo de assistência mútua e o parágrafo 2 exige das Partes requeridas a respectiva capacidade de resposta. Além disso, o disposto no parágrafo 2 encontra-se em conformidade com o princípio segundo o qual os termos e condições de prestação da referida cooperação deverão ser os

definidos nos tratados, acordos e legislações nacionais aplicáveis à assistência jurídica mútua em questões penais. Ao abrigo do parágrafo 3, a resposta a um pedido de assistência mútua deverá ocorrer numa base expedita, sempre que (1) existam motivos para crer que os dados em causa sejam particularmente vulneráveis a perdas ou modificações, ou (2) os tratados, acordos ou legislações prescrevam uma cooperação expedita.

Acesso transfronteiriço a dados informatizados armazenados com autorização ou quando disponíveis ao público (Artigo 32º)

293. Os redactores da Convenção debateram longamente a questão de saber em que circunstâncias deverá ser permitido a uma Parte aceder unilateralmente aos dados informatizados, armazenados no território de uma outra Parte, sem requerer a assistência mútua. Foram examinadas em pormenor todas as situações nas quais se considera admissível que os Estados actuem de forma unilateral, bem como as situações nas quais tal não será aceitável. Os redactores chegaram, pois, à conclusão de que, nesta fase, não seria ainda possível elaborar um regime global, legalmente vinculatório, que regulamentasse esta matéria. Tal deve-se, em parte, à inexistência, até à data, de uma experiência objectiva relativamente a este tipo de situações, ao que se acrescenta o facto de se considerar que a resolução adequada está, frequentemente, ligada à conjuntura do caso em concreto, pelo que se torna difícil estipular regras gerais. Por fim, os redactores decidiram que apenas seriam definidas, ao abrigo do Artigo 32º da Convenção, as situações nas quais, por unanimidade, a acção unilateral se mostrasse aceitável. Deste modo, foi acordado que não serão regulamentadas outras situações em relação às quais não tenham sido ainda recolhidos novos dados que permitam ditar a experiência e prosseguir os debates sobre a questão. O parágrafo 3 do Artigo 39º determina, assim, que as restantes situações não serão nem autorizadas nem excluídas ao abrigo da presente Convenção.

294. O Artigo 32º (Acesso transfronteiriço a dados informatizados armazenados com autorização ou quando disponíveis ao público) trata duas situações: a primeira, quando os dados acedidos se encontram publicamente disponíveis e, segunda, quando a Parte acedeu a, ou recebeu, dados localizados fora do seu território através de um sistema informático situado no seu território, e obteve o consentimento legal e voluntário da pessoa autorizada, nos termos da lei, a proceder à divulgação dos dados junto da referida Parte e por meio do dito sistema. A questão de quem é a pessoa "legalmente autorizada" a divulgar os dados poderá variar em função das circunstâncias, da natureza jurídica da

pessoa e da respectiva legislação aplicável. Por exemplo, uma mensagem de correio electrónico de uma dada pessoa poderá ser armazenada num outro país por um fornecedor de serviços, ou a pessoa poderá intencionalmente armazenar os dados num outro país. Estas pessoas poderão, assim, recuperar os dados e, visto que dispõem de uma autoridade legal, proceder voluntariamente à divulgação dos dados junto dos serviços competentes para a aplicação da lei, ou permitir a estes últimos o acesso aos dados em conformidade com as disposições contidas neste Artigo.

Assistência mútua relativamente à recolha de dados de tráfego em tempo real (Artigo 33º)

295. Em muitos casos, os investigadores não estão certos de poder localizar a origem de uma comunicação ao seguirem as pistas fornecidas pelos registos de transmissões anteriores, uma vez que os dados de tráfego considerados cruciais poderão ter sido automaticamente eliminados por um fornecedor de serviços que esteja integrado na cadeia de transmissão, sem que tenha havido oportunidade para requerer a sua preservação. É, pois, vital para o trabalho desenvolvido pelos investigadores de cada Parte, a obtenção de dados de tráfego em tempo real, no que respeita a comunicações transmitidas por meio de sistemas informáticos situados no território de outra Parte. Assim, ao abrigo do disposto no Artigo 33º (Assistência mútua relativamente à recolha de dados de tráfego em tempo real), cada Parte obrigar-se-á a proceder à recolha de dados de tráfego em tempo real, a favor de uma outra Parte. O presente Artigo impõe às Partes a cooperação nesta matéria mas, tal como para outras disposições, deverão ser respeitadas as modalidades de assistência mútua em vigor, o que significa que as cláusulas e condições relativas à cooperação atrás mencionada são, geralmente, as que figuram nos tratados, acordos e legislações aplicáveis que regulamentam a assistência jurídica mútua em matéria penal.

296. Em muitos países, a assistência mútua é prestada, de uma maneira geral, no que se refere à recolha em tempo real de dados de tráfego, uma vez que uma tal recolha é vista como implicando uma menor intrusão do que a intercepção de dados de conteúdo, ou do que a operação de busca e apreensão. Contudo, vários são os Estados que adoptam uma abordagem mais restrita. Assim, da mesma forma que as Partes poderão formular uma reserva em conformidade com o parágrafo 3 do Artigo 14º (Âmbito das disposições processuais), no que diz respeito ao âmbito da medida nacional equivalente, as Partes são autorizadas, em virtude do parágrafo 2, a limitar o âmbito de aplicação desta medida a um conjunto mais estrito de infracções do que o previsto pelo Artigo 23º (Princípios gerais relativos à cooperação internacional).

Todavia, o parágrafo contém uma ressalva: sob nenhuma circunstância deverá o conjunto de infracções ser mais restrito do que o das infracções para as quais se poderá recorrer a esta medida num caso análogo a nível interno. De facto, como a recolha em tempo real de dados de tráfego é, por vezes, o único meio de identificar o autor de uma infracção e considerando que esta medida se reveste de um carácter menos intrusivo, a utilização da expressão "pelo menos" no parágrafo 2 visa incentivar as Partes a permitir a concessão de uma assistência tão alargada quanto possível, isto é, mesmo em caso de inexistência de criminalidade dupla.

Assistência mútua relativamente à intercepção de dados de conteúdo (Artigo 34º)

297. Devido ao elevado grau de intrusão inerente à intercepção, a obrigação de prestar assistência mútua, para efeitos de intercepção de dados de conteúdo, é limitada. A assistência deverá, pois, ser prestada na medida permitida pelos tratados e legislações aplicáveis das Partes. Visto que a cooperação para fins de intercepção de dados de conteúdo representa uma área emergente, e por isso ainda pouco explorada, no contexto da prática de assistência mútua, foi decidido remeter para os regimes e legislações nacionais em vigor em matéria de assistência mútua, o âmbito da obrigação de assistência e as limitações dessa mesma obrigação. Citamos, a este respeito, as observações relativas aos Artigos 14º, 15º e 21º, bem como a Recomendação Nº R (85) 10 relativa à aplicação prática da Convenção Europeia sobre Assistência Mútua em Matéria Penal no que se refere às cartas rogatórias para a intercepção de telecomunicações.

Título 3 – Rede 24/7

Rede 24/7 (Artigo 35º)

298. Tal como anteriormente mencionado, a eficácia da luta contra as infracções cometidas por meio de sistemas informáticos e a eficácia da recolha de provas sob a forma electrónica estará directamente relacionada com a rapidez de intervenção. Além do mais, bastará premir-se algumas teclas em qualquer parte do mundo para que, instantaneamente, se produzam efeitos a milhares de quilómetros de distância. Por esse motivo, as modalidades de assistência mútua e cooperação policial existentes requerem vias suplementares para fazer face ao desafio colocado pela era informática. A via instituída pelo presente Artigo baseia-se na experiência adquirida através de uma rede já implantada e que foi criada sob os auspícios do grupo dos países mais industrializados, o

G8. Em virtude deste Artigo, cada Parte ficará obrigada a designar um ponto de contacto que esteja disponível 24 horas por dia, 7 dias por semana, a fim de assegurar uma assistência imediata ao nível das investigações e dos processos penais levados a cabo em conformidade com o domínio de aplicação do presente Capítulo, nomeadamente tal como definido no Artigo 35º, parágrafo 1, alíneas a) – c). Foi considerado que a constituição da referida rede se conta entre os meios mais importantes, previstos pela presente Convenção, de garantir que as Partes dispõem da capacidade necessária para responder eficazmente aos desafios colocados, ao nível da aplicação da lei, pela criminalidade informática e pelos crimes relacionados com computadores.

299. Ao ponto de contacto 24/7 de cada Parte caberá quer a viabilização quer a aplicação directa de um determinado número de medidas tais como, inter alia, a prestação de aconselhamento técnico, a preservação de dados, a recolha de provas, o fornecimento de informação de natureza jurídica e a localização de suspeitos. Pela expressão "informação de natureza jurídica" que figura no parágrafo 1, deverá entender-se os pareceres dados, a uma outra Parte que apresente um pedido de assistência mútua, no que concerne a todos os pré-requisitos exigidos nos termos da lei relativamente a uma cooperação formal ou informal.

300. Cada Parte dispõe de uma total liberdade para determinar qual o posicionamento do ponto de contacto, no seio da estrutura dos seus serviços competentes para a aplicação da lei. Algumas Partes poderão desejar englobar o ponto de contacto 24/7 no seio da sua autoridade central para fins de assistência mútua, enquanto outras poderão julgar mais conveniente posicioná-lo junto de uma unidade policial especializada no combate ao crime informático ou relacionado com computadores, embora possam surgir outras opções intimamente ligadas à estrutura governamental e ao sistema jurídico de uma Parte. Uma vez que o ponto de contacto 24/7 tem a seu cargo, simultaneamente, a prestação de aconselhamento técnico para pôr termo a uma invasão ou detectar a origem da mesma e o desempenho de tarefas associadas à cooperação internacional, tal como a localização de suspeitos, não existe apenas uma única solução adequada e é de prever que a estrutura da rede evolua ao longo do tempo. Aquando da nomeação do ponto de contacto nacional, deverá ser dada a devida atenção à necessidade de comunicação com pontos de contacto estrangeiros e que, portanto, utilizem outras línguas.

301. O parágrafo 2 determina que, de entre as funções principais a serem desempenhadas pelo ponto de contacto 24/7, destaca-se a capacidade para viabilizar a execução rápida das tarefas que não são levadas a cabo por si

directamente. Por exemplo, se o ponto de contacto 24/7 de uma Parte estiver integrado numa unidade policial, deverá dispor dos meios necessários a uma coordenação expedita das suas acções com as de outros serviços competentes no seio do governo, tais como a autoridade central responsável pela extradição ou assistência mútua no plano internacional, a fim de permitir que as medidas que se impõem possam ser tomadas a qualquer momento, independentemente da hora do dia ou da noite. O parágrafo 2 exige ainda que o ponto de contacto 24/7 de cada Parte esteja habilitado a realizar, de forma célere, as necessárias comunicações com outros membros da rede.

302. O parágrafo 3 determina que cada ponto de contacto da rede deverá encontrar-se munido do equipamento apropriado. Assim, para um funcionamento correcto da rede, será essencial dispor de telefones, faxes e computadores actualizados, sendo que, a par com os avanços tecnológicos, deverão ser introduzidos no sistema outros materiais de comunicação e análise. O parágrafo 3 exige igualmente que o pessoal que integra a equipa de cada uma das Partes, no seio da rede, disponha da devida formação na área da criminalidade informática a fim de poder responder eficazmente.

Capítulo IV – Disposições Finais

303. Com algumas excepções, as disposições contidas no presente Capítulo baseiam-se essencialmente nas "Cláusulas finais tipo para as convenções e acordos celebrados no quadro do Conselho da Europa", as quais foram aprovadas pelo Comité de Ministros na 315ª assembleia dos Delegados, realizada em Fevereiro de 1980. Dado que, na sua maioria, os artigos 36º a 48º se remetem ao texto das cláusulas-tipo ou são inspirados na longa prática de elaboração de Convenções do Conselho da Europa, não suscitam comentários específicos. Todavia, certas modificações às cláusulas-tipo ou algumas novas disposições deverão ser objecto de uma explicação. A este respeito, salientamos o facto de as cláusulas-tipo terem sido adoptadas como um conjunto de disposições de carácter não vinculatório. Tal como indicado na Introdução às Cláusulas-Tipo, "as presentes cláusulas finais tipo destinam-se apenas a facilitar o papel desempenhado pelos comités de especialistas e a evitar divergências textuais que não teriam uma real justificação. As cláusulas-tipo não são, de forma alguma, vinculatórias podendo adaptar-se cláusulas diferentes a situações particulares."

Assinatura e entrada em vigor (Artigo 36º)

304. O parágrafo 1 do Artigo 36º foi redigido tendo em consideração vários precedentes definidos noutras convenções elaboradas no âmbito do Conselho

da Europa, como por exemplo, na Convenção relativa à Transferência de Pessoas Condenadas (STE nº 112) e na Convenção relativa ao Branqueamento, Detecção, Apreensão e Confisco dos Produtos do Crime (STE nº 141), as quais podem ser assinadas, antes da sua entrada em vigor, não apenas pelos Estados-membros do Conselho da Europa mas também pelos Estados não membros que tenham participado na sua elaboração. Esta cláusula destina-se a permitir ao maior número de países interessados, e não somente aos membros do Conselho da Europa, tornarem-se Partes contratantes das convenções, com a maior brevidade possível. Neste caso específico, esta cláusula aplica-se a quatro Estados não membros, a saber, o Canadá, o Japão, a África do Sul e os Estados Unidos da América, os quais participaram activamente na elaboração da Convenção. Após a sua entrada em vigor, em conformidade com o disposto no parágrafo 3, poderão ser convidados a aderir à Convenção outros estados não membros, aos quais esta disposição não é aplicável, de acordo com o prescrito pelo parágrafo 1 do Artigo 37º.

305. O parágrafo 3 do Artigo 36º determina que serão 5 as ratificações, aceitações ou aprovações exigidas para que a Convenção possa entrar em vigor. Sendo superior ao limite habitualmente fixado pelos tratados do Conselho da Europa, este número traduz a convicção de que é necessário um número ligeiramente mais elevado de Estados, de modo a ser possível enfrentar, com êxito, o desafio colocado pela criminalidade informática ou relacionada com computadores, a nível internacional. Contudo, o número é suficientemente baixo para que a entrada em vigor da Convenção não seja desnecessariamente adiada. De entre os cincos Estados iniciais, três deverão obrigatoriamente ser membros do Conselho da Europa, podendo os restantes dois fazer parte dos quatro Estados não membros que participaram na elaboração da Convenção. Como é natural, esta cláusula permite igualmente a entrada em vigor da Convenção a partir do momento em que cinco Estados-membros do Conselho da Europa expressem o seu consentimento no sentido de ficarem vinculados à referida Convenção.

Adesão à Convenção (Artigo 37º)

306. O Artigo 37º foi igualmente redigido com base nos precedentes que figuram noutras convenções do Conselho da Europa, mas inclui um elemento adicional. Em consonância com a sua longa prática, o Comité de Ministros decide, por sua iniciativa própria ou mediante solicitação, convidar um Estado não membro que não tenha participado na elaboração de uma Convenção, a aderir à mesma após ter consultado todas as Partes contratantes, quer sejam

estas Estados-membros ou não. Por outras palavras, isto implica que, caso uma das Partes contratantes se oponha à adesão do Estado não membro, o Comité de Ministros não prosseguirá com o referido convite de adesão à Convenção. Todavia, ao abrigo da formulação habitual, o Comité de Ministro poderá – em princípio – convidar o Estado não membro a aderir a uma convenção mesmo que uma Parte (um Estado não membro) levante objecções à sua adesão. Tal significa que – em teoria – não é conferido, normalmente, qualquer direito de veto aos Estados Partes, não membros, no que toca ao processo de alargamento dos tratados do Conselho da Europa a outros Estados não membros. Contudo, foi expressamente introduzido o requisito segundo o qual o Comité de Ministros deverá consultar e obter a aprovação unânime de todas as Partes Contratantes – não apenas a dos membros do Conselho da Europa – antes de convidar um Estado não membro a aderir à Convenção. Tal como referido acima, este requisito é coerente com a prática estabelecida e reconhece que todas as Partes contratantes da Convenção deverão ser livres de decidir quais os Estados não membros com que irão manter as relações decorrentes dos tratados celebrados. Não obstante esse facto, a decisão formal de convidar um Estado não membro a aderir, será tomada, em conformidade com a prática instituída, pelos representantes das Partes contratantes com direito de voto no seio do Comité de Ministros. A referida decisão exige uma maioria de dois terços, tal como previsto pelo Artigo 20, alínea d., dos Estatutos do Conselho da Europa, e a unanimidade dos votos dos representantes das Partes contratantes que tenham sido nomeados nessa qualidade para deliberar no seio do Comité de Ministros.

307. Os Estados Federais que desejem aderir à Convenção e que tencionem apresentar uma declaração em conformidade com o disposto no Artigo 41º, deverão entregar previamente uma minuta do texto da declaração a que se refere o parágrafo 3 do Artigo 41º, de modo a que as Partes estejam em posição de avaliar em que medida a aplicação da cláusula federal, por uma potencial Parte contratante, poderia afectar a implementação da Convenção (consultar o parágrafo 320º).

Efeitos da Convenção (Artigo 39º)

308. Os parágrafos 1 e 2 do Artigo 39º abordam o tema da relação entre a Convenção e outros tratados ou acordos internacionais existentes. As cláusulas-tipo supracitadas não abrangem as relações entre as convenções do Conselho da Europa, nem as relações entre estas e outros tratados, bilaterais ou multilaterais, celebrados fora do Conselho da Europa. A abordagem

habitualmente utilizada nas Convenções do Conselho da Europa no domínio do direito penal (por exemplo, no Acordo relativo ao Tráfico Ilegal por Via Marítima (STE nº 156)) é a seguinte: (1) as novas convenções não afectam os direitos e as obrigações decorrentes das convenções multilaterais, já existentes a nível internacional, relativamente a questões especiais; (2) as Partes contratantes de uma nova convenção poderão celebrar, entre si, acordos bilaterais ou multilaterais, relativamente às questões contempladas pela Convenção, com a finalidade de complementar e reforçar as suas disposições ou de facilitar a aplicação dos princípios nela contidos; e (3) no caso de uma ou mais Partes terem já celebrado um acordo ou tratado relativamente a uma questão abrangida pela Convenção ou, se de algum outro modo, tiverem já estabelecido as suas relações quanto a essa questão, as Partes poderão aplicar o referido acordo ou tratado ou reger as suas relações em conformidade com o mesmo, alternativamente à presente Convenção, desde que tal contribua para facilitar a cooperação internacional.

309. Na medida em que, de um modo geral, a Convenção visa completar e não substituir os tratados e acordos, bilaterais e multilaterais, celebrados entre as Partes, os autores consideraram que a menção, eventualmente redutora, a "questões especiais" não se revelava particularmente instrutiva e que poderia gerar alguma confusão. Esse é o motivo pelo qual, o parágrafo 1 do Artigo 39º se limita a indicar que a presente Convenção tem por objectivo complementar outros acordos ou tratados bilaterais ou multilaterais aplicáveis, tal como celebrados entre as Partes. Assim, em vez de se apresentar uma lista exaustiva, são citados os exemplos de três tratados do Conselho da Europa, em particular: a Convenção Europeia de Extradição datada de 1957 (STE nº 24), a Convenção Europeia sobre Assistência Mútua em Matéria Penal, de 1959 (STE nº 30) e o seu respectivo Protocolo Adicional, datado de 1978 (STE nº 99). Consequentemente, no que respeita às questões de âmbito geral, tais acordos ou tratados deverão, em princípio, ser aplicados pelas Partes contratantes da Convenção sobre o Cibercrime. No que diz respeito às questões de âmbito mais específico que somente se encontrem regulamentadas pela Convenção, a regra de interpretação lex specialis derogat legi generali impõe que as Partes atribuam a prioridade às regras contidas na presente Convenção. O Artigo 30º constitui disso um exemplo, ao estabelecer a divulgação expedita dos dados de tráfego preservados, sempre que se mostre necessário identificar o caminho através do qual foi transmitida uma determinada comunicação. Nesta área específica, a Convenção, enquanto lex specialis, deverá definir uma regra de primeira instância relativamente às disposições que figuram nos acordos de assistência mútua de carácter mais geral.

310. Do mesmo modo, os redactores entenderam que uma formulação linguística que condicionasse a aplicação de acordos vigentes ou futuros ao facto de os mesmos "reforçarem" ou "facilitarem" a cooperação, poderia ser problemática na medida em que, segundo a abordagem adoptada no capítulo dedicado à cooperação internacional, se presume que as Partes irão aplicar os respectivos tratados e acordos internacionais.

311. Perante a existência de um tratado ou acordo de assistência mútua que sirva de base para a cooperação, a presente Convenção apenas complementará, quando tal se afigure necessário, as disposições existentes. Assim, por exemplo, a presente Convenção estipula que se proceda à transmissão dos pedidos de assistência mútua através de meios de comunicação expeditos (consultar o parágrafo 3 do Artigo 25º) caso tal possibilidade não se encontre contemplada ao abrigo do tratado ou acordo inicial.

312. Em consonância com a natureza supletiva da Convenção e, em especial, com a sua abordagem sobre a cooperação internacional, o parágrafo 2 prevê que as Partes são igualmente livres de aplicar os acordos vigentes, bem como aqueles que possam futuramente entrar em vigor. Esta disposição tem como precedente a Convenção relativa à Transferência de Pessoas Condenadas (STE nº 112). Sem dúvida que, no contexto da cooperação internacional, se espera que a aplicação de outros acordos internacionais (muitos dos quais proporcionam soluções largamente comprovadas no domínio da prestação de assistência mútua internacional) contribua efectivamente para promover e incentivar a cooperação. Em conformidade com as disposições da presente Convenção, as Partes poderão ainda decidir a aplicação das suas cláusulas relativas à cooperação internacional, em vez da aplicação do disposto nos outros acordos atrás mencionados (consultar o Artigo 27(1)). Nesse caso, as disposições relativas à cooperação, enunciadas no Artigo 27º, prevalecerão sobre as normas aplicáveis constantes dos referidos acordos. Visto que a Convenção prevê, em geral, a existência de obrigações mínimas, o parágrafo 2 do Artigo 39º reconhece às Partes a liberdade de assumirem as obrigações que se revestem de uma maior especificidade, adicionalmente às obrigações já definidas pela Convenção, sempre que se trate de estabelecer as suas relações no que toca a questões abrangidas pela Convenção. Todavia, tal não representa um direito absoluto: as Partes deverão respeitar os objectivos e os princípios da Convenção, pelo que não poderão assumir obrigações que se revelem contrárias ou incompatíveis com os fins da presente Convenção.

313. Os redactores concluíram ainda que, no que se refere à determinação das relações entre a Convenção e outros acordos internacionais, as Partes poderão

também inspirar-se nas respectivas disposições constantes da Convenção de Viena sobre o Direito dos Tratados.

314. A Convenção consagra os seus esforços à tentativa de responder à necessidade de harmonização que actualmente impera, sem no entanto pretender regulamentar todas as questões inerentes à criminalidade informática ou relacionada com computadores. Assim, foram introduzidas as disposições do parágrafo 3 a fim de tornar claro que a Convenção apenas abrange ou afecta aquilo que nela é tratado. Permanecerão pois, inalterados todos os outros direitos, restrições, obrigações e responsabilidades, eventualmente existentes mas que não sejam tratados pela presente Convenção. Poderemos encontrar os precedentes de uma tal "cláusula de salvaguarda" no contexto de outros acordos internacionais como, por exemplo, a Convenção das Nações Unidas sobre a luta contra o financiamento do terrorismo.

Declarações (Artigo 40º)

315. O Artigo 40º faz referência a certos artigos que dizem, essencialmente, respeito às infracções definidas pela Convenção na secção relativa ao direito substantivo e, em virtude dos quais, as Partes são autorizadas a introduzir determinados elementos adicionais especificados, que são susceptíveis de modificar o âmbito de aplicação das ditas disposições. Os referidos elementos adicionais visam tomar em consideração certas diferenças teóricas ou jurídicas que, num tratado de âmbito mundial, são talvez mais justificáveis do que simplesmente no contexto do Conselho da Europa. As declarações são entendidas como sendo interpretações aceitáveis das disposições da Convenção e deverão distinguir-se das reservas, as quais permitem que as Partes excluam ou modifiquem os efeitos jurídicos de certas obrigações definidas pela Convenção. Uma vez que, para as Partes contratantes da Convenção, é importante tomar conhecimento de quaisquer elementos adicionais que possam ter sido introduzidos pelas outras Partes, foi estipulada a obrigação de comunicar os ditos elementos ao Secretário Geral do Conselho da Europa, no acto da assinatura ou aquando do depósito dos instrumentos de ratificação, aceitação, aprovação ou adesão. Esta notificação é especialmente importante no que se refere à definição das infracções, uma vez que, para exercerem determinados poderes processuais, as Partes deverão ter preenchido o requisito da dupla criminalidade. Não se julgou necessário estabelecer um número limite relativamente às declarações.

Cláusula Federal (Artigo 41º)

316. Em consonância com o objectivo de permitir que o maior número possível de Estados possa adquirir a qualidade de Parte contratante, o Artigo 41º prevê um tipo especial de declaração que tem por finalidade responder às dificuldades que os Estados federais poderão enfrentar, em resultado da sua típica divisão de poderes entre as autoridades federais e regionais. Fora do domínio do direito penal, existem precedentes para as declarações ou reservas federais relativamente a outros acordos internacionais[11]. Neste contexto, o Artigo 41º constata que poderão existir variações menores de aplicação, em consequência da legislação e da prática interna, bem estabelecida, de uma Parte que seja um Estado federal. As referidas variações deverão ter por base a sua Constituição ou outros princípios fundamentais relativamente à divisão dos poderes, em matéria de justiça penal, entre o governo central e os Estados constituintes ou outras entidades territoriais de um Estado federal. Foi, pois, considerado pelos autores da Convenção que a aplicação da cláusula federal apenas implicaria variações pouco significativas na implementação da Convenção.

317. Tomemos o exemplo dos Estados Unidos: segundo a sua Constituição e ao abrigo dos princípios fundamentais do federalismo, é a legislação penal federal que geralmente é aplicada se os actos em questão produzirem efeitos sobre o comércio entre os Estados constituintes ou entre estes e o estrangeiro, enquanto que os casos de menor importância ou de interesse meramente local são, em geral, do foro dos Estados constituintes. Esta abordagem do federalismo permite ainda que a legislação penal federal dos EUA abranja, em larga medida, os actos ilícitos previstos pela presente Convenção, mas reconhece que continuarão a ser da competência dos Estados constituintes todos e quaisquer actos de menor impacto ou de carácter puramente local. Em certos casos, englobados nesta categoria restrita de actos regulamentados pelo Estado constituinte e não pela legislação federal, um Estado constituinte não poderá instituir uma medida que normalmente pertença ao campo de aplicação da Convenção. Assim, por exemplo, uma invasão do sistema de um computador pessoal autónomo ou de uma rede de computadores interligados no seio de um mesmo edifício, apenas será do foro penal se a lei do Estado, no qual se deu a ocorrência, assim

11. Por exemplo, a Convenção relativa ao Estatuto dos Refugiados, de 28 de Julho de 1951, Art. 34º; a Convenção relativa ao Estatuto dos Apátridas, de 28 de Setembro de 1954, Art. 37º; a Convenção sobre o Reconhecimento e a Execução de Sentenças Arbitrais Estrangeiras, de 10 de Junho de 1958, Art. 11º; e a Convenção Internacional sobre a Protecção da Herança Cultural e Natural da Humanidade, de 16 de Novembro de 1972, Art. 34º.

o determinar. Por outro lado, caso o acesso ao computador ocorresse através da Internet, a referida invasão seria considerada uma infracção, ao abrigo da lei federal, uma vez que a utilização da Internet produz efeitos sobre o comércio entre os Estados constituintes ou entre estes e o estrangeiro, sendo esta uma condição necessária à aplicação da legislação federal. A implementação da presente Convenção, por meio da legislação federal dos Estados Unidos ou da lei de outros Estados federais que se encontrem sob circunstâncias similares, far-se-á em conformidade com as disposições constantes do Artigo 41º.

318. O campo de aplicação da cláusula federal foi limitado às disposições contidas no Capítulo II (direito penal substantivo, direito processual e jurisdição). Os Estados federais que façam uso desta disposição, não se verão desvinculados da obrigação de cooperar com as outras Partes, em virtude do prescrito pelo Capítulo III, devendo tal aplicar-se mesmo nos casos em que um Estado constituinte ou uma outra entidade territorial análoga, no qual esteja situado um fugitivo ou uma prova, não penalize tal conduta ou não disponha de procedimentos em conformidade com a Convenção.

319. No que diz respeito às disposições cuja aplicação seja da competência legislativa dos Estados constituintes ou de outras entidades territoriais análogas, o governo federal deverá remeter as ditas disposições às autoridades de tais entidades, juntamente com o seu parecer favorável (Artigo 41º, parágrafo 2). Um Estado federal que apresente uma declaração em virtude do disposto no parágrafo 1 do Artigo 41º, deverá fornecer indicações suficientemente precisas, por forma a que as outras Partes possam avaliar o efeito potencial da aplicação da cláusula federal sobre a implementação das disposições da Convenção.

Reservas (Artigo 42º)

320. O Artigo 42º prevê um conjunto de situações nas quais é possível formular uma reserva. Esta abordagem deriva do facto de a Convenção cobrir uma área do direito penal e do direito processual penal que se afigura como sendo relativamente nova para muitos Estados. Além disso, a vocação mundial da Convenção, a qual será aberta a Estados-membros e Estados não membros do Conselho da Europa, faz com que seja necessário prever tais possibilidades de reservas. Estas têm como objectivo permitir que o maior número possível de Estados possa tornar-se uma Parte contratante da Convenção, conferindo a tais Estados a possibilidade de conservar determinadas abordagens e seguir conceitos que se mostrem compatíveis com a sua legislação nacional. Ao mesmo tempo, os redactores procuraram limitar as possibilidades de formulação de

reservas a fim de garantir, tanto quanto possível, a uniformidade na aplicação da Convenção pelas Partes. Assim sendo, as Partes não poderão formular outras reservas para além das enunciadas na Convenção, devendo fazê-lo apenas no acto da assinatura ou aquando do depósito dos seus instrumentos de ratificação, aceitação, aprovação ou adesão.

321. Com base no pressuposto de que, para algumas Partes, certas reservas seriam essenciais para evitar o conflito com os seus princípios constitucionais ou princípios jurídicos fundamentais, o Artigo 43º não impõe um período limite específico para a revogação das reservas, apenas ditando que as mesmas deverão ser retiradas logo que as circunstâncias o permitam.

322. A fim de poder exercer alguma pressão sobre as Partes para que estas, pelo menos, ponderem a revogação das suas reservas, a Convenção autoriza o Secretário Geral do Conselho da Europa a, periodicamente, inquirir as Partes relativamente às perspectivas de revogação das reservas formuladas. Esta possibilidade de inquirir as Partes constitui uma prática corrente no quadro de diversos instrumentos do Conselho da Europa. As Partes poderão, assim, indicar as reservas que, do seu ponto de vista, se impõe que sejam mantidas relativamente a determinadas disposições, bem como 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 da Convenção.

Modificações (Artigo 44º)

323. O Artigo 44º tem como precedente a Convenção relativa ao Branqueamento, Detecção, Apreensão e Confisco dos Produtos do Crime (STE nº 141), na qual esta disposição foi inserida como uma inovação, ao nível das convenções de direito penal elaboradas no quadro do Conselho da Europa. Considera-se que o processo de modificação é, essencialmente, aplicável a alterações pouco significativas de carácter técnico e processual. Assim, os redactores entenderam que as alterações verdadeiramente importantes deverão ser introduzidas na Convenção sob a forma de protocolos adicionais.

324. As Partes poderão, por si próprias, estudar a necessidade da introdução de modificações ou da elaboração de protocolos, mediante a aplicação do processo de consulta definido no Artigo 46º. O Comité Europeu para os Problemas Criminais (CDPC) deverá, com regularidade, ser mantido informado a este respeito, bem como tomar as medidas que se afigurem necessárias a

fim de apoiar as Partes, em termos dos esforços por estas desenvolvidos no sentido de modificar e complementar a Convenção.

325. De acordo com o parágrafo 5, toda e qualquer modificação adoptada somente deverá entrar em vigor após todas as Partes terem comunicado ao Secretário Geral a sua aceitação. Esta disposição visa garantir que a Convenção irá evoluir de uma maneira uniforme.

Resolução de litígios (Artigo 45º)

326. O parágrafo 1 do Artigo 45º determina que o Comité Europeu para os Problemas Criminais (CDPC) deverá ser mantido informado acerca da interpretação e aplicação das disposições que figuram na Convenção. O parágrafo 2 impõe às Partes a obrigação de procurar a resolução pacífica de quaisquer conflitos advenientes da interpretação ou da aplicação da presente Convenção. Todo e qualquer procedimento de resolução de litígios utilizado deverá ser alvo de acordo entre as Partes envolvidas. A presente disposição sugere três mecanismos possíveis para a resolução de litígios: o próprio Comité Europeu para os Problemas Criminais (CDPC), um tribunal arbitral ou o Tribunal Internacional de Justiça.

Processo de Consulta das Partes (Artigo 46º)

327. O Artigo 46º define a criação de 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 electrónica, bem como à possibilidade de complemento e modificação da Convenção. As consultas deverão analisar, nomeadamente, as questões decorrentes da utilização e implementação da Convenção, entre as quais se contam os efeitos das declarações e das reservas apresentadas em conformidade com os Artigos 40, [41] e 42.

328. O processo caracteriza-se pela sua flexibilidade, na medida em que caberá às Partes a decisão sobre a forma e o momento de se reunirem, se assim o desejarem. Os redactores consideraram que este processo será útil no sentido de assegurar que todas as Partes na Convenção, incluindo os Estados não membros do Conselho da Europa, possam participar – numa base de igualdade – em quaisquer mecanismos de seguimento, ao mesmo tempo que são preservadas as competências do Comité Europeu para os Problemas

Criminais (CDPC). Este último, deverá ser regularmente informado acerca das consultas realizadas entre as Partes, bem como, agir de forma a facilitar tais consultas e tomar as medidas necessárias para apoiar as Partes no âmbito dos seus esforços para complementar e modificar a presente Convenção. Tendo em conta as necessidades de uma prevenção e de uma penalização eficazes da cibercriminalidade, e atendendo também às questões associadas aos aspectos da vida privada, ao potencial impacto nas actividades comerciais e a outros factores relevantes, poderão ser de alguma utilidade para estas consultas os contributos dados pelas partes interessadas, nomeadamente, as autoridades competentes para a aplicação da lei, organizações não governamentais e instituições do sector privado (consultar igualmente o parágrafo 14).

329. O parágrafo 3 prevê uma revisão do funcionamento da Convenção, após decorrido um prazo de três anos a contar da data da sua entrada em vigor, podendo então ser recomendadas as modificações que se revelem apropriadas. O CDPC deverá levar a cabo esta revisão, contando para esse efeito com a ajuda das Partes.

330. O parágrafo 4 prevê que, salvo nos casos em que sejam suportados pelo Conselho da Europa, deverão ser da responsabilidade das Partes quaisquer encargos inerentes ao financiamento das consultas realizadas em conformidade com o disposto no parágrafo 1 do Artigo 46º. Todavia, para além do Comité Europeu para os Problemas Criminais (CDPC), também o Secretariado do Conselho da Europa deverá apoiar as Partes no quadro das suas actividades desenvolvidas ao abrigo da presente Convenção.

Primeiro protocolo adicional relativo à incriminação de actos de natureza racista e xenófoba praticados através de sistemas informáticos (STE No. 189), Estrasburgo, 28 de Janeiro de 2003

Os Estados-Membros do Conselho da Europa e os outros Estados Partes na Convenção sobre o Cibercrime, aberta à assinatura em Budapeste, a 23 de Novembro de 2001, signatários do presente Protocolo;

Considerando que objectivo do Conselho da Europa é o de realizar uma união mais estreita entre os seus membros;

Relembrando que todas as pessoas nascem livres e iguais em dignidade e direitos;

Realçando a necessidade de garantir uma integral e eficaz implementação de todos os direitos humanos sem discriminação ou distinção, conforme consignado nos instrumentos europeus e internacionais;

Convictos de que os actos de natureza racista e xenófoba constituem uma violação dos direitos humanos e uma ameaça ao Estodo de Direito e à estabilidade democrática;

Considerando que os ordenamentos jurídicos nacionais e o direito internacional devem dispor de respostas jurídicas adequadas à propaganda de natureza racista e xenófoba através de sistemas informáticos;

Conscientes de que a difusão de tais actos é, frequentemente, objecto de incriminação nos ordenamentos jurídicos nacionais;

Considerando a Convenção sobre o Cibercrime, na qual se prevêem meios modernos e flexíveis de cooperação internacional e convictos da necessidade de harmonizar as disposições do direito substantivo relativas à luta contra a propaganda de natureza racista e xenófoba;

Conscientes de que os sistema informáticos oferecem meios sem precedentes de liberdade de expressão e comunicação a nível planetário;

Reconhecendo que a liberdade de expressão constitui um dos pilares essenciais da sociedade democrática, sendo uma das condições fundamentais para o seu progresso e para o desenvolvimento do ser humano;

Preocupados, contudo, com o risco de uso indevido ou de abuso de tais sistemas informáticos para efeitos de difusão de propaganda de natureza racista e xenófoba;

Tendo presente a necessidade de garantir um equilíbrio adequado entre a liberdade de expressão e a luta eficaz contra actos de natureza racista e xenófoba;

Reconhecendo que o presente Protocolo não pretende colidir com os princípios consagrados nos ordenamentos jurídicos nacionais a propósito da liberdade de expressão;

Tendo em conta os instrumentos jurídicos internacionais relevantes nesta matéria, nomeadamente a Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais e o seu Protocolo n.º 12 relativo à interdição geral de discriminação, bem como as Convenções do Conselho da Europa sobe cooperação em matéria penal, nomeadamente a Convenção sobre o Cibercrime, a Convenção Internacional das Nações Unidas sobre a Eliminação de Todas as Formas de Discriminação Racial, assinada a 21 de Dezembro de 1965 , a Acção Comum da União Europeia, de 15 de Julho de 1996, adoptada pelo Conselho com base no Artigo K.3 do Tratado da União Europeia e relativa à acção a tomar para combater o racismo e a xenofobia;

Congratulande-se com os recentes desenvolvimentos destinados a aprofundar o entendimento e a cooperação internacionais com vista ao combate do racismo e da xenofobia;

Tendo em consideração o Plano de Acção adoptado pelos Chefes de Estado e de Governo do Conselho da Europa por ocasião da sua Segunda Cimeira (Estrasburgo, 10-11 de Outubro de 1997), visando obter respostas comuns face ao desenvolvimento das novas tecnologias de informação baseadas nas normas e nos valores do Conselho da Europa;

Acordaram no seguinte:

Capítulo I – Disposições comuns

Artigo 1° – Objectivo

O objectivo do presente Protocolo é a complementaridade, pelas Partes no presente Protocolo, das disposições constantes da Convenção sobre o Cibercrime, aberta à assinatura em Budapeste, a 23 de Novembro de 2001, (adiante denominada "a Convenção") relativamente à incriminação de actos de natureza racista e xenófoba praticados através de sistemas informáticos.

Artigo 2° – Definição

1. Para os fins do presente Protocolo, a expressão:

"*material racista e xenófobo*" designa qualquer material escrito, imagem ou outra representação de ideias e teorias que preconize ou encoraje o ódio, a discriminação ou a violência contra qualquer pessoa ou grupo de pessoas, em função da sua raça, cor, ascendência ou origem nacional ou étnica, ou ainda da sua religião na medida em que esta sirva de pretexto a qualquer um dos outros elementos ou incite à prática de tais actos.

2. As expressões e os termos utilizados do presente Protocolo serão interpretados da mesma maneira que os utilizados na Convenção.

Capítulo II – Medidas a tomar a nível nacional

Artigo 3° – Difusão de material racista e xenófobo através de sistemas informáticos

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para tipificar, no seu direito interno, comi infracções penais, quando cometidas de forma intencional, as seguintes condutas:

A difusão ou outras formas de colocação à disposição do público, através de um sistema informático, de material racista e xenófobo.

2. As Partes poderão reserva-se o direito de não incriminar as condutas previstas no n.° 1 do presente artigo sempre que o material, conforme definido no n.° 1 do artigo 2°, preconize, promova ou incite à discriminação não associada a ódio ou violência e desde que cobertos por outros mecanismos eficazes.

3. Não obstante o disposto no n.° 2 do presente artigo, as Partes poderão reservar-se o direito de não aplicar o disposto no n.° 1 supra aos casos de discriminação relativamente aos quais não possam prever as sanções eficazes previstas no n.° 2, por força dos princípios consagrados nos respectivos ordenamentos jurídicos no tocante à liberdade de expressão.

Artigo 4° – Ameaça com motivação racista e xenófoba

Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para tipificar, no seu direito interno, como infracção penal, quando praticada intencional e ilegitimamente, a seguinte conduta:

Ameaça, através de um sistema informático, de cometer um crime grave confrme definido pelo ordenamento jurídico interno contra (i) uma pessoa por pertencer a um grupo que se caracterize pela sua raça, cor, ascendência ou origem nacional ou étnica, ou, ainda, pela sua religião, na medida em que esta sirva de pretexto a qualquer um dos outros elementos; (ii) um grupo de pessoas que se distinga por qualquer uma das referidas características.

Artigo 5° – Insulto com motivação racista e xenófoba

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para tipificar, no seu direito interno, como infracção penal, quando praticada intencional e ilegitimamente, a seguinte conduta:

Insulto público, através de um sistema informático, (i) dirigido a uma pessoa por pertencer a um grupo que se caracterize pela sua raça, cor, ascendência ou origem nacional ou étnica, ou, ainda pela sua religião, na medida em que esta sirva de pretexto a qualquer um dos outros elementos ; (ii) dirigido a um grupo de pessoas que se distinga por qualquer uma das referidas características.

2. As Partes poderão:

a. Exigir que a infracção prevista no n.° 1 do presente artigo vise expor a pessoa ou o grupo de pessoas aí referidas ao ódio, ao desprezo ou ao ridículo ; ou

b. Reservar-se o direito de não aplicar, no todo ou em parte, o disposto no n.° 1 do presente artigo.

Artigo 6° – Negação, minimização grosseira, aprovação ou justificação do genocídio ou dos crimes contra a humanidade

1. Cada Parte adoptará as medidas legislativas o outras que se revelem necessárias para tipificar, no seu direito interno, como infracções penais, quando praticadas intencional e ilegitimamente, as seguintes condutas:

a difusão ou outras formas de colocação à disposição do público, através de um sistema informático, de material que negue, minimize de forma grosseira, aprove ou justifique actos constitutivos de genocídio ou de crimes contra a humanidade, conforme definidos pelo direito internacional e reconhecidos como tal por uma decisão definitiva emanada do Tribunal Militar Internacional estabelecido pelo Acordo de Londres, de 8 de Agosto de 1945, ou de qualquer outro tribunal internacional estabelecido por instrumentos internacionais pertinentes e cuja competência tenha sido reconhecida pela Parte interessada.

2. As Partes poderão:

a. Prever que a negação ou a minimização grosseira, conforme prevista no n.° 1 do presente artigo, seja praticada com a intenção de incitar ao ódio, à discriminação ou a violência contra uma pessoa ou um grupo de possoas em função da sua raça, cor, ascendência ou origem nacional ou étnica ou, ainda, da sua religião, na medida em que esta sirva como pretexto a qualquer um dos outros elementos ; ou

b. Reservar-se o direito de não aplicar, no todo ou em parte, o disposto no n.° 1 do presente artigo.

Artigo 7° – Auxílio e cumplicidade

Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para tipificar, no seu direito interno, como infracção penal, quando praticado intencional e ilegitimamente, o acto de auxiliar na prática de um crime conforme definido no presente Protocolo, ou de agir como cúmplice em tal prática, visando a prática efectiva de tal infracção.

Capítulo III – Relações entre a Convenção e o Protocolo

Artigo 8° – Relações entre a Convenção e o presente Protocolo

1. Os artigos 1°, 12°, 13°, 22°, 41°, 44°, 45°, e 46° da Convenção serão correspondentemente aplicáveis ao presente Protocolo.

2. As Partes tornarão extensível a aplicação das medidas estabelecidas nos artigos 14° a 21° e 23° a 35° da Convenção aos artigos 2° a 7° do presente Protocolo.

Capítulo IV – Disposições finais

Artigo 9° – Expressão do consentimento em ficar vinculado

1. O presente Protocol estará aberto à assinatura dos Estados signatários da Convenção, os quais poderão expressar o seu consentimento em ficarem vinculados por :

a. Assinatura, sem reserva de ratificação, aceitação ou aprovação ; ou

b. Assinatura, sob reserva de ratificação, aceitação ou aprovação, seguida de ratificação, aceitação ou aprovação.

2. Nenhum Estado poderá assinar o presente Protocolo sem reserva de ratificação, aceitação ou aprovação, nem depositar o seu instrumento de ratificação, aceitação ou aprovação se não tiver jà depositado, ou não depositar em simultâneo, o seu instrumento de ratificação, aceitação ou aprovação da Convenção.

3. Os instrumentos de ratificação, aceitação ou aprovação serão depositados junto do Secretário-Geral do Conselho da Europa.

Artigo 10° – Entrada em vigor

1. 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 Estados tenham expresso o seu consentimento em ficarem vinculados pelo presente Protocolo, de acordo com o disposto no artigo 9°.

2. Relativamente a qualquer Estado que expresse ulteriormente o seu consentimento em ficar vinculado pelo presente Protocolo, este entrará em vigor no primeiro dia dos mês seguinte ao termo de um período de três meses a contar da data de assinatura sem reserva de ratificação, aceitação ou aprovação, ou do depósito do seu instrumento de ratificação, aceitação ou aprovação.

Artigo 11° – Adesão

1. Após a entrada em vigor do presente Protocolo, qualquer Estado que tenha aderido à Convenção poderá aderir, igualmente, ao presente Protocolo.

2. A adesão será efectuada mediante o depósito, junto do Secretário-Geral do Conselho da Europa, de um instrumento de adesão, o qual produzirá efeitos no primeiro dia do mês seguinte ao termo de um período de três meses a contar da data do seu depósito.

Artigo 12° – Reservas e Declarações

1. As reservas e as declarações formuladas por uma Parte relativamenta a uma disposição da Convenção serão, igualmente, aplicáveis ao presente Protocolo, salvo se a referida Parte expresse intenção conrária no momento da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão.

2. Mediante notificação escrita dirigida ao Secretário-Geral do Conselho da Europa, qualquer Parte poderá, no momento da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, declarar que se fará prevalecer da reserva ou das reservas previstas nos artigos 3°, 5° e 6° do presente Protocolo. Uma Parte poderá, igualmente, formular, relativamente às disposições constantes do presente Protocolo, as reservas previstas no n.° 2 do artigo 22° e no n.° 1 do artigo 41° da Convenção, sem prejuízo da aplicação feita por essa Parte relativamente à Convenção. Nenhuma outra serva poderá ser formulada.

3. Mediante notificação escrita dirigida ao Secretario-Geral do Conselho da Europa, qualquer Parte poderá, no momento da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, declarar que se reservar a possibilidade de exigir elementos adicionais conforme previstas no n.° 2.a do artigo 5º e no n.° 2.a do artigo 6º do presente Protocolo.

Artigo 13 – Estatuto e retirada de reservas

1. A Parte que tenha formulado uma reserva em conformidade com o artigo 12° acima, pode retirá-la no todo ou em parte, logo que as circunstâncias o permitam. A retirada produzira efeito na data de recepção de uma notificação dirigida ao Secretário-Geral do Conselho da Europa. Se a notificação indicar que a retirada da reserva deve produzir efeito numa data precisa e essa data for posterior à da recepção da notificação pelo Secretário-Geral, a retirada produz efeito nessa data posterior.

2. O Secretário-Geral do Conselho da Europa pode, periodicamente, pedir às Partes que formularam uma ou mais reservas no termos do artigo 12° informações sobre as perspectivas de levantamento dessas reserva.

Artigo 14° – Aplicação territorial

1. Qualquer Estado pode, no momento da assinatura ou no momento do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, designar o, ou os territórios aos quais se aplicará a presente Protocolo.

2. Cada Estado pode subsequentemente, em qualquer altura, mediante declaração dirigida ao Secretário-Geral do Conselho da Europa, alargar a aplicação da presente Protocolo a qualquer outro território designado na declaração. O Protocolo entrará em vigor relativamente a este território no primeiro dia do mês seguinte ao termo de um prazo de três meses após a data da recepção da declaração pelo Secretário-Geral.

3. Qualquer declaração feita em conformidade com os dois números anteriores pode ser retirada, relativamente a qualquer um dos territórios nela designados, mediante notificação dirigida ao Secretário-Geral do Conselho da Europa. A retirada entrará em vigor no primeiro dia do mês seguinte ao termo de um prazo de três meses após a data da recepção da notificação pelo Secretário-Geral.

Artigo 15° – Denúncia

1. Qualquer Pare poderá, a todo o momento, denunciar o presente Protocolo mediante notificação ao Secretário-Geral do Conselho da Europa.

2. Tal denúncia produzirá efeitos no primeiro dia do mês seguinte ao termo de um período de três meses a contar da data de recepção da notificação pelo Secretário-Geral.

Artigo 16° – Notificação

O Secretário-Geral do Conselho da Europa notificará os Estados Membros do Conselho da Europa, os Estados não Membros que tenham participado na elaboração do presente Protocolo e qualquer Estado que a ele tenha aderido, ou tenha sido convidado a aderir, de:

a. Qualquer assinatura;

b. Depósito de qualquer instrumento de ratificação, aceitação, aprovação ou adesão;

c. Qualquer data de entrada em vigor do presente Protocolo em conformidade com os seus artigos 9°, 10° et 11°,

d. Qualquer outro acto, notificação ou comunicação relacionado com o presente Protocolo.

Em fé do que, os abaixo assinados, devidamente autorizados para o efeito, assinaram o presente Protocolo.

Feito em Estrasburgo, a 28 de Janeiro de 2003, em francês es inglês, fazendo ambos os textos igualmente fé, num único exemplar que será depositado nos arquivos do Conselho da Europa. O Secretário-Geral do Conselho da Europa transmitirá cópias autenticadas a cada um dos Estados Membros do Conselho da Europa, aos Estados não Membros que tenham particpato na elaboração do presente Protocolo e a qualquer Estados convidado a aderir ao presente Protocolo.

Relatório Explicativo do Protocolo Adicional à Convenção sobre o cibercrime

O texto do presente Relatório explicativo não constitui um instrumento que forneça uma interpretação vinculativa do Protocolo, embora possa ser suscetível de facilitar a aplicação das disposições nele contidas. O presente Protocolo será aberto à assinatura em Estrasburgo, em 28 de janeiro de 2003, por ocasião da Primeira Parte ou da Sessão de 2003 da Assembleia Parlamentar.

Introdução

1. Desde a adoção, em 1948, da Declaração Universal dos Direitos do Homem, a comunidade internacional realizou progressos importantes no combate contra o racismo, a discriminação racial, a xenofobia e a intolerância conexa. Foram promulgadas leis nacionais e internacionais e foram adotados vários instrumentos internacionais em matéria de direitos humanos, nomeadamente a Convenção Internacional de Nova Iorque, de 1965, sobre a Eliminação de Todas as Formas de Discriminação Racial, celebrada no âmbito das Nações Unidas (CERD). Embora já tenham sido realizados progressos, o desejo de um mundo livre de ódio racial e de preconceitos continua a estar apenas parcialmente cumprido.

2. À medida que os desenvolvimentos tecnológicos, comerciais e económicos aproximam os povos do mundo, a discriminação racial, a xenofobia e outras formas de intolerância continuam a existir nas nossas sociedades. A globalização comporta riscos que podem conduzir à exclusão e ao aumento das desigualdades, muitas vezes seguindo critérios raciais e étnicos.

3. Em especial, o surgimento de redes de comunicação internacionais como a Internet proporciona a determinadas pessoas meios modernos e poderosos de apoiar o racismo e a xenofobia e permite-lhes divulgar fácil e amplamente expressões que contêm essas ideias. Para investigar e processar judicialmente essas pessoas, a cooperação internacional é fundamental. A Convenção sobre o Cibercrime (STE 185), a seguir designada "a Convenção", foi elaborada de modo a permitir a assistência mútua em matéria de crimes informáticos no sentido mais lato, de uma forma flexível e moderna.

O presente Protocolo tem dois objetivos: em primeiro lugar, harmonizar o direito penal substantivo no combate contra o racismo e a xenofobia na Internet e, em segundo lugar, melhorar a cooperação internacional neste domínio. Este tipo de harmonização representa um adjuvante no combate a estes crimes tanto no plano nacional como no plano internacional. As infrações correspondentes no

direito interno podem impedir a utilização abusiva de sistemas informáticos para fins racistas pelas Partes cujas leis neste domínio estão menos bem definidas. Consequentemente, o útil intercâmbio de experiências comuns, em termos do tratamento prático dos casos, também poderá ser assim intensificado. A cooperação internacional (em especial, na extradição e na assistência jurídica mútua) fica pois facilitada, por exemplo, no que toca aos requisitos de criminalidade dupla.

4. O comité que elaborou a Convenção debateu a possibilidade de incluir outras infrações relacionadas com o conteúdo, tais como a distribuição de propaganda racista através de sistemas informáticos. Todavia, o comité não se encontrava em posição de alcançar um consenso no que respeita à criminalização de tal conduta. Se, por um lado, se constatava a existência de uma percentagem significativa a favor da introdução deste ponto enquanto infração penal, algumas delegações manifestaram grande preocupação face à inclusão desta disposição apontando como fundamento a liberdade de expressão. Ciente da complexidade desta matéria, foi decidido que o comité iria remeter ao Comité Europeu para os Problemas Criminais (CDPC) a questão da elaboração de um Protocolo adicional à Convenção.

5. A Assembleia Parlamentar, no seu Parecer 226(2001) sobre a Convenção, recomendou a elaboração imediata de um protocolo à Convenção intitulado "Alargamento do âmbito de aplicação da Convenção de modo a incluir novas formas de infração", com o objetivo de definir e criminalizar, *inter alia,* a divulgação de propaganda racista.

6. Por conseguinte, o Comité de Ministros confiou ao Comité Europeu para os Problemas Criminais (CDPC) e, em especial, ao seu Comité de Peritos sobre a Criminalização dos Atos de Natureza Racista e Xenófoba cometidos através de Sistemas Informáticos (PC-RX), a tarefa de preparar um projeto de Protocolo adicional, um instrumento juridicamente vinculativo aberto à assinatura e ratificação das Partes contratantes na Convenção, que aborde, nomeadamente, o seguinte:

i. a definição e o âmbito dos elementos para a criminalização de atos de caráter racista e xenófobo cometidos através de redes informáticas, incluindo a produção, oferta, divulgação ou outras formas de distribuição de materiais ou mensagens com tais conteúdos através de redes informáticas;

ii. o âmbito de aplicação das disposições substantivas, processuais e de cooperação internacional da Convenção sobre o Cibercrime à investigação e ação penal das infrações a definir no âmbito do Protocolo adicional.

7. O presente Protocolo envolve um alargamento do âmbito de aplicação da Convenção, incluindo das suas disposições substantivas, processuais e de cooperação internacional, de modo a abranger também as infrações de propaganda racista e xenófoba. Assim, para além da harmonização dos elementos de direito substantivo desses comportamentos, o Protocolo visa melhorar a capacidade das Partes para utilizarem os meios e as vias de cooperação internacional previstos na Convenção neste domínio.

Comentário sobre os artigos do Protocolo

Capítulo I – Disposições comuns

Artigo 1º – Objeto

8. O objetivo do presente Protocolo é a complementaridade, pelas Partes no presente Protocolo, das disposições relativamente à criminalização de atos de natureza racista e xenófoba praticados através de sistemas informáticos.

9. As disposições do Protocolo têm caráter vinculativo. Para cumprir estas obrigações, os Estados Partes têm não só de promulgar legislação adequada, mas também de assegurar a sua aplicação efetiva.

Artigo 2º – Definição

N.º 1 – "Material racista e xenófobo"

10. Foram elaborados vários instrumentos jurídicos a nível internacional e nacional para combater o racismo ou a xenofobia. Os redatores deste Protocolo tiveram especialmente em conta: i) a Convenção Internacional sobre a Eliminação de Todas as Formas de Discriminação Racial (CERD), ii) o Protocolo n.º 12 (STE 177) à Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (CEDH), iii) a Ação Comum de 15 de julho de 1996 da União Europeia, adotada pelo Conselho com base no artigo K.3 do Tratado da União Europeia, relativa à ação contra o racismo e a xenofobia, iv) a Conferência Mundial contra o Racismo, a Discriminação Racial, a Xenofobia e a Intolerância Conexa (Durban, 31 de agosto-setembro de 2001), v) as conclusões da Conferência Europeia contra o Racismo (Estrasburgo, 13 de outubro de 2000), vi) o estudo exaustivo publicado pela Comissão Europeia contra o Racismo e a Intolerância (ECRI) publicado em agosto de 2000 (CRI(2000)27) e vii) a Proposta de Decisão-Quadro do Conselho relativa ao combate contra o racismo e a xenofobia (no quadro da União Europeia), apresentada em novembro de 2001 pela Comissão Europeia.

11. O artigo 10.º da CEDH reconhece o direito à liberdade de expressão, que inclui a liberdade de opinião e de receber e transmitir informações e ideias. O artigo 10.º da CEDH é aplicável não só às informações e ideias que são acolhidas favoravelmente ou consideradas inofensivas ou indiferentes, mas também às que ofendem, chocam ou perturbam o Estado ou qualquer setor da população[12]. No entanto, o Tribunal Europeu dos Direitos do Homem considerou que as ações do Estado destinadas a restringir o direito à liberdade de expressão estavam devidamente justificadas ao abrigo das restrições previstas no artigo 10.º, n.º 2, da CEDH, em especial quando essas ideias ou expressões violavam os direitos de terceiros. Este Protocolo, com base em instrumentos nacionais e internacionais, estabelece em que medida a divulgação de expressões e ideias racistas e xenófobas viola os direitos de terceiros.

12. 12. A definição contida no artigo 2.º refere-se a textos, livros, revistas, declarações, mensagens, etc., imagens (por exemplo, imagens, fotografias, desenhos, etc.) ou qualquer outra representação de pensamentos ou teorias, de natureza racista e xenófoba, num formato tal que possam ser armazenados, processados e transmitidos através de um sistema informático.

13. A definição contida no artigo 2.º do presente Protocolo refere-se a certas condutas a que o conteúdo do material pode conduzir, e não à expressão de sentimentos/crenças/aversão contidos no material em causa. A definição baseia-se, tanto quanto possível, em definições e documentos nacionais e internacionais existentes (ONU, UE).

14. A definição exige que esse material defenda, promova, incite ao ódio, à discriminação ou à violência. "Defenda" refere-se a um fundamento a favor do ódio, da discriminação ou da violência, "promova" refere-se a um incentivo ou a uma promoção do ódio, da discriminação ou da violência e "incite" refere-se a instar outros ao ódio, à discriminação ou à violência.

15. O termo "violência" refere-se ao uso ilegal da força, ao passo que o termo "ódio" se refere a aversão ou inimizade intensa.

16. Na interpretação do termo "discriminação", deve-se ter em conta a CEDH (artigo 14.º e Protocolo n.º 12) e a jurisprudência pertinente, bem como o artigo 1.º da CERD. A proibição de discriminação contida na CEDH garante a todas as pessoas sujeitas à jurisdição de um Estado Parte a igualdade no exercício dos direitos e liberdades protegidos pela própria CEDH. O artigo 14.º da CEDH

12. Ver, neste contexto, por exemplo, o acórdão Handyside de 7 de dezembro de 1976, série A, n.º 24, p. 23, n.º 49. 3.

prevê uma obrigação geral para os Estados, acessória aos direitos e liberdades nela previstos. Neste contexto, o termo "discriminação" utilizado no Protocolo refere-se a um tratamento diferente e injustificado concedido a pessoas ou a um grupo de pessoas com base em determinadas características. Em vários acórdãos (como o processo "linguístico belga", o acórdão Abdulaziz, Cabales e Balkandali[13] o Tribunal Europeu dos Direitos do Homem declarou que "uma diferença de tratamento é discriminatória se 'não tiver justificação objetiva e razoável', ou seja, se não prosseguir um 'objetivo legítimo' ou se não existir uma 'relação razoável de proporcionalidade entre os meios utilizados e o objetivo pretendido'". A questão de saber se o tratamento é ou não discriminatório deve ser apreciada à luz das circunstâncias específicas do caso em apreço. As orientações para a interpretação do termo "discriminação" também podem ser encontradas no artigo 1.º da CERD, em que o termo "discriminação racial" significa "qualquer distinção, exclusão, restrição ou preferência fundada na raça, cor, ascendência ou origem nacional ou étnica que tenha como objetivo ou como efeito destruir ou comprometer o reconhecimento, o gozo ou o exercício, em condições de igualdade, dos direitos do homem e das liberdades fundamentais nos domínios político, económico, social, cultural ou de qualquer outro domínio da vida pública".

17. O ódio, a discriminação ou a violência têm de ser dirigidos contra qualquer indivíduo ou grupo de indivíduos, pelo facto de pertencerem a um grupo caracterizado pela "raça, cor, ascendência ou origem nacional ou étnica, bem como pela religião, se utilizados como pretexto para qualquer destes fatores".

18. Note-se que estes motivos não são exatamente os mesmos que constam, por exemplo, no artigo 1.º do Protocolo n.º 12 à CEDH, uma vez que alguns deles são estranhos ao conceito de racismo ou xenofobia. Os motivos constantes no artigo 2.º do presente Protocolo também não são idênticos aos contidos na CERD, uma vez que este última aborda a "discriminação racial", em geral, e não o "racismo", enquanto tal. Globalmente, estes fundamentos devem ser interpretados na aceção do direito e da prática nacionais e internacionais estabelecidos. No entanto, alguns deles requerem explicações adicionais quanto ao seu significado específico no contexto do presente Protocolo.

19. O termo "ascendência" refere-se principalmente a pessoas ou grupos de pessoas descendentes de pessoas que podem ser identificadas por determinadas características (como a raça ou a cor), mas podendo não se verificar

13. Abulaziz, Cabales e Balkandali, acórdão de 28 de maio de 1985, série A, n.º 94, p. 32, n.º 62; processo "linguístico belga", acórdão de 23 de julho de 1968, série A, n.º 6, p. 34, n.º 10.

já necessariamente todas essas características. Não obstante, devido à sua ascendência, essas pessoas ou grupos de pessoas podem ser alvo de ódio, discriminação ou violência. "Ascendência" não se refere à origem social.

20. O conceito de "origem nacional" deve ser entendido num sentido factual lato. Pode referir-se à história dos indivíduos, não apenas no que respeita à nacionalidade ou à origem dos seus antepassados, mas também à sua pertença nacional, independentemente de, do ponto de vista jurídico, ainda a possuir. Quando as pessoas têm mais do que uma nacionalidade ou são apátridas, a interpretação lata deste conceito pretende protegê-las se forem discriminadas por qualquer destes motivos. Além disso, o conceito de "origem nacional" pode referir-se não só à pertença a um dos países internacionalmente reconhecidos como tal, mas também a minorias ou outros grupos de pessoas, com características semelhantes.

21. O conceito de "religião" surge, com frequência, nos instrumentos internacionais e na legislação nacional. O termo refere-se a convicções e crenças. A inclusão deste termo como tal na definição envolveria o risco de ir para além do âmbito de aplicação do presente Protocolo. No entanto, a religião pode ser utilizada como pretexto, álibi ou substituto de outros fatores enumerados na definição. Por conseguinte, o termo "religião" deve ser interpretado neste sentido restrito.

N.º 2

22. Ao indicar que as expressões e os termos utilizados no presente Protocolo serão interpretados da mesma maneira que os utilizados na Convenção, este artigo assegura uma interpretação uniforme de ambos. Isto significa que os termos e expressões utilizados neste Relatório explicativo devem ser interpretados da mesma forma que esses termos e expressões são interpretados no Relatório explicativo da Convenção.

Capítulo II – Medidas a tomar a nível nacional

Considerações gerais

23. As infrações previstas no presente Protocolo contêm uma série de elementos comuns extraídos da Convenção. Por razões de clareza, são a seguir incluídos os parágrafos correspondentes do Relatório explicativo da Convenção.

24. Uma especificidade das infrações englobadas reside no requisito expresso de que a conduta em causa seja seguida "sem que tal direito lhe assista". Isto reflete a noção de que a conduta descrita nem sempre é punível per se, mas

poderá ser legal ou justificada não só em casos aos quais se aplicam as clássicas exceções prescritas nos termos da lei como, por exemplo, o consentimento, a autodefesa ou a necessidade, mas também quando estamos perante outros princípios ou interesses que levam à exclusão da responsabilidade criminal (por exemplo, para fins de aplicação da lei, académicos ou de investigação). A expressão "sem que tal direito lhe assista" deve o seu significado ao contexto em que é utilizada. Assim, não constituindo uma restrição à forma como as Partes implementam o conceito no seu direito interno, a expressão poderá referir-se a uma conduta seguida sem autoridade (quer seja de natureza legislativa, executiva, administrativa, judicial, contratual ou consensual) ou a uma conduta que não se encontra, de outra forma coberta pelas defesas legais, alegações, justificações ou princípios relevantes ao abrigo do direito interno. O Protocolo coloca portanto de lado a conduta assumida em consonância com a autoridade governamental legítima (por exemplo quando o governo da Parte age no sentido de manter a ordem pública, proteger a segurança nacional ou investigar infrações penais). Além do mais as atividades comuns e legítimas inerentes à conceção de redes ou a práticas comuns de exploração e de comércio legítimas não deverão ser penalizadas. Cabe assim às Partes determinar a forma como tais exemplos são implementados no âmbito dos seus sistemas jurídicos internos (ao abrigo do direito penal ou outro).

25. Todas as infrações enunciadas no Protocolo deverão ser cometidas "intencionalmente" para que seja imputável a responsabilidade criminal. Em determinados casos, a infração inclui um elemento intencional específico adicional. Os redatores do Protocolo, à semelhança dos da Convenção, acordaram que o significado exato do termo "intencionalmente" deveria ser deixado ao critério de interpretação nacional. As pessoas não podem ser responsabilizadas penalmente por qualquer das infrações previstas no presente Protocolo se não tiverem a intenção exigida. Não será suficiente, por exemplo, para que um fornecedor de serviços seja responsabilizado penalmente nos termos desta disposição, que tal fornecedor de serviços desempenhe um papel de intermediário no contexto da transmissão deste material, através de uma página Web ou de canais de notícias (newsrooms) que contenham o referido material, sem que esteja preenchido o requisito intencional, neste caso particular, em virtude do disposto na legislação nacional. Além do mais, um fornecedor de serviços não é obrigado a monitorizar tais condutas e conteúdos a fim de evitar a responsabilidade criminal.

26. No que diz respeito ao conceito de "sistema informático", este é o mesmo que o contido na Convenção e explicado nos n.os 23 e 24 do respetivo Relatório explicativo. Trata-se de uma aplicação do artigo 2.º do presente Protocolo (ver também a explicação do artigo 2.º supra).

Artigo 3º – Difusão de material racista e xenófobo através de um sistema informático

27. Este artigo exige que os Estados Partes criminalizem a divulgação ou outras formas de colocação à disposição do público de material racista e xenófobo através de um sistema informático. O ato de divulgação ou disponibilização só é criminoso se a intenção for também dirigida ao caráter racista e xenófobo do material.

28. "Divulgação" refere-se à difusão ativa de material racista e xenófobo a outros, tal como definido no artigo 2.º do Protocolo, ao passo que "disponibilização" se refere à colocação online de material racista e xenófobo para a utilização por outros. Este termo também engloba a criação ou compilação de hiperligações de modo a facilitar o acesso a tais materiais.

29. O termo "do público" utilizado no artigo 3.º deixa claro que as comunicações ou expressões privadas comunicadas ou transmitidas através de um sistema informático não são abrangidas pelo âmbito de aplicação desta disposição. Com efeito, tais comunicações ou expressões, como as formas tradicionais de correspondência, estão protegidas pelo artigo 8.º da CEDH.

30. A questão de apurar se uma comunicação de material racista e xenófobo é considerada uma comunicação privada ou difusão ao público tem de ser determinada com base nas circunstâncias do caso em apreço. Em primeiro lugar, o que conta é a intenção do remetente de que a mensagem em causa só seja recebida pelo destinatário predeterminado. A existência desta intenção subjetiva pode ser estabelecida com base em vários fatores objetivos, tais como o conteúdo da mensagem, a tecnologia utilizada, as medidas de segurança aplicadas e o contexto em que a mensagem é enviada. Quando essas mensagens são enviadas simultaneamente para mais do que um destinatário, o respetivo número e a natureza da relação entre o remetente e o(s) destinatário(s) constitui um fator para determinar se essa comunicação pode ser considerada privada.

31. O intercâmbio de material racista e xenófobo em salas de conversa (chat rooms), a publicação de mensagens semelhantes em grupos de notícias ou fóruns de discussão são exemplos da disponibilização desse material ao público. Nestes casos, o material é acessível a qualquer pessoa. Mesmo quando o acesso ao material exige uma autorização por meio de uma palavra-passe, o material é acessível ao público quando essa autorização é concedida a alguém ou a qualquer pessoa que preencha determinados critérios. A fim de determinar se a disponibilização ou distribuição era ou não pública, importa ter em conta a natureza da relação entre as pessoas em causa.

32. Os n.os 2 e 3 são incluídos para prever uma possibilidade de reserva em circunstâncias muito limitadas, devendo ser lidos em conjunto e em sequência. Assim sendo, uma Parte tem, em primeiro lugar, a possibilidade de não imputar responsabilidade penal às condutas previstas no presente artigo sempre que o material preconize, promova ou incite à discriminação não associada a ódio ou violência e desde que existam por outros mecanismos eficazes. Por exemplo, esses mecanismos podem ser civis ou administrativos. Sempre que uma Parte não possa, devido aos princípios estabelecidos no seu sistema jurídico em matéria de liberdade de expressão, prever tais mecanismos, pode reservar-se o direito de não aplicar a obrigação prevista no n.º 1 do presente artigo, desde que esta apenas diga respeito à defesa, promoção ou incitamento à discriminação que não esteja associada ao ódio ou à violência. Uma Parte pode restringir ainda mais o âmbito da reserva exigindo que a discriminação seja, por exemplo, insultuosa, degradante ou ameaçadora para um grupo de pessoas.

Artigo 4º – Ameaça com motivação racista e xenófoba

33. A maioria da legislação prevê a criminalização da ameaça em geral. Os redatores concordaram em salientar no Protocolo que, sem sombra de dúvida, as ameaças com motivações racistas e xenófobas devem ser criminalizadas.

34. O conceito de "ameaça" pode referir-se a uma ameaça que gera receio nas pessoas a quem a ameaça é dirigida de que sofrerão a prática de uma infração penal grave (por exemplo, que afete a vida, a segurança ou a integridade pessoais, danos graves a bens, etc., da vítima ou dos seus familiares). É da competência dos Estados Partes determinar o que constitui uma infração penal grave.

35. De acordo com este artigo, a ameaça tem de ser dirigida a: i) uma pessoa por pertencer a um grupo que se caracterize pela sua raça, cor, ascendência ou origem nacional ou étnica, ou, ainda pela sua religião, na medida em que esta sirva de pretexto a qualquer um dos outros elementos, ou ii) dirigida a um grupo de pessoas que se distinga por qualquer uma das referidas características. Não existe qualquer restrição de que a ameaça tenha de ser pública. Este artigo abrange igualmente as ameaças das comunicações privadas.

Artigo 5º – Insulto com motivação racista e xenófoba

36. O artigo 5.º aborda a questão de insultar publicamente uma pessoa ou um grupo de pessoas por pertencerem ou se considerar pertencerem a um grupo que se distingue por características específicas. O conceito de "insulto"

refere-se a qualquer expressão ofensiva, de desprezo ou injuriosa que lese a honra ou a dignidade de uma pessoa. Deve resultar claro da própria expressão que o insulto está diretamente relacionado com a pertença da pessoa insultada ao grupo. Ao contrário do que acontece em caso de ameaça, um insulto expresso em comunicações privadas não é abrangido por esta disposição.

37. O n.º 2, alínea i), permite às Partes exigir que a conduta tenha igualmente por efeito que a pessoa ou o grupo de pessoas esteja, não só potencialmente, mas também efetivamente exposto ao ódio, ao desprezo ou ao ridículo.

38. O n.º 2, alínea ii), permite às Partes formular reservas que vão mais além, até mesmo aos aspetos em que o n.º 1 não é aplicável.

Artigo 6º – Negação, minimização grosseira, aprovação ou justificação do genocídio ou dos crimes contra a humanidade

39. Nos últimos anos, vários processos foram tratados pelos tribunais nacionais em que pessoas (em público, nos meios de comunicação social, etc.) expressaram ideias ou teorias que visam negar, minimizar grosseiramente, aprovar ou justificar os crimes graves ocorridos, em especial, durante a Segunda Guerra Mundial (em especial o Holocausto). A motivação para tais comportamentos é frequentemente apresentada com o pretexto da investigação científica, ao passo que visam efetivamente apoiar e promover a motivação política que deu origem ao Holocausto. Além disso, estes comportamentos inspiraram ou até estimularam e incentivaram grupos racistas e xenófobos na sua ação, nomeadamente através de sistemas informáticos. A expressão dessas ideias insulta (a memória) as pessoas que foram vítimas desse mal, bem como os seus familiares. Por último, ameaça a dignidade da comunidade humana.

40. O artigo 6.º, que tem uma estrutura semelhante à do artigo 3.º, aborda este problema. Os redatores concordaram ser importante criminalizar as expressões que neguem, minimizem grosseiramente, aprovem ou justifiquem atos que constituam genocídio ou crimes contra a humanidade, tal como definidos pelo direito internacional e reconhecidos como tal por decisões definitivas e vinculativas do Tribunal Militar Internacional, instituído pelo Acordo de Londres de 8 de abril de 1945[14]. Tal deve-se ao facto de as condutas mais importantes e estabelecidas que deram origem a genocídios e crimes contra a humanidade terem ocorrido durante o período de 1940-1945. No entanto, os redatores reconheceram que, desde então, ocorreram outros casos de genocídio e crimes

14. Acórdão Lehideux e Isorni de 23 de setembro de 1998, Relatórios 1998-VII, para. 47.

contra a humanidade, fortemente motivados por teorias e ideias de natureza racista e xenófoba. Por conseguinte, os redatores consideraram necessário não limitar o âmbito de aplicação desta disposição apenas aos crimes cometidos pelo regime nazi durante a Segunda Guerra Mundial e estabelecidos como tal pelo Tribunal de Nuremberga, mas também aos genocídios e crimes contra a humanidade instituídos por outros tribunais internacionais criados desde 1945 por instrumentos jurídicos internacionais pertinentes (como as Resoluções do Conselho de Segurança das Nações Unidas, tratados multilaterais, etc.). Esses tribunais podem ser, por exemplo, os tribunais penais internacionais para a ex-Jugoslávia, para o Ruanda ou o Tribunal Penal Internacional Permanente. Este artigo permite remeter para decisões definitivas e vinculativas de futuros tribunais internacionais, na medida em que a competência desse tribunal seja reconhecida pela Parte signatária do presente Protocolo.

41. A disposição destina-se a esclarecer que factos cuja exatidão histórica tenha sido demonstrada não podem ser negados, minimizados grosseiramente, aprovados ou justificados para sustentar estas teorias e ideias detestáveis.

42. O Tribunal Europeu dos Direitos Humanos deixou claro que a negação ou a revisão de "factos históricos claramente estabelecidos – como o Holocausto – [...] seriam excluídos da proteção do artigo 10.º pelo artigo 17.º" da CEDH (ver, neste contexto, o acórdão Lehideux e Isorni de 23 de setembro de 1998).

43. O artigo 6.º, n.º 2, permite a uma Parte: i) exigir, através de uma declaração, que a negação ou a minimização grosseira, conforme prevista no artigo 6.º, n.º 1, seja praticada com a intenção de incitar ao ódio, à discriminação ou à violência contra uma pessoa ou um grupo de pessoas em função da sua raça, cor, ascendência ou origem nacional ou étnica ou, ainda, da sua religião, na medida em que esta sirva como pretexto a qualquer um dos outros elementos, ou ii) utilizar uma reserva, autorizando uma Parte a não aplicar – no todo ou em parte – esta disposição.

Artigo 7º – Auxílio e cumplicidade

44. O objetivo do presente artigo é instituir como infrações penais o auxílio ou a cumplicidade na prática de quaisquer das infrações definidas ao abrigo do disposto nos artigos 3.º a 6.º. Contrariamente à Convenção, o Protocolo não prevê a criminalização da tentativa de cometer as infrações nele contidas, uma vez que muitas das condutas criminalizadas têm uma natureza preparatória.

45. A responsabilidade advém do auxílio ou da cumplicidade nos casos em que a pessoa que comete uma infração definida pelo Protocolo é apoiada

por outra pessoa que pretende igualmente que a infração seja cometida. Por exemplo, embora a transmissão de material racista e xenófobo através da Internet requeira a assistência de fornecedores de serviços enquanto intermediários, um fornecedor de serviços que não apresente qualquer intenção criminal não poderá ser responsabilizado ao abrigo do disposto nesta secção. Assim não existe qualquer dever por parte de um fornecedor de serviços de fiscalizar ativamente os conteúdos em causa de modo a evitar a responsabilidade criminal conforme estabelecido nesta disposição.

46. Tal como se verifica com todas as infrações definidas em conformidade com as disposições do Protocolo, o auxílio ou a cumplicidade deverão ocorrer de forma intencional.

Capítulo III – Relações entre a Convenção e o presente Protocolo

Artigo 8º – Relações entre a Convenção e o presente Protocolo

47. O artigo 8.° aborda as relações entre a Convenção e o presente Protocolo. Esta disposição evita a inclusão de uma série de disposições da Convenção no presente Protocolo. Indica que algumas das disposições da Convenção se aplicam, *mutatis mutandis,* ao presente Protocolo (por exemplo, no que diz respeito à responsabilidade acessória e às sanções, às jurisdições e a uma parte das disposições finais). O n.º 2 recorda às Partes que o significado definido na Convenção se deve aplicar às infrações do Protocolo. Por razões de clareza, são especificados os artigos conexos.

Capítulo IV – Disposições finais

48. As disposições contidas no presente Capítulo baseiam-se, essencialmente, nas "Cláusulas-tipo finais para as convenções e acordos celebrados no quadro do Conselho da Europa", as quais foram aprovadas pelo Comité de Ministros na 315.ª reunião dos Delegados, realizada em fevereiro de 1980. Dado que, na sua maioria, os artigos 9.º a 16.º 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. Todavia, certas modificações às cláusulas-tipo ou algumas novas disposições deverão ser objeto de uma explicação adicional. A este respeito, é de salientar o facto de as cláusulas-tipo terem sido adotadas como um conjunto de disposições de caráter não vinculativo. Tal como indicado na introdução às cláusulas-tipo, "as presentes cláusulas-tipo finais destinam-se apenas a facilitar o papel desempenhado pelos comités de peritos e a evitar divergências textuais que não teriam uma

real justificação. O modelo não é, de modo algum, vinculativo e podem ser adotadas cláusulas diferentes para se adaptarem a casos específicos (neste contexto ver também os n.os 304-330 do Relatório explicativo da Convenção).

49. O artigo 12.º, n.º 2, especifica que as Partes podem utilizar a reserva definida nos artigos 3.º, 5.º e 6.º do presente Protocolo. Nenhuma outra reserva poderá ser formulada.

50. O presente Protocolo só está aberto à assinatura dos signatários da Convenção. O Protocolo entrará em vigor três meses após cinco Partes na Convenção terem manifestado o seu consentimento em ficar vinculadas pelo mesmo (artigos 9.º a 10.º).

51. A Convenção permite reservas relativamente a determinadas disposições que, através da cláusula de ligação do artigo 8.º do Protocolo, podem também ter efeitos nas obrigações de uma Parte ao abrigo do Protocolo. No entanto, uma Parte pode notificar o Secretário-Geral de que não aplicará esta reserva no que respeita ao teor do Protocolo. Tal está expresso no artigo 12.º, n.º 2, do Protocolo.

52. No entanto, quando uma Parte não tiver feito uso dessa possibilidade de reserva ao abrigo da Convenção, pode ter necessidade de restringir as suas obrigações em relação às infrações previstas no Protocolo. O artigo 12.º, n.º 2, permite que as Partes o façam em relação ao artigo 22.º, n.º 2, e ao artigo 41.º, n.º 1, da Convenção.

Segundo Protocolo Adicional relativo ao reforço da cooperação e da divulgação de provas sob a forma eletrónica (STCE No. 224), Estrasburgo, 12 de Maio de 2022

Preâmbulo

Os Estados-Membros do Conselho da Europa e os outros Estados Partes na Convenção sobre o Cibercrime, (STE n.º 185, a seguir designada "a Convenção"), aberta à assinatura em Budapeste, a 23 de Novembro de 2001, signatários do presente Protocolo;

Tendo em conta o alcance e o impacto da Convenção em todas as regiões do mundo;

Recordando que a Convenção já foi complementada pelo Protocolo Adicional relativo à incriminação de atos de natureza racista e xenófoba praticados através de sistemas informáticos (STE n.º 189), aberto à assinatura em Estrasburgo em 28 de janeiro de 2003 (a seguir designado "o Primeiro Protocolo"), entre as Partes nesse Protocolo;

Tendo em conta os tratados do Conselho da Europa em vigor sobre a cooperação em matéria penal, bem como outros acordos e convénios sobre cooperação em matéria penal entre as Partes na Convenção;

Tendo igualmente em conta a Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (STE n.º 108), com a redação que lhe foi dada pelo seu Protocolo de alterações (STCE n.º 223), aberta à assinatura em Estrasburgo em 10 de outubro de 2018, e à qual qualquer Estado pode ser convidado a aderir;

Reconhecendo a utilização crescente das tecnologias da informação e da comunicação, incluindo os serviços de Internet, e o aumento do cibercrime, que constitui uma ameaça para a democracia e o Estado de direito e que muitos Estados também consideram como uma ameaça para os direitos humanos;

Reconhecendo igualmente o número crescente de vítimas de cibercrime e a importância de obter justiça para essas vítimas;

Recordando que os governos têm a responsabilidade de proteger a sociedade e os indivíduos contra a criminalidade não apenas offline, mas também online, nomeadamente através de investigações e ações penais eficazes;

Conscientes de que os elementos de prova de qualquer infração penal são cada vez mais armazenados em formato eletrónico em sistemas informáticos em jurisdições estrangeiras, múltiplas ou desconhecidas, e convictos de que são necessárias medidas adicionais para obter de forma legítima esses elementos de prova a fim de permitir uma resposta eficaz da justiça penal e defender o Estado de direito;

Reconhecendo a necessidade de uma cooperação reforçada e mais eficaz entre os Estados e o setor privado, e que, neste contexto, é necessária uma maior clareza ou segurança jurídica para os fornecedores de serviços e outras entidades no que diz respeito às circunstâncias em que podem responder a pedidos diretos das autoridades de justiça penal de outras Partes para a divulgação de dados eletrónicos;

Visando, por conseguinte, reforçar a cooperação em matéria de cibercrime e de recolha de provas sob forma eletrónica de qualquer infração penal para efeitos de investigações ou processos penais específicos através de instrumentos adicionais relativos a uma assistência mútua e a outras formas de cooperação entre as autoridades competentes mais eficientes, à cooperação em situações de emergência, e à cooperação direta entre as autoridades competentes e os fornecedores de serviços e outras entidades na posse ou controlo de informação pertinente;

Convictos de que uma cooperação transfronteiras eficaz para fins de justiça penal, incluindo entre os setores público e privado, beneficia de condições e salvaguardas eficazes para a proteção dos direitos humanos e das liberdades fundamentais;

Reconhecendo que a recolha de provas sob a forma eletrónica para investigações penais diz frequentemente respeito a dados pessoais e reconhecendo

o requisito, em muitas Partes, de proteger a privacidade e os dados pessoais para cumprir as suas obrigações constitucionais e internacionais; e

Cientes da necessidade de garantir que as medidas de justiça penal eficazes em matéria de cibercrime e de recolha de provas sob a forma eletrónica estejam sujeitas a condições e salvaguardas que deverão assegurar a proteção adequada dos direitos humanos e das liberdades fundamentais, incluindo os direitos decorrentes das obrigações que os Estados assumiram ao abrigo dos instrumentos internacionais aplicáveis em matéria de direitos humanos, como a Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais de 1950 (STE n.º 5) do Conselho da Europa, o Pacto Internacional sobre os Direitos Civis e Políticos das Nações Unidas de 1966, a Carta Africana dos Direitos do Homem e dos Povos, a Convenção Americana sobre os direitos do Homem de 1969, e outros tratados internacionais sobre direitos humanos;

Acordaram no seguinte:

Capítulo I – Disposições comuns

Artigo 1.º – Objeto

O presente Protocolo tem por objetivo complementar:

a. a Convenção entre as Partes no presente Protocolo; e

b. o Primeiro Protocolo entre as Partes no presente Protocolo que também são Partes no Primeiro Protocolo.

Artigo 2.º – Âmbito de aplicação

1. Salvo disposição em contrário no presente Protocolo, as medidas descritas no presente Protocolo são aplicáveis:

a. 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 e com a recolha de provas sob a forma eletrónica de uma infração penal; e

b. entre as Partes no Primeiro Protocolo que são Partes no presente Protocolo, em investigações ou processos penais específicos relativos a infrações penais estabelecidas nos termos do Primeiro Protocolo.

2. Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para darem cumprimento às obrigações estabelecidas no presente Protocolo.

Artigo 3.º – Definições

1. As definições constantes dos artigos 1.º e 18.º, n.º 3, da Convenção aplicam-se ao presente Protocolo.

2. Para efeitos do presente Protocolo, aplicam-se as seguintes definições adicionais:

a. "autoridade central" refere-se à 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;

b. "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, cujo objeto seja a recolha ou a produção de provas relativamente a investigações ou processos penais específicos;

c. "emergência" refere-se a uma situação na qual existe um risco significativo e iminente para a vida ou a segurança de uma pessoa singular;

d. "dados pessoais" refere-se a informação relativa a uma pessoa singular identificada ou identificável;

e. "parte que procede à transferência" refere-se à Parte que transmite os dados em resposta a um pedido ou como parte de uma equipa de investigação conjunta ou, para efeitos da secção 2 do capítulo II, uma Parte em cujo território está localizado um fornecedor de serviços de transmissão ou uma entidade que presta serviços de registo de nomes de domínio.

Artigo 4.º – Língua

1. Os pedidos, as ordens e a informação que os acompanha, apresentados a uma Parte, devem ser redigidos numa língua aceite pela Parte requerida ou pela Parte notificada nos termos do artigo 7.º, n.º 5, ou ser acompanhados de uma tradução nessa língua.

2. As ordens nos termos do artigo 7.º e os pedidos nos termos do artigo 6.º, bem como qualquer informação que os acompanhe, devem ser:

a. apresentados numa língua da outra Parte na qual o fornecedor de serviços ou a entidade aceita um processo nacional comparável;

b. apresentados numa outra língua aceite pelo fornecedor de serviços ou pela entidade; ou

c. acompanhados por uma tradução numa das línguas indicadas nos n.º 2, alínea a) ou b).

Capítulo II – Medidas de cooperação reforçada

Secção 1 – Princípios gerais aplicáveis ao capítulo II

Artigo 5.º – Princípios gerais aplicáveis ao capítulo II

1. As Partes cooperarão, tanto quanto possível, em conformidade com as disposições do presente capítulo.

2. A secção 2 do presente capítulo é constituída pelos artigos 6.º e 7.º. Estabelece os procedimentos que reforçam a cooperação direta com fornecedores e entidades no território de outra Parte. A secção 2 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.

3. A secção 3 do presente capítulo é constituída pelos artigos 8.º e 9.º. Estabelece os procedimentos para reforçar a cooperação internacional entre autoridades para a divulgação de dados informáticos armazenados. 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.

4. A secção 4 do presente capítulo é constituída pelo artigo 10.º. Estabelece os procedimentos relativos à assistência mútua de emergência. A secção 4 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.

5. A secção 5 do presente capítulo é constituída pelos artigos 11.º e 12.º. A secção 5 aplica-se 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.

6. Quando, em conformidade com as disposições do presente Protocolo, a Parte requerida estiver autorizada a prestar cooperação subordinada à existência de dupla incriminação, esta condição será considerada como satisfeita se a conduta que constitui a infração relativamente à qual foi efetuado o pedido de assistência, for qualificada como infração penal pelo seu direito interno, quer o direito interno classifique ou não a infração na mesma categoria de infrações ou a designe ou não pela mesma terminologia que o direito da Parte requerente.

7. As disposições do presente capítulo não restringem a 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.

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

1. Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes, para efeitos de investigações ou processos penais específicos, a apresentar um pedido a uma entidade que preste serviços de registo de nomes de domínio no território de outra Parte para obter informação que esteja na posse ou sob o controlo da entidade, com vista a identificar ou a contactar o titular de um nome de domínio.

2. Cada Parte adotará as medidas legislativas e outras que considere necessárias para permitir que uma entidade no seu território divulgue essa informação em resposta a um pedido apresentado ao abrigo do n.º 1, sujeito às condições razoáveis previstas no direito interno.

3. O pedido apresentado nos termos do n.º 1 deve incluir:

a. a data de emissão do pedido e a identidade e os dados de contacto da autoridade competente que emite o pedido;

b. o nome de domínio sobre o qual é solicitada a informação e uma lista pormenorizada da informação solicitada, incluindo os elementos de dados específicos;

c. uma declaração de que o pedido é emitido nos termos do presente Protocolo, 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; e

d. o prazo e o modo de divulgação da informação e quaisquer outras instruções processuais especiais.

4. Se for aceitável para a entidade, uma Parte poderá apresentar um pedido nos termos do n.º 1 em formato eletrónico, podendo ser necessário níveis apropriados de segurança e autenticação.

5. Em caso de não cooperação por parte de uma entidade descrita no n.º 1, a Parte requerente pode solicitar à entidade que explique a razão para não divulgar a informação solicitada. A Parte requerente poderá solicitar a consulta com a Parte na qual a entidade está localizada, a fim de determinar as medidas disponíveis para obter a informação.

6. No momento da assinatura do presente Protocolo ou aquando do depósito do seu instrumento de ratificação, aceitação ou aprovação, ou em qualquer outro momento, cada Parte comunicará ao Secretário-Geral do Conselho da Europa a autoridade designada para efeitos de consulta nos termos do n.º 5.

7. O Secretário-Geral do Conselho da Europa criará e manterá atualizado um registo das autoridades assim designadas pelas Partes nos termos do n.º 6. Cada Parte assegurará em permanência a exatidão dos dados fornecidos para o registo.

Artigo 7.º – Divulgação de informação sobre subscritores

1. Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para habilitar as respetivas autoridades competentes a emitir uma ordem que será diretamente apresentada a um fornecedor de serviços no território de outra Parte para obter a divulgação de informação específica e armazenada sobre subscritores na posse ou sob o controlo desse fornecedor de serviços, sempre que essa informação sobre o subscritor seja necessária para as investigações ou processos penais específicos da Parte emissora.

2. a. Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para que um fornecedor de serviços no seu território divulgue informação sobre subscritores em resposta a um pedido nos termos do n.º 1.

b. No momento da assinatura do presente Protocolo ou aquando do depósito do seu instrumento de ratificação, aceitação ou aprovação, uma Parte pode – no que diz respeito às ordens emitidas a fornecedores de serviços no seu território – realizar a seguinte declaração: "A ordem 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".

3. O ordem a que se refere o n.º 1 deve incluir:

a. a autoridade emissora e a data de emissão;

b. uma declaração de que a ordem é emitida nos termos do presente Protocolo;

c. o nome e o endereço do ou dos fornecedores de serviços a notificar;

d. a infração ou infrações que são objeto da investigação ou do processo penal;

e. a autoridade que solicita a informação específica sobre o subscritor, se não for a autoridade emissora; e

f. uma descrição pormenorizada da informação específica solicitada sobre o subscritor.

4. A ordem a que se refere o n.º 1 deve ser acompanhada pela seguinte informação suplementar:

a. os fundamentos jurídicos internos que habilitam a autoridade a emitir a ordem;

b. uma referência às disposições legais e às sanções aplicáveis à infração objeto de investigação ou de ação penal;

c. os dados de contacto da autoridade à qual o fornecedor de serviços deve devolver a informação sobre o subscritor, junto da qual pode solicitar informação complementar ou a quem deve responder de outra forma;

d. o prazo e o modo de devolução da informação sobre o subscritor;

e. se a preservação de dados já tiver sido solicitada, incluir a data de preservação e qualquer número de referência aplicável;

f. quaisquer instruções processuais especiais;

g. se aplicável, uma declaração de que se realizou a notificação simultânea nos termos do n.º 5; e

h. qualquer outra informação que possa ajudar a obter a divulgação da informação do subscritor.

5. a. Uma Parte pode, no momento da assinatura do presente Protocolo ou aquando do depósito do seu instrumento de ratificação, aceitação ou aprovação, e em qualquer outro momento, notificar o Secretário-Geral do Conselho da Europa de que, quando uma ordem é emitida nos termos do n.º 1 a um fornecedor de serviços no seu território, a Parte requer, em todos os casos ou em circunstâncias identificadas, a notificação simultânea da ordem, a informação suplementar e uma síntese dos factos relacionados com o inquérito ou o processo.

b. Independentemente de uma Parte exigir ou não a notificação nos termos do n.º 5, alínea a), poderá exigir que o fornecedor de serviços consulte as autoridades da Parte em circunstâncias identificadas antes da divulgação.

c. As autoridades notificadas nos termos do n.º 5., alínea a) ou consultadas nos termos do n.º 5, alínea b) poderão, sem demora indevida, dar instruções ao fornecedor de serviços para que não divulgue a informação sobre o subscritor se:

i. a divulgação puder prejudicar investigações ou processos penais nessa Parte; ou

ii. as condições ou motivos de recusa forem aplicáveis nos termos do artigo 25.º, n.º 4, e do artigo 27.º, n.º 4, da Convenção caso as informações sobre o subscritor tivessem sido solicitadas através da assistência mútua.

d. As autoridades notificadas nos termos do n.º 5, alínea a) ou consultadas nos termos do n.º 5, alínea b):

i. podem solicitar informação adicional à autoridade referida no n.º 4, alínea c), para efeitos da aplicação do n.º 5, alínea c), e não as deve divulgar ao fornecedor de serviços sem o consentimento dessa autoridade; e

ii. informarão imediatamente a autoridade referida no n.º 4, alínea c), caso o fornecedor de serviços tenha recebido instruções no sentido

de não divulgar a informação relativa ao subscritor, indicando as razões para tal.

e. Uma Parte designará uma única autoridade para receber a notificação nos termos do n.º 5, alínea a) e executará as ações descritas nos n.º 5, alínea b) e c) e n.º 5, alínea d. Nos termos do n.º 5, alínea a), a Parte deverá, no momento da primeira notificação ao Secretário-Geral do Conselho da Europa comunicar-lhe os dados de contacto dessa autoridade.

f. O Secretário-Geral do Conselho da Europa criará e manterá atualizado um registo das autoridades designadas pelas Partes e se estas requerem notificação nos termos do n.º 5, alínea a) e em que circunstâncias. Cada Parte assegurará em permanência a exatidão dos dados que fornece para o registo.

6. Se o fornecedor de serviços o aceitar, uma Parte pode apresentar uma ordem nos termos do n.º 1 e informação suplementar nos termos do n.º 4 em formato eletrónico. Uma Parte poderá apresentar a notificação e informação adicional nos termos do n.º 5 em formato eletrónico, podendo ser necessário níveis apropriados de segurança e autenticação.

7. Se um fornecedor de serviços informar a autoridade referida no n.º 4, alínea c), de que não divulgará a informação solicitada sobre o subscritor, ou se não divulgar a informação sobre o subscritor em resposta à ordem nos termos do n.º 1 no prazo de trinta (30) dias a contar da receção da ordem ou do prazo estipulado no n.º 4, alínea d), o que for mais longo, as autoridades competentes da Parte emissora podem solicitar a execução da ordem apenas através do artigo 8.º ou de outras formas de assistência mútua. As Partes poderão solicitar a um fornecedor de serviços que indique um motivo para recusar a divulgação da informação sobre o subscritor solicitada na ordem.

8. Uma Parte poderá, no momento da assinatura do presente Protocolo ou aquando do depósito do seu instrumento de ratificação, aceitação ou aprovação, declarar que a Parte emissora deve solicitar ao fornecedor de serviços a divulgação da informação sobre o subscritor antes de a solicitar ao abrigo do artigo 8.º, a menos que a Parte emissora forneça uma explicação razoável para não o ter realizado.

9. No momento da assinatura do presente Protocolo ou aquando do depósito do seu instrumento de ratificação, aceitação ou aprovação, uma Parte poderá:

a. reservar-se o direito de não aplicar o presente artigo; ou

b. 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, reservar-se o direito de não aplicar o presente artigo a esses números.

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

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

1. Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes a emitir uma ordem a apresentar no âmbito de um pedido a outra Parte com vista a obrigar um fornecedor de serviços no território da Parte requerida a apresentar [informação] específica e armazenada

a. sobre subscritores, e

b. dados de tráfego

na posse ou sob o controlo desse fornecedor de serviços que sejam necessários para as investigações ou processos penais específicos da Parte.

2. Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para dar execução a uma ordem nos termos do n.º 1 apresentada por uma Parte requerente.

3. No seu pedido, a Parte requerente apresenta a ordem nos termos do n.º 1, a informação de apoio e quaisquer instruções processuais especiais à Parte requerida.

a. A ordem deve especificar:
   i. a autoridade emissora e a data de emissão da ordem;
   ii. uma declaração de que a ordem é apresentada nos termos do presente Protocolo;
   iii. o nome e o endereço do ou dos fornecedores de serviços a notificar;
   iv. a infração ou infrações que são objeto da investigação ou do processo penal;
   v. a autoridade que solicita a informação ou os dados, se não for a autoridade emissora; e

vi. uma descrição pormenorizada da informação ou dos dados solicitados.

b. A informação de apoio, fornecida com o objetivo de ajudar a Parte requerida a executar a ordem e que não deverá ser divulgada ao fornecedor de serviços sem o consentimento da Parte requerente, deve especificar:

i. os fundamentos jurídicos internos que habilitam a autoridade a emitir a ordem;

ii. as disposições legais e as sanções aplicáveis à infração ou infrações objeto de investigação ou de ação penal;

iii. o motivo pelo qual a Parte requerente considera que o fornecedor de serviços está na posse ou controlo dos dados;

iv. uma síntese dos factos relacionados com a investigação ou o processo;

v. a pertinência da informação ou dos dados para a investigação ou o processo;

vi. os dados de contacto de uma autoridade ou autoridades que podem fornecer informação adicional;

vii. se a preservação de informação ou de dados já foi solicitada, incluindo a data de preservação e qualquer número de referência aplicável; e

viii. se a informação ou os dados já foram solicitados por outros meios e, em caso afirmativo, de que forma.

c. A Parte requerente poderá solicitar que a Parte requerida aplique instruções processuais especiais.

4. Uma Parte poderá declarar, no momento da assinatura do presente Protocolo ou aquando do depósito do seu instrumento de ratificação, aceitação ou aprovação, e em qualquer outro momento, que é necessária informação de apoio adicional para dar cumprimento às ordens previstas no n.º 1.

5. A Parte requerida aceitará os pedidos em formato eletrónico, podendo exigir níveis apropriados de segurança e autenticação antes de aceitar o pedido.

6. a. A partir da data de receção de toda a informação especificada nos n.º 3 e 4, a Parte requerida envidará todos os esforços razoáveis para notificar o fornecedor de serviços no prazo de quarenta e cinco (45) dias, se não antes, e ordenará a devolução da informação ou dos dados solicitados o mais tardar:

i. vinte (20) dias no caso de informação sobre subscritores; e

ii. quarenta e cinco (45) dias no caso dos dados de tráfego.

b. A Parte requerida assegurará a transmissão da informação ou dos dados produzidos à Parte requerente sem demora indevida.

7. Se a Parte requerida não puder cumprir as instruções previstas no n.º 3, alínea c), da forma solicitada, informará imediatamente a Parte requerente e, se for caso disso, especificará as condições em que poderá cumpri-las, após o que a Parte requerente determinará se o pedido deve, ainda assim, ser executado.

8. A Parte requerida poderá recusar a execução de um pedido pelos motivos estabelecidos no artigo 25.º, n.º 4, ou no artigo 27.º, n.º 4, da Convenção, ou poderá impor as condições que considere necessárias para permitir a execução do pedido. A Parte requerida poderá adiar a execução dos pedidos pelas razões estabelecidas nos termos do artigo 27.º, n.º 5, da Convenção. A Parte requerida notificará a Parte requerente logo que possível da recusa, das condições ou do adiamento. A Parte requerida notificará igualmente a Parte requerente de outras circunstâncias suscetíveis de atrasar significativamente a execução do pedido. O artigo 28.º, n.º 2, alínea b), da Convenção é aplicável ao presente artigo.

9. a. Se a 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.

b. 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.

10. No momento da assinatura do presente Protocolo ou aquando do depósito do seu instrumento de ratificação, aceitação ou aprovação, cada Parte comunicará ao Secretário-Geral do Conselho da Europa e manterá atualizados os dados de contacto das autoridades designadas:

a. para apresentar uma ordem nos termos do presente artigo; e

b. para receber uma ordem nos termos do presente artigo.

11. Uma Parte poderá, no momento da assinatura do presente Protocolo ou aquando do depósito do seu instrumento de ratificação, aceitação ou aprovação, declarar que, ao abrigo do presente artigo, exige que os pedidos de outras Partes lhe sejam apresentados pela autoridade central da Parte requerente

ou por qualquer outra autoridade que as Partes interessadas determinem de comum acordo.

12. O Secretário-Geral do Conselho da Europa criará e manterá atualizado um registo das autoridades assim designadas pelas Partes nos termos do n.º 10. Cada Parte assegurará em permanência a exatidão dos dados fornecidos para o registo.

13. No momento da assinatura do presente Protocolo ou aquando do depósito do seu instrumento de ratificação, aceitação ou aprovação, uma Parte poderá reservar-se o direito de não aplicar o presente artigo aos dados de tráfego.

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

1. a. Cada Parte adotará as medidas legislativas e de outra natureza que possam ser necessárias para que o seu ponto de contacto da rede 24/7 referido no artigo 35.º da Convenção ("ponto de contacto") possa, em caso de emergência, transmitir um pedido e receber um pedido de um ponto de contacto de outra Parte que procure assistência imediata para obter de um fornecedor de serviços no território dessa Parte a divulgação expedita de dados informáticos armazenados e especificados que estejam na posse ou sob o controlo desse fornecedor de serviços, sem um pedido de assistência mútua.

b. Uma Parte poderá, no momento da assinatura do presente Protocolo ou aquando do depósito do seu instrumento de ratificação, aceitação ou aprovação, declarar que não executará os pedidos ao abrigo do n.º 1, alínea a) que visem apenas a divulgação de informação sobre subscritores.

2. Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para permitir, nos termos do n.º 1:

a. que as suas autoridades recolham dados junto de um fornecedor de serviços no seu território, na sequência de um pedido apresentado nos termos do n.º 1;

b. que um fornecedor de serviços no seu território divulgue os dados solicitados às suas autoridades em resposta a um pedido apresentado ao abrigo do n.º 2, alínea a); e

c. que as suas autoridades disponibilizem os dados solicitados à Parte requerente.

3. O pedido a que se refere o n.º 1 deve incluir:

a. a autoridade competente que solicita os dados e a data em que o pedido foi emitido;

b. uma declaração de que o pedido é emitido nos termos do presente Protocolo;

c. o nome e o endereço do ou dos fornecedores na posse ou com o controlo dos dados solicitados;

d. a infração ou infrações que são objeto da investigação ou do processo penal e uma referência às suas disposições jurídicas e sanções aplicáveis;

e. factos suficientes para demonstrar a existência de uma situação de emergência e a forma como os dados solicitados lhe dizem respeito;

f. uma descrição pormenorizada dos dados solicitados;

g. quaisquer instruções processuais especiais; e

h. qualquer outra informação que possa ajudar a obter a divulgação dos dados solicitados.

4. A Parte requerida aceitará um pedido em formato eletrónico. Uma Parte poderá igualmente aceitar um pedido transmitido oralmente e requerer confirmação em formato eletrónico, podendo exigir níveis apropriados de segurança e autenticação antes de aceitar o pedido.

5. Uma Parte poderá, no momento da assinatura do presente Protocolo ou aquando do depósito do seu instrumento de ratificação, aceitação ou aprovação, declarar que, na sequência da execução do pedido, exige que as Partes requerentes apresentem o pedido e qualquer informação suplementar transmitida em seu apoio, num formato e através desse canal, que poderá incluir assistência mútua, conforme especificado pela Parte requerida.

6. A Parte requerida informará de forma rápida e expedita a Parte requerente da sua decisão sobre o pedido apresentado nos termos do n.º 1 e, se for o caso, especificará as condições nas quais disponibilizará os dados e quaisquer outras formas de cooperação que possam estar disponíveis.

7. a. Se uma Parte requerente não puder cumprir uma condição imposta pela Parte requerida nos termos do n.º 6, informará imediatamente a Parte requerida desse facto. A Parte requerida determinará então se a informação ou o material deverá, ainda assim, ser disponibilizado. Se a Parte requerente aceitar esta condição, ficará vinculada pela mesma.

b. 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.

Secção 4 – Procedimentos relativos à assistência mútua de emergência

Artigo 10.º – Assistência mútua de emergência

1. Cada Parte poderá solicitar assistência mútua de forma rápida e expedita, se considerar que existe uma situação de emergência. O pedido apresentado nos termos do presente artigo deverá incluir, para além dos outros elementos requeridos, uma descrição dos factos que demonstrem a existência de uma situação de emergência e da forma como a assistência solicitada lhe diz respeito.

2. Uma Parte requerida aceitará tal pedido em formato eletrónico, podendo exigir níveis apropriados de segurança e autenticação antes de aceitar o pedido.

3. A Parte requerida poderá solicitar de forma rápida e expedita informação suplementar para avaliar o pedido. A Parte requerente deverá fornecer essa informação suplementar de forma rápida e expedita.

4. Uma vez confirmada a existência de uma situação de emergência e de estarem preenchidos os demais requisitos para a assistência mútua, a Parte requerida deverá responder de forma rápida e expedita ao pedido.

5. Cada Parte assegurará que uma pessoa da sua autoridade central ou de outras autoridades responsáveis pela resposta a pedidos de assistência mútua está disponível vinte e quatro horas por dia, sete dias por semana, para dar resposta a um pedido ao abrigo do presente artigo.

6. A autoridade central ou outras autoridades responsáveis pela assistência mútua das Partes requerente e requerida poderão determinar de comum acordo que os resultados da execução de um pedido nos termos do presente artigo, ou uma cópia prévia dos mesmos, poderão ser disponibilizados à Parte requerente através de um canal diferente do utilizado para o pedido.

7. Na ausência de um tratado ou acordo de assistência mútua com base numa legislação uniforme ou recíproca em vigor entre a Parte requerente e a Parte requerida, o artigo 27.º, n.º 2, alínea b), e n.º 3 a n.º 8, e o artigo 28.º, n.º 2 a 4, da Convenção serão aplicáveis ao presente artigo.

8. Quando existir tal tratado ou acordo, o presente artigo será complementado pelas disposições desse tratado ou acordo, a menos que as Partes interessadas decidam por mútuo acordo aplicar, em seu lugar, alguma ou todas as disposições da Convenção referidas no n.º 7 do presente artigo.

9. Cada Parte poderá, no momento da assinatura do presente Protocolo ou no momento do depósito do seu instrumento de ratificação, aceitação ou aprovação, declarar que os pedidos também podem ser enviados diretamente às suas autoridades judiciais, por intermédio da Organização Internacional de Polícia Criminal (Interpol) ou ao seu ponto de contacto 24/7, criado nos termos do artigo 35.º da Convenção. Nesses casos, uma cópia será dirigida às autoridades centrais da Parte requerida por intermédio da autoridade central da Parte requerente. Quando um pedido for enviado diretamente a uma autoridade judicial da Parte requerida e essa autoridade não for competente para o tratar, transmiti-lo-á à autoridade nacional competente e informará diretamente a Parte requerente desse facto.

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

Artigo 11.º – Videoconferência

1. A Parte requerente poderá solicitar, e a Parte requerida poderá permitir que os depoimentos e declarações sejam obtidos de uma testemunha ou de um perito por videoconferência. A Parte requerente e a Parte requerida consultar-se-ão a fim de facilitar a resolução de quaisquer questões que possam surgir no que respeita à execução do pedido, incluindo, se for caso disso: qual a Parte que presidirá, as autoridades e pessoas que deverão estar presentes, se uma ou ambas as Partes administrarão juramentos, advertências ou instruções particulares à testemunha ou ao perito, a forma de interrogação da testemunha ou do perito, a forma como deverão garantir o devido respeito pelos direitos da testemunha ou do perito, o tratamento das reclamações de privilégio ou imunidade, o tratamento das objeções às perguntas ou respostas, e se uma ou ambas as Partes deverão disponibilizar serviços de tradução, de interpretação e de transcrição.

2. a. As autoridades centrais das Partes requerida e requerente devem comunicar diretamente entre si para efeitos do presente artigo. Uma Parte requerida poderá aceitar um pedido em formato eletrónico, podendo exigir níveis apropriados de segurança e autenticação antes de aceitar o pedido.

b. A Parte requerida informará a Parte requerente dos motivos da não execução ou do atraso da execução do pedido. O artigo 27.º, n.º 8, da Convenção é aplicável ao presente artigo. Sem prejuízo de qualquer outra condição que uma Parte requerida possa impor em conformidade com o presente artigo, é aplicável o artigo 28.º, n.º 2 a 4 da Convenção.

3. A Parte requerida que preste assistência ao abrigo do presente artigo envidará esforços para obter a presença da pessoa cujo depoimento ou declaração é solicitado. Quando apropriado, a Parte requerida poderá, na medida do possível e ao abrigo da sua legislação, tomar as medidas necessárias para obrigar uma testemunha ou um perito a comparecer na Parte requerida num determinado momento e local.

4. Os procedimentos relativos à realização da videoconferência especificados pela Parte requerente devem ser cumpridos, exceto em caso de incompatibilidade com a legislação interna da Parte requerida. Em caso de incompatibilidade ou na medida em que o procedimento não tenha sido especificado pela Parte requerente, a Parte requerida aplica o procedimento ao abrigo da sua legislação interna, salvo decisão mútua em contrário das Partes requerente e requerida.

5. Sem prejuízo de qualquer competência ao abrigo do direito interno da Parte requerente, quando, no decurso da videoconferência, a testemunha ou o perito:

a. prestar intencionalmente uma falsa declaração quando a Parte requerida o tiver obrigado a testemunhar com veracidade, em conformidade com a legislação interna da Parte requerida;

a. se recusar a testemunhar quando a Parte requerida o tiver obrigado a testemunhar, em conformidade com a legislação interna da Parte requerida; ou

c. cometer outras faltas que sejam proibidas pelo direito interno da Parte requerida no decurso desse procedimento;

esta poderá ser sancionada na Parte requerida do mesmo modo que se essa conduta tivesse sido cometida no decurso do seu procedimento interno.

6. a. Salvo decisão mútua em contrário entre a Parte requerente e a Parte requerida, a Parte requerida suportará todos os custos relacionados com a execução de um pedido ao abrigo do presente artigo, exceto:

i. os honorários de um perito que seja testemunha;

ii. os custos de tradução, interpretação e transcrição; e

iii. os custos de natureza extraordinária.

b. Se a execução de um pedido impuser custos extraordinários, a Parte requerente e a Parte requerida deverão consultar-se a fim de determinar as condições em que o pedido poderá ser executado.

7. Quando mutuamente acordado entre a Parte requerente e a Parte requerida:

a. as disposições do presente artigo poderão aplicar-se à realização de audioconferências;

b. a tecnologia de videoconferência poderá ser utilizada para fins, ou audiências, diferentes dos descritos no n.º 1, inclusive para efeitos de identificação de pessoas ou objetos.

8. Se a Parte requerida optar por permitir a audição de um suspeito ou arguido, poderá exigir condições e salvaguardas especiais no que diz respeito à obtenção de depoimentos ou declarações dessa pessoa, ou à entrega de notificações ou à aplicação de medidas processuais a essa pessoa.

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

1. De comum acordo, as autoridades competentes de duas ou mais Partes poderão instituir e operacionalizar uma equipa de investigação conjunta nos seus territórios, com vista a facilitar as investigações ou processos penais, sempre que se considere que uma coordenação reforçada é particularmente útil. As autoridades competentes serão determinadas pelas respetivas Partes interessadas.

2. 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.

3. Uma Parte poderá 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.

4. Essas autoridades competentes e participantes comunicarão diretamente, à exceção de as Partes poderem determinar por mútuo acordo outros canais de comunicação apropriados sempre que circunstâncias excecionais exigirem uma coordenação mais centralizada.

5. Quando for necessário adotar medidas de investigação no território de uma das Partes interessadas, as autoridades participantes dessa Parte poderão solicitar às suas próprias autoridades que tomem essas medidas sem que as outras Partes tenham de apresentar um pedido de assistência mútua. Essas medidas serão executadas pelas autoridades dessa Parte no seu território, nas condições aplicáveis ao abrigo do direito interno no âmbito de uma investigação nacional.

6. A utilização da informação ou dos elementos de prova fornecidos pelas autoridades participantes de uma Parte às autoridades participantes de outras Partes interessadas poderá ser recusada ou restringida nos termos do acordo descrito nos n.º 1 e 2. Se esse acordo não estabelecer condições para recusar ou restringir a utilização, as Partes poderão usar a informação ou os elementos de prova disponibilizados:

a. para os fins para os quais o acordo foi celebrado;

b. para a deteção, a investigação e a repressão de infrações penais diferentes daquelas para as quais o acordo foi celebrado, sujeito à autorização prévia das autoridades que disponibilizam a informação ou os elementos de prova. No entanto, a autorização não será exigida quando os princípios jurídicos fundamentais da Parte que utiliza a informação ou os elementos de prova exigirem que esta divulgue a informação ou os elementos de prova para proteger os direitos de uma pessoa acusada num processo penal. Nesse caso, essas autoridades deverão notificar sem demora indevida as autoridades que disponibilizaram a informação ou os elementos de prova; ou

c. para prevenir uma emergência. Nesse caso, as autoridades participantes que receberam a informação ou os elementos de prova notificam sem demora indevida as autoridades participantes que tenham disponibilizado a informação ou os elementos de prova, salvo em caso de mútuo acordo do contrário.

7. Na ausência de um acordo conforme descrito nos n.º 1 e 2, poderão realizar-se investigações conjuntas, caso a caso, em condições mutuamente

acordadas. Este 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 em causa.

Capítulo III – Condições e salvaguardas

Artigo 13º – Condições e salvaguardas

Em conformidade com o artigo 15.º da Convenção, 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.

Artigo 14.º – Proteção de dados pessoais

1. Âmbito

a. Salvo disposição em contrário prevista no n.º 1, alíneas b) e c), cada Parte tratará os dados pessoais que recebe ao abrigo do presente Protocolo em conformidade com os n.º 2 a 15 do presente artigo.

b. 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.º 2 a 15, exceto quando o contrário for mutuamente acordado pelas Partes interessadas.

c. Se a Parte que procede à transferência e a Parte recetora não estiverem mutuamente vinculadas ao abrigo de um acordo descrito no n.º 1, alínea b), poderão determinar mutuamente que a transferência de dados pessoais ao abrigo do presente Protocolo pode ter lugar com base noutros acordos ou convénios entre as Partes interessadas em substituição dos n.º 2 a 15.

d. Cada Parte considerará que o tratamento de dados pessoais nos termos do n.º 1, alíneas a) e b) cumpre os requisitos do seu quadro jurídico em matéria

de proteção de dados pessoais para as transferências internacionais de dados pessoais, não sendo necessária qualquer outra autorização de transferência ao abrigo desse quadro jurídico. Uma Parte só poderá recusar ou impedir transferências de dados para outra Parte ao abrigo do presente Protocolo por razões de proteção de dados: i) nas condições estabelecidas no n.º 15 quando for aplicável o n.º 1, alínea a), ou ii) nos termos de um acordo ou convénio referido no n.º 1, alíneas b) ou c), quando for aplicável um desses números.

e. Nenhuma disposição do presente artigo obstará a que uma Parte aplique salvaguardas mais rigorosas ao tratamento dos dados pessoais recebidos ao abrigo do presente Protocolo pelas suas próprias autoridades.

2. Finalidade e utilização

a. A Parte que tenha recebido dados pessoais procederá ao seu tratamento para os fins descritos no artigo 2.º. 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. O presente artigo não afetará a possibilidade de a Parte que procede à transferência impor condições adicionais nos termos do presente Protocolo num caso específico, todavia, essas condições não incluirão condições genéricas de proteção de dados.

b. 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.

3. Qualidade e integridade

Cada Parte adotará 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.

4. Dados sensíveis

O tratamento por uma Parte de 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, só poderá verificar-se mediante as salvaguardas apropriadas para evitar o risco de efeitos prejudiciais injustificados, decorrentes da utilização desses dados, em especial contra a discriminação ilegal.

5. Períodos de conservação

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 fim de cumprir esta obrigação, deverá prever no seu quadro jurídico interno, períodos de conservação específicos ou uma revisão periódica da necessidade de continuar a conservar os dados.

6. Decisões automatizadas

As decisões que produzam um efeito adverso significativo para os interesses relevantes da pessoa a quem se referem os dados pessoais não poderão basear-se exclusivamente no tratamento automatizado de dados pessoais, a menos que o direito interno o autorize e existam salvaguardas apropriadas que incluam a possibilidade de obter intervenção humana.

7. Segurança dos dados e incidentes de segurança

a. Cada Parte assegurará que dispõe de medidas tecnológicas, físicas e organizativas apropriadas para a proteção dos dados pessoais, em particular no que se refere à perda ou ao acesso, divulgação, alteração ou destruição acidental ou não autorizado ("incidente de segurança").

b. Após a deteção de um incidente de segurança em que exista um risco significativo de danos físicos ou não físicos para as pessoas ou para a outra Parte, a Parte recetora avaliará prontamente a probabilidade e a magnitude dos mesmos e adotará prontamente as medidas apropriadas para mitigar esses danos. Essas medidas incluirão a notificação à autoridade transmissora 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 poderá 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 perigo as medidas de proteção da segurança pública. Essas medidas incluirão igualmente a notificação da pessoa afetada, a menos que a Parte tenha tomado as medidas apropriadas para que deixe de existir um risco significativo. A notificação à pessoa em causa poderá ser adiada ou omitida nas condições estabelecidas no n.º 12, alínea a), ponto i. A Parte notificada poderá solicitar consultas e informação adicional sobre o incidente e a resposta ao mesmo.

c. No momento da assinatura do presente Protocolo ou aquando do depósito do seu instrumento de ratificação, aceitação ou aprovação, cada Parte comunicará ao Secretário-Geral do Conselho da Europa a autoridade ou autoridades

a notificar nos termos do n.º 7, alínea b) para efeitos do capítulo II, secção 2: a informação disponibilizada pode ser posteriormente alterada.

8. Manutenção de registos

Cada Parte manterá registos ou disporá de outros meios apropriados para demonstrar a forma como os dados pessoais de uma pessoa são acedidos, utilizados e divulgados num caso específico.

9. Partilha ulterior no seio de uma Parte

a. 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).

b. Não obstante o disposto no n.º 9, alínea a), uma Parte que tenha formulado uma reserva ao abrigo do artigo 17.º poderá disponibilizar dados pessoais que tenha recebido aos seus Estados constituintes ou a 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.

c. Em caso de indícios de uma aplicação indevida do presente número, a Parte que procede à transferência pode solicitar consultas e a informação pertinente sobre os referidos indícios.

10. Transferência ulterior para outro Estado ou organização internacional

a. A Parte recetora só poderá transferir os dados pessoais 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 nos termos do n.º 10, alínea b).

b. No momento da assinatura do presente Protocolo ou aquando do depósito do seu instrumento de ratificação, aceitação ou aprovação, cada Parte comunicará ao Secretário-Geral do Conselho da Europa a autoridade ou autoridades a conceder autorização para efeitos do capítulo II, secção 2; a informação disponibilizada pode ser posteriormente alterada.

11. Transparência e notificação

a. Cada Parte deverá notificar, através da publicação de avisos gerais ou de um aviso pessoal, a pessoa cujos dados pessoais tenham sido recolhidos, no que diz respeito:

i. ao fundamento jurídico e a finalidade ou finalidades do tratamento;

ii. quaisquer períodos de conservação ou revisão nos termos do n.º 5, consoante aplicável;

iii. os destinatários ou categorias de destinatários a quem esses dados são divulgados; e

iv. o acesso, retificação e recurso disponíveis.

b. Uma Parte poderá sujeitar qualquer requisito de notificação pessoal a restrições razoáveis ao abrigo do seu quadro jurídico interno, em conformidade com as condições estabelecidas no n.º 12, alínea a), ponto i).

c. 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, a Parte que procede à transferência adotará medidas para que a outra Parte seja informada no momento da transferência sobre este requisito e os dados de contacto apropriados. A notificação pessoal não será realizada se a outra Parte tiver solicitado que a disponibilização dos dados seja mantida confidencial, caso se apliquem as condições relativas às restrições previstas no n.º 12, alínea a), ponto i). Logo que essas restrições deixem de ser aplicáveis e a notificação pessoal possa ser realizada, a outra Parte adotará medidas para que a Parte que procede à transferência seja informada. 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.

12. Acesso e retificação

a. Cada Parte assegurará que qualquer pessoa cujos dados pessoais 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:

i. uma cópia escrita ou eletrónica da documentação conservada sobre essa pessoa que contenha os seus dados pessoais e a informação disponível, indicando a base jurídica e as finalidades do tratamento, os períodos de conservação e os destinatários ou as categorias de destinatários dos dados ("acesso"), bem como a informação relativa às opções de recurso disponíveis, desde que, num caso específico, o acesso possa estar sujeito à aplicação de restrições proporcionadas permitidas pelo seu quadro jurídico interno, 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;

ii. a retificação quando os dados pessoais da pessoa sejam inexatos ou tenham sido objeto de tratamento incorreto; a retificação deverá incluir – se apropriado e razoável tendo em conta os motivos da retificação e o contexto particular do tratamento – a correção, o aditamento, a eliminação ou a anonimização, a restrição do tratamento ou o bloqueio.

b. Se o acesso ou a retificação for negado ou restringido, 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. Deverá ainda indicar os motivos dessa recusa ou restrição e fornecer informação sobre as opções de recurso disponíveis. Quaisquer despesas incorridas para obter acesso devem limitar-se ao que seja razoável e não excessivo.

13. Recursos judiciais e extrajudiciais

Cada Parte deverá dispor de vias de recurso judiciais e extrajudiciais eficazes para proporcionar reparação pelas violações do presente artigo.

14. Supervisão

Cada Parte deverá dispor 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. As funções e os poderes dessas autoridades, agindo individual ou cumulativamente, incluirão poderes de investigação, o poder de dar seguimento a reclamações e a capacidade de tomar medidas corretivas.

15. Consulta e suspensão

Uma Parte poderá suspender a transferência de dados pessoais para outra Parte se dispuser de provas substanciais de que a outra Parte viola sistemática ou materialmente os termos do presente artigo ou de que está iminente uma violação material. 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. No entanto, uma Parte poderá suspender provisoriamente as transferências em caso de violação sistemática ou material que represente um risco significativo e iminente para a vida ou a segurança de uma pessoa singular ou um prejuízo substancial para a sua reputação ou situação económica, devendo, nesse caso, notificar e iniciar imediatamente consultas com a outra Parte. Se a consulta não tiver

conduzido a uma resolução, a outra Parte poderá suspender reciprocamente as transferências se dispuser de provas substanciais de que a suspensão pela Parte que suspende era contrária ao disposto no presente número. A Parte que suspende deverá levantar a suspensão logo que a infração que justifica a suspensão tenha sido corrigida; qualquer suspensão recíproca será levantada nesse momento. Os dados pessoais transferidos antes da suspensão continuarão a ser tratados em conformidade com o presente Protocolo.

Capítulo IV - Disposições finais

Artigo 15.º – Efeitos do presente protocolo

1. a. O artigo 39.º, n.º 2, da Convenção é aplicável ao presente Protocolo.

b. No que diz respeito às Partes que são membros da União Europeia, essas Partes poderão, nas suas relações mútuas, aplicar a legislação da União Europeia que rege as matérias abrangidas pelo presente Protocolo.

c. O n.º 1, alínea b), não afeta a plena aplicação do presente Protocolo entre as Partes que são membros da União Europeia e outras Partes.

2. O artigo 39.º, n.º 3, da Convenção é aplicável ao presente Protocolo.

Artigo 16° - Assinatura e entrada em vigor

1. O presente Protocolo estará aberto à assinatura das Partes na Convenção, as quais poderão expressar o seu consentimento em ficarem vinculadas por:

a. assinatura, sem reserva de ratificação, aceitação ou aprovação; ou

b. assinatura, sob reserva de ratificação, aceitação ou aprovação, seguida de ratificação, aceitação ou aprovação.

2. Os instrumentos de ratificação, aceitação ou aprovação serão depositados junto do Secretário-Geral do Conselho da Europa.

3. 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, em conformidade com as disposições dos n.º 1 e 2 deste artigo.

4. Em relação a qualquer Parte na Convenção que posteriormente exprima o seu consentimento em vincular-se ao presente Protocolo, este entrará em vigor no primeiro dia do mês seguinte ao termo de um período de três meses

após a data em que a Parte tenha expresso o seu consentimento em ficar vinculada pelo presente Protocolo, em conformidade com as disposições dos n.º 1 e 2 deste artigo.

Artigo 17.º – Cláusula federal

1. Um Estado federal pode reservar-se o direito de assumir as obrigações nos termos do presente Protocolo na medida em que sejam compatíveis com os princípios fundamentais que governam as relações entre o seu governo central e os Estados federados, ou outras entidades territoriais análogas, desde que:

a. o Protocolo se aplique ao governo central do Estado federal;

b. essa reserva não afete as obrigações de cooperação pretendida por outras Partes em conformidade com as disposições do capítulo II; e

c. as disposições do artigo 13.º sejam aplicáveis aos Estados que constituem o Estado federal ou a outras entidades territoriais similares.

2. Uma outra Parte poderá impedir as autoridades, fornecedores ou entidades no seu território de cooperarem em resposta a um pedido ou ordem apresentado diretamente pelo Estado constituinte ou outra entidade territorial similar de um Estado federal que tenha formulado uma reserva nos termos do n.º 1, salvo se esse Estado federal notificar 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. O Secretário-Geral do Conselho da Europa criará e manterá atualizado um registo dessas notificações.

3. Outra Parte não impedirá que as autoridades, fornecedores ou entidades no seu território cooperem com um Estado constituinte ou outra entidade territorial similar com base numa reserva nos termos do n.º 1, se tiver sido apresentada uma ordem ou um pedido através do governo central ou de um acordo da equipa de investigação conjunta nos termos do artigo 12.º com a participação do governo central. Nessas situações, o governo central deverá prever o cumprimento das obrigações aplicáveis do Protocolo, desde que, no que respeita à proteção dos dados pessoais disponibilizados aos Estados constituintes ou a entidades territoriais similares, apenas sejam aplicáveis os termos do artigo 14.º, n.º 9, ou, se aplicável, os termos de um acordo ou convénio descrito no artigo 14.º, n.º 1, alínea b) ou c).

4. No que se refere às disposições do presente Protocolo, cuja execução seja da competência legislativa dos Estados federados ou de outras entidades territoriais análogas que não são, nos termos do sistema constitucional da federação obrigados a tomar medidas legislativas, o governo central levará com parecer favorável as referidas disposições ao conhecimento das autoridades competentes dos Estados federais incitando-os a adotar as medidas adequadas para as executar.

Artigo 18° – Aplicação territorial

1. O presente Protocolo será aplicável ao território ou territórios especificados numa declaração realizada por uma Parte nos termos do artigo 38.º, n.º 1 ou 2, da Convenção, na medida em que essa declaração não tenha sido levantada nos termos do artigo 38.º, n.º 3.

2. 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.

3. Uma declaração nos termos do n.º 2 do presente artigo poderá ser levantada, no que diz respeito a qualquer território indicado na declaração, mediante notificação dirigida ao Secretário-Geral do Conselho da Europa. Esse levantamento produzirá efeitos no primeiro dia do mês seguinte ao termo de um período de três meses após a data de receção da referida notificação pelo Secretário-Geral.

Artigo 19° - Reservas e declarações

1. Mediante notificação escrita dirigida ao Secretário-Geral do Conselho da Europa, qualquer Parte na Convenção poderá, no momento da assinatura deste Protocolo ou do depósito do seu instrumento de ratificação, aceitação ou aprovação, declarar que se fará prevalecer da reserva ou das reservas previstas no artigo 7°, n.º 9, alíneas a) e b), no artigo 8.º, n.º 13 e no artigo 17.º do presente Protocolo. Nenhuma outra reserva poderá ser formulada.

2. Mediante notificação escrita dirigida ao Secretário-Geral do Conselho da Europa, qualquer Parte na Convenção poderá, no momento da assinatura deste Protocolo ou do depósito do seu instrumento de ratificação, aceitação ou aprovação, realizar a declaração ou declarações indicadas no artigo 7.º, n.º 2, alínea b) e n.º 8, no artigo 8.º, n.º 11, no artigo 9.º, n.º1, alínea b) e n.º 5,

no artigo 10.º, n.º 9, alínea b), no artigo 12.º, n.º 3, e no artigo 18.º, n.º 2 do presente Protocolo.

3. Por notificação escrita dirigida ao Secretário-Geral do Conselho da Europa, qualquer Parte na Convenção fará qualquer declaração ou declarações, notificações ou comunicações identificadas no artigo 7.º, n.º 5, alíneas a) e e), no artigo 8.º, n.º 4 e 10, alínea 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 nele especificados.

Artigo 20.º – Estatuto e levantamento de reservas

1. A Parte que tenha formulado uma reserva em conformidade com o artigo 19.°, n.º 1, poderá levantá-la no todo ou em parte, logo que as circunstâncias o permitam. Esse levantamento produzirá efeito na data de receção de uma notificação dirigida ao Secretário-Geral do Conselho da Europa. Se a notificação indicar que o levantamento da reserva deve produzir efeitos numa data precisa e essa data for posterior à da receção da notificação pelo Secretário-Geral, o levantamento produz efeitos nessa data posterior.

2. O Secretário-Geral do Conselho da Europa pode solicitar, periodicamente, às Partes que formularam uma ou mais reservas no termos do artigo 19.°, n.º 1, informações sobre as perspetivas de levantamento dessa ou dessas reservas.

Artigo 21.º – Aditamentos

1. Quaisquer aditamentos ao presente Protocolo podem ser propostos por qualquer uma das Partes no Protocolo e serão comunicados pelo Secretário-Geral do Conselho da Europa aos Estados-Membros do Conselho da Europa e às Partes e signatários na Convenção, bem como a qualquer Estado que tenha sido convidado a aderir à Convenção.

2. Qualquer aditamento proposto por uma Parte deve ser comunicado ao Comité Europeu para os Problemas Criminais (CDPC), que submeterá ao Comité de Ministros o seu parecer relativamente ao aditamento proposto.

3. O Comité de Ministros avaliará o aditamento proposto e o parecer apresentado pelo Comité Europeu para os Problemas Criminais (CDPC) e, após consulta das Partes na presente Convenção, poderá adotar o referido aditamento.

4. O texto de qualquer aditamento adotado pelo Comité de Ministros em conformidade com o n.º 3 será comunicado às Partes no presente Protocolo para aceitação.

5. Qualquer aditamento adotado em conformidade com o n.º 3 entrará em vigor no trigésimo dia após todas Partes no Protocolo terem informado o Secretário-Geral acerca da sua aceitação.

Artigo 22.º – Resolução de litígios

O artigo 45.º da Convenção é aplicável ao presente Protocolo.

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

1. O artigo 46.º da Convenção é aplicável ao presente Protocolo.

2. As Partes avaliarão periodicamente a utilização e aplicação efetivas das disposições do presente Protocolo. O artigo 2.º do Regulamento Interno do Comité da Convenção sobre Cibercrime, revisto em 16 de outubro de 2020 aplica-se, *mutatis mutandis*. As Partes deverão rever inicialmente e poderão alterar por consenso os procedimentos desse artigo aplicáveis ao presente Protocolo cinco anos após a entrada em vigor do presente Protocolo.

3. A revisão 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

1. Qualquer Parte poderá, a qualquer momento, denunciar o presente Protocolo mediante notificação enviada ao Secretário-Geral do Conselho da Europa.

2. A denúncia produzirá efeitos no primeiro dia do mês seguinte ao termo de um período de três meses após a data de receção da notificação pelo Secretário-Geral.

3. A denúncia da Convenção por uma Parte no presente Protocolo constitui uma denúncia do presente Protocolo.

4. A informação ou elementos de prova transferidos antes da data efetiva da denúncia continuarão a ser tratados em conformidade com o presente Protocolo.

Artigo 25.º – Notificação

O Secretário-Geral do Conselho da Europa notificará os Estados-Membros do Conselho da Europa, as Partes e os signatários da Convenção, bem como qualquer Estado que tenha sido convidado a aderir à presente Convenção de:

a. qualquer assinatura;

b. o depósito de qualquer instrumento de ratificação, aceitação ou aprovação;

c. qualquer data de entrada em vigor do presente Protocolo em conformidade com o artigo 16°, n.º 3 e 4;

d. todas as declarações ou reservas formuladas em conformidade com o artigo 19.º ou o levantamento de reservas formuladas em conformidade com o artigo 20.º;

e. qualquer outro ato, notificação ou comunicação relacionado com o presente Protocolo.

Relatório explicativo do segundo protocolo adicional

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

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".

Notas de orientação

En su 8ª reunión plenaria (diciembre de 2012), el Comité del Convenio sobre la ciberdelincuencia (T-CY) decidió emitir notas de orientación destinadas a facilitar la utilización y la aplicación efectivas del Convenio de Budapest sobre la ciberdelincuencia, teniendo en cuenta las novedades jurídicas, políticas y técnicas.[15]

Las notas de orientación reflejan el entendimiento común entre las Partes con respecto al uso del Convenio.

El Convenio de Budapest "utiliza un lenguaje neutro en cuanto a la tecnología de manera tal que los delitos contemplados en el derecho penal puedan aplicarse tanto a las tecnologías actuales como a las futuras".[16] El propósito es asegurar que las nuevas formas de delincuencia queden siempre cubiertas por el Convenio.

15. Véase el mandato del T-CY (artículo 46 del Convenio de Budapest).
16. Párrafo 36 del Informe explicativo

Nota de orientação sobre a noção de "sistema informático"[17]

Artigo 1.a da Convenção de Budapeste sobre o Cibercrime

1. Introdução

Na sua 1ª reunião em Estrasburgo, nos dias 20 e 21 de março de 2006, o T-CY debateu o alcance da expressão "sistema informático", tal como se encontra definida no artigo 1.a da Convenção de Budapeste, tendo em conta as novas formas de tecnologia, que vão para além dos simples computadores de escritório ou computadores centrais tradicionais.

Desde a altura em que a Convenção foi redigida, apareceram novos dispositivos, nomeadamente a geração moderna de telemóveis ou "smartphones", assistentes digitais pessoais (PDA), tablets e outros que permitem produzir, tratar ou transmitir dados. Daí a necessidade de ver se a noção de "sistema informático" que a Convenção de Budapeste utiliza cobre estes novos dispositivos.

O T-CY decidiu, em 2006, que os dispositivos em questão estavam cobertos pela definição de "sistema informático" que figura no artigo 1.a da Convenção.

A presente nota de orientação baseia-se neste entendimento comum das Partes, tal como refletido no relatório da 1ª reunião (documento T-CY(2006)11).

2. Artigo 1.a da Convenção de Budapeste sobre o Cibercrime (STE 185)

Texto da Convenção

Artigo 1º –Definições

Para efeitos da presente Convenção:

a "sistema informático" significa qualquer dispositivo isolado ou conjunto de dispositivos interconectados ou relacionados entre si, sendo que um ou vários desses dispositivos asseguram, em execução de um programa, o tratamento automatizado de dados;

Extrato do Relatório Explicativo

> 23. Um sistema informático, nos termos a que se refere a Convenção, é um equipamento composto por hardware e software desenvolvidos para o tratamento

17. Adotada pelo T-CY, na sua 8ª reunião plenária

automático de dados digitais. Poderá incluir dispositivos de entrada, saída e armazenamento. Poderá funcionar independentemente ou estar ligado em rede com outros dispositivos semelhantes. O termo "Automático" significa sem a intervenção direta do Homem e a expressão "tratamento de dados" significa que os dados no sistema informático são operados através da execução de um programa de computador. Um "programa de computador" é um conjunto de instruções passíveis de serem executadas pelo computador para obter o resultado pretendido. Um computador pode executar diferentes programas. Um sistema informático é, normalmente, composto por vários dispositivos, distinguindo-se o processador ou unidade central de processamento e os periféricos. Um "periférico" consiste num aparelho que desempenha determinadas funções específicas em interação com a unidade de processamento, tal como uma impressora, um monitor de vídeo, um leitor/gravador de CD ou outro dispositivo de armazenamento.

24. Uma rede é uma interligação entre dois ou mais sistemas informáticos. As ligações podem ser de terra (por exemplo, fio ou cabo), sem fio (por exemplo, rádio, infravermelhos, ou satélite) ou ambas. Uma rede poderá ser geograficamente limitada a uma pequena área (rede de área local - LAN) ou cobrir uma vasta área (rede de área alargada - WAN), podendo estas redes estar interligadas entre si. A Internet é uma rede global composta por muitas redes interligadas, sendo que todas usam os mesmos protocolos. Existem outros tipos de redes, ligadas ou não à Internet, que permitem comunicar dados entre sistemas informáticos. Estes sistemas informáticos podem estar conectados à rede como terminais de saída ou como um meio de facilitar a comunicação na rede. O importante é que os dados sejam permutados através da rede.

3. Declaração do T-CY sobre a noção de "sistema informático" (Artigo 1.a da Convenção de Budapeste)

O artigo 1.a da Convenção define um "sistema informático" como "qualquer dispositivo isolado ou conjunto de dispositivos interconectados ou relacionados entre si, sendo que um ou vários desses dispositivos asseguram, em execução de um programa, o tratamento automatizado de dados".

O T-CY considera que esta definição engloba, por exemplo, os telemóveis modernos, que são aparelhos multifuncionais, capazes de produzir, tratar e transmitir dados, incluindo as suas múltiplas funções, nomeadamente, aceder à Internet, enviar correio eletrónico, transmitir anexos, carregar conteúdos ou descarregar documentos.

O T-CY tem igualmente consciência de que os assistentes digitais pessoais, quer sejam ou não dotados de funcionalidade sem fios, também produzem, tratam e transmitem dados.

O T-CY sublinha que, quando estes dispositivos executam tais funções, tratam "dados informáticos", tal como definidos no artigo 1.b. Além disso, o T-CY considera que eles geram também, ao fazê-lo, "dados relativos ao tráfego", no sentido do artigo 1.d.

Visto terem a capacidade para processar tais dados, estes dispositivos comportam-se como um "sistema informático", tal como definido no artigo 1.a.

O T-CY considera que esta aceção corresponde à interpretação de "sistema informático" contida no Relatório Explicativo da Convenção e que esta visa abranger estes dispositivos nessa capacidade.

Conclusão

O T-CY considera que a definição de "sistema informático" que figura no artigo 1.a cobre as novas formas de tecnologia que vão para além dos simples computadores de escritório ou computadores centrais tradicionais, tais como os telemóveis modernos, os smartphones, os assistentes digitais pessoais e os tablets ou dispositivos similares.

Nota de orientação sobre as disposições da Convenção de Budapeste cobrindo os botnets[18]

Introdução

Na sua 8ª reunião plenária (dezembro de 2012), o Comité da Convenção sobre o Cibercrime (T-CY) decidiu emitir notas de orientação visando facilitar a utilização e implementação efetivas da Convenção de Budapeste sobre o Cibercrime, nomeadamente à luz dos desenvolvimentos jurídicos, políticos e tecnológicos.[19]

As notas de orientação refletem uma análise da aplicação da Convenção de Budapeste comum a todas as suas Partes.

A presente nota trata das questões dos botnets.

A Convenção de Budapeste "recorre a uma linguagem neutra em termos tecnológicos, de modo a que as infrações definidas ao abrigo do direito penal substantivo possam ser aplicáveis quer às tecnologias atuais quer às tecnologias futuras envolvidas".[20] Isto serve para assegurar que as novas formas de malware ou infrações sejam sempre cobertas pela Convenção.

Esta Nota de orientação mostra em que medida diferentes artigos da Convenção se aplicam aos botnets.

Disposições relevantes da Convenção de Budapeste sobre o Cibercrime (STE 185)

O termo "botnet" pode designar:

> "uma rede de computadores que foram contaminados por software malicioso (vírus informáticos). Uma tal rede de computadores comprometidos ("zombies") pode ser ativada para executar certas ações, tais como atacar sistemas informáticos (ciberataques). Estes "zombies" podem ser controlados, muitas vezes sem o conhecimento dos utilizadores dos computadores comprometidos, por outro computador, também conhecido como 'centro de comando e de controlo'".[21]

18. Adotada pela 9ª reunião plenária do T-CY (4-5 junho 2013)
19. Ver o mandato do T-CY (Artigo 46º da Convenção de Budapeste).
20. Parágrafo 36 do Relatório Explicativo
21. Proposta de diretiva do Parlamento Europeu e do Conselho relativa aos ataques contra os sistemas informáticos e revogando a decisão-quadro do Conselho 2005/222/JHA (com (2010) 517 final)

Os computadores podem ser interligados para fins criminosos ou para boas causas.[22] O facto de estes botnets serem constituídos por computadores interligados não é portanto relevante. O elemento essencial é que os computadores dos botnets são utilizados sem autorização, para fins criminosos e para causar um impacto considerável.

Os botnets são visados pelas seguintes secções da Convenção, em função da ação precisa que executam. Cada disposição contém um critério de intenção ("sem autorização", "sem intenção fraudulenta", etc.) que deverá ser de fácil prova em presença dos botnets.

Artigos relevantes	**Exemplos**
Artigo 2º – Acesso ilegítimo	A criação e operação de um botnet requerem o acesso ilegítimo a sistemas informáticos.[23] Os botnets podem servir para aceder ilegalmente a outros sistemas informáticos.
Artigo 3º – Interceção ilegítima	Os botnets podem utilizar meios técnicos para intercetar transmissões não públicas de dados informáticos para, de ou dentro de um sistema informático.
Artigo 4º – Interferência em dados	A criação de um botnet altera sempre e pode danificar, eliminar, deteriorar ou suprimir dados informáticos. Os próprios botnets danificam, eliminam, deterioram, alteram ou suprimem dados informáticos.
Artigo 5º – Interferência em sistemas	Os botnets podem entravar o funcionamento de um sistema informático, nomeadamente através de ataques por negação de serviço distribuído.[24]

22. Redes de computadores podem ser criadas voluntariamente para fins criminosos. As infrações cometidas por estas redes são cobertas pela Convenção, mas não são discutidas nesta Nota.
23. Ver também a Nota de orientação nº 1 sobre a noção de "sistema informático"
24. Ver a nota de orientação separada.

Artigos relevantes	Exemplos
Artigo 6º – Uso indevido de dispositivos	Os botnets são todos dispositivos abrangidos pela definição que consta do artigo 6º, pois são concebidos ou adaptados essencialmente para cometer as infrações previstas nos artigos 2º a 5º.[25] Os próprios programas utilizados para criar e operar os botnets entram assim no campo do artigo 6º. Consequentemente, o artigo 6º tipifica como infração penal a produção, a venda, a obtenção para utilização, a importação, a distribuição, ou outras formas de disponibilização ou posse de dispositivos, tais como os botnets ou os programas utilizados para a sua criação ou operação.
Artigo 7º – Falsidade informática	Segundo a forma como tenha sido concebido, o botnet pode introduzir, alterar, eliminar ou suprimir dados informáticos, resultando em dados não autênticos, com o intuito de que tais dados sejam considerados ou utilizados para fins legais como se fossem autênticos.
Artigo 8º – Burla informática	Os botnets podem causar a perda de bens a uma pessoa e permitir a uma outra pessoa obter um benefício económico mediante a introdução, alteração, eliminação ou supressão de dados informáticos e/ou a interferência no funcionamento de um sistema informático.
Artigo 9º – Pornografia infantil	Os botnets podem distribuir materiais resultantes da exploração de crianças.
Artigo 10º – Infrações penais relacionadas com a violação do direito de autor e dos direitos conexos	Os botnets podem distribuir ilicitamente dados protegidos por leis relativas à propriedade intelectual.
Artigo 11º – Tentativa e cumplicidade	Os botnets podem ser utilizados para tentar cometer várias das infrações especificadas no tratado ou para ser cúmplice na sua prática.

25. As Partes que emitam reservas relativamente ao artigo 6º devem no entanto criminalizar a venda, distribuição ou disponibilização dos dispositivos cobertos por este artigo.

Artigos relevantes	Exemplos
Artigo 13º – Sanções	Os botnets servem para fins criminosos múltiplos, alguns dos quais se revestem de gravidade para as pessoas, as instituições públicas ou privadas ou as infraestruturas críticas. É contudo possível que as sanções previstas pela legislação nacional de algumas Partes em casos de infrações ligadas aos botnets sejam demasiado brandas e não permitam tomar em consideração as circunstâncias agravantes, a tentativa ou a cumplicidade. Poderá, assim, ser eventualmente necessário que estas Partes considerem a revisão da sua legislação. Nos termos do artigo 13º, as Partes deverão portanto assegurar que as infrações penais relacionadas com os botnets "sejam passíveis de sanções eficazes, proporcionais e dissuasivas, incluindo as penas privativas de liberdade". Para as pessoas coletivas, poderão ser aplicadas sanções penais ou não penais, incluindo as sanções pecuniárias. As Partes podem igualmente tomar em consideração as circunstâncias agravantes, por exemplo se os botnets afetarem um número significativo de sistemas ou os ataques causarem danos consideráveis, incluindo mortes ou ferimentos ou danos a infraestruturas críticas.

Declaração do T-CY

A lista de artigos relacionados com os botnets apresentada acima ilustra as múltiplas infrações que podem ser cometidas por meio dos botnets e as disposições penais que poderão aplicar-se.

Portanto, o T-CY pode afirmar que os botnets, sob os seus diferentes aspetos, estão cobertos pela Convenção de Budapeste.

Nota de orientação sobre ataques DDOS[26]

Introdução

Na sua 8ª reunião plenária (dezembro de 2012), o Comité da Convenção sobre o Cibercrime (T-CY) decidiu emitir notas de orientação visando facilitar a utilização e implementação efetivas da Convenção de Budapeste sobre o Cibercrime, nomeadamente à luz dos desenvolvimentos jurídicos, políticos e tecnológicos.[27]

As notas de orientação refletem uma análise da aplicação da Convenção de Budapeste comum a todas as suas Partes.

A presente nota aborda a questão dos ataques por negação de serviço (DOS) e por negação de serviço distribuído (DDOS).

A Convenção de Budapeste "recorre a uma linguagem neutra em termos tecnológicos, de modo a que as infrações definidas ao abrigo do direito penal substantivo possam ser aplicáveis quer às tecnologias atuais quer às tecnologias futuras envolvidas".[28] Isto serve para assegurar que as novas formas de malware ou crime sejam sempre cobertas pela Convenção.

Esta Nota de orientação mostra em que medida diferentes artigos da Convenção se aplicam aos ataques DOS e DDOS.

Disposições relevantes da Convenção de Budapeste sobre o Cibercrime (STE 185)

Os ataques por negação de serviço (DOS) visam tornar um sistema informático indisponível para os seus utilizadores por diversos meios, que podem incluir a saturação dos computadores ou redes alvo com pedidos de comunicação externos, tornando assim lento o acesso ao serviço pelos utilizadores legítimos. Os ataques por negação de serviço distribuído (DDOS) são executados por vários computadores em simultâneo. Existem atualmente várias maneiras comuns de lançar ataques DOS e DDOS, por exemplo enviando pedidos incorretos a um sistema informático; ultrapassando o número máximo de utilizadores; e enviando mais mensagens de correio eletrónico para os servidores do que o sistema consegue receber e tratar.

26. Adotada na 9ª Reunião plenária do T-CY (4-5 junho 2013)
27. Ver o mandato do T-CY (Artigo 46º da Convenção de Budapeste).
28. Parágrafo 36 do Relatório Explicativo

Os ataques DOS e DDOS são cobertos pelas seguintes secções da Convenção, em função do efeito prático de cada ataque. Cada disposição contém um critério de intenção ("sem autorização", "com intenção fraudulenta", etc.) que deve ser fácil de provar em casos de ataques DOS e DDOS.

Interpretação pelo T-CY da criminalização dos ataques DDOS

Artigos relevantes	**Exemplos**
Artigo 2º – Acesso ilegítimo	Um sistema informático pode ser acedido através de ataques DOS e DDOS.
Artigo 4º – Interferência em dados	Os ataques DOS e DDOS podem danificar, eliminar, deteriorar, alterar ou suprimir dados informáticos.
Artigo 5º – Interferência em sistemas	O objetivo de um ataque DOS ou DDOS é precisamente entravar gravemente o funcionamento de um sistema informático.
Artigo 11º – Tentativa e cumplicidade	Os ataques DOS e DDOS podem ser utilizados para cometer várias das infrações especificadas na Convenção ou para se tornar cúmplice da sua prática (tais como falsidade informática, artigo 7º; burla informática, artigo 8º; infrações penais relacionadas com pornografia infantil, artigo 9º; e infrações penais relacionadas com a violação dos direitos de autor e dos direitos relacionados, artigo 10º).
Artigo 13º – Sanções	Os ataques DOS e DDOS podem ser perigosos de muitas maneiras, especialmente quando são dirigidos contra sistemas que são cruciais para a vida do dia-a-dia – por exemplo se os sistemas bancário ou hospitalar ficarem indisponíveis. É contudo possível que as sanções previstas pela legislação nacional de algumas Partes em casos de ataques DOS e DDOS sejam demasiado brandas e não permitam tomar em consideração as circunstâncias agravantes, a tentativa ou a cumplicidade. Poderá, assim, ser eventualmente necessário que estas Partes considerem a revisão da sua legislação. Nos termos do artigo 13º, as Partes deverão portanto assegurar que as infrações penais relacionadas com tais ataques "sejam passíveis de sanções eficazes, proporcionais e dissuasivas, incluindo as penas privativas de liberdade". Para as pessoas coletivas, poderão ser aplicadas sanções penais ou não penais, incluindo as sanções pecuniárias.

	As Partes podem igualmente tomar em consideração as circunstâncias agravantes, por exemplo se os ataques DOS e DDOS afetarem um número significativo de sistemas ou causarem danos consideráveis, incluindo mortes ou ferimentos ou danos a infraestruturas críticas.

Declaração do T-CY

A lista de artigos relacionados com ataques DOS e DDOS apresentada acima ilustra as múltiplas infrações que podem ser cometidas por meio destes ataques.

Portanto, o T-CY pode afirmar que os diferentes aspetos de tais ataques estão cobertos pela Convenção de Budapeste.

Nota de orientação sobre a fraude por usurpação de identidade e phishing[29]

Introdução

Na sua 8ª reunião plenária (dezembro de 2012), o Comité da Convenção sobre o Cibercrime (T-CY) decidiu emitir notas de orientação visando facilitar a utilização e implementação efetivas da Convenção de Budapeste sobre o Cibercrime, nomeadamente à luz dos desenvolvimentos jurídicos, políticos e tecnológicos.[30]

As notas de orientação refletem uma análise da aplicação da Convenção de Budapeste comum a todas as suas Partes.

A presente nota trata da questão da fraude por usurpação de identidade e phishing e por práticas similares[31].

A Convenção de Budapeste "recorre a uma linguagem neutra em termos tecnológicos, de modo a que as infrações definidas ao abrigo do direito penal substantivo possam ser aplicáveis quer às tecnologias atuais quer às tecnologias futuras envolvidas".[32] Isto serve para assegurar que as novas formas de crime sejam sempre cobertas pela Convenção

Esta Nota de orientação mostra em que medida diferentes artigos da Convenção se aplicam à usurpação de identidade por via informática e relacionada com a fraude.

Usurpação de identidade e phishing

Embora não exista uma definição universalmente aceite nem uma utilização consistente desta expressão, a "usurpação de identidade" envolve geralmente infrações penais que consistem em obter e utilizar de forma fraudulenta os dados de identidade de outra pessoa (sem o seu conhecimento ou consentimento). A expressão "fraude de identidade" é por vezes utilizada como sinónimo, embora englobe igualmente a utilização de uma identidade falsa, que não é necessariamente real.

---

29. Adotada na 9ª Reunião plenária do T-CY (4-5 junho 2013).
30. Ver o mandato do T-CY (Artigo 46º da Convenção de Budapeste).
31. Estas práticas são conhecidas por nomes diversos, tais como spear phishing, SMiShing, pharming e vishing.
32. Parágrafo 36 do Relatório Explicativo

Embora os dados de identificação pessoal de uma pessoa real ou fictícia possam ser utilizados abusivamente para vários atos ilícitos, a presente nota de orientação concentra-se apenas na usurpação de identidade relacionada com a fraude.

Isto pode implicar a apropriação fraudulenta de dados relativos à identidade (tais como o nome, data de nascimento, endereço atual, endereços anteriores) de outra pessoa, sem o seu conhecimento ou consentimento. Estes dados de identificação pessoal são em seguida utilizados para obter bens e serviços no nome dessa pessoa.

Atos similares podem assumir formas diversas, como o "phishing", "pharming", "spear phishing", "spoofing" ou qualquer conduta análoga visando, por exemplo, obter uma palavra-passe ou outros códigos de acesso, frequentemente através de mensagens de correio eletrónico ou sítios web falsos.

A usurpação de identidade é um verdadeiro flagelo que afeta governos, empresas e cidadãos. Este fenómeno mina a confiança nas tecnologias da informação.

A maioria dos sistemas jurídicos não preveem o delito específico de usurpação de identidade. Os autores da usurpação de identidade são normalmente acusados de crimes mais graves (como a fraude financeira). A obtenção de uma identidade falsa implica normalmente a prática de uma infração, tal como a falsificação de documentos ou a alteração de dados informáticos. Uma identidade falsa facilita a prática de muitos crimes, incluindo a imigração ilegal, o tráfico de seres humanos, o branqueamento de capitais, o tráfico de drogas, a fraude financeira contra os governos e o setor privado, mas é mais geralmente associada à fraude.

No plano conceptual, a usurpação de identidade pode dividir-se em três fases distintas:

- Fase 1 – A obtenção de dados de identidade, por meios diversos como o roubo físico, a utilização de motores de busca, ataques do interior ou do exterior (acesso ilícito a sistemas informáticos, trojans, keyloggers, spyware e outro malware) ou recorrendo ao phishing e/ou a outras técnicas de engenharia social.
- Fase 2 – A posse e a cessão de dados de identidade, incluindo a venda destes dados a terceiros.
- Fase 3 – A utilização de dados de identidade para cometer fraude ou outras infrações, por exemplo assumindo a identidade de outra pessoa

para explorar contas bancárias e cartões de crédito, abrir novas contas, contrair empréstimos e créditos, encomendar bens e serviços ou distribuir malware.

Em conclusão: a usurpação de identidade (incluindo o phishing e condutas similares) serve geralmente para a preparação de novos atos criminosos, tais como a fraude informática. Mesmo que a usurpação de identidade não seja tipificada como infração penal em si, as autoridades competentes para a aplicação da lei poderão processar as infrações penais associadas.

Interpretação do T-CY relativamente à criminalização da fraude por usurpação de identidade, nos termos da Convenção de Budapeste

A Convenção de Budapeste trata antes de mais dos atos criminosos e não aborda expressamente as técnicas ou tecnologias empregues. Consequentemente, não contém disposições específicas sobre a usurpação de identidade ou o phishing. Contudo, a plena aplicação das disposições de direito substantivo da Convenção permitirá aos Estados tipificar como infrações penais as condutas relacionadas com a usurpação de identidade.

A Convenção obriga os Estados a tipificar como infração penal condutas tais como o acesso ilícito a um sistema informático, a interceção ilegal de dados, a interferência em dados, a interferência em sistemas, o uso indevido de dispositivos e a burla informática:

Fases	**Artigo da Convenção**	**Exemplos**
Fase 1 – Obtenção de dados de identidade	Artigo 2º – Acesso ilegítimo	Quando um pirata contorna a proteção da palavra-passe, regista a digitação nas teclas (keylogging) ou explora falhas de software, o computador pode ser acedido ilicitamente para fins de usurpação de identidade e phishing.
		O acesso ilegítimo a sistemas informáticos é uma das infrações mais comummente cometidas para obter dados sensíveis, tais como dados de identidade.
	Artigo 3º – Interceção ilegítima	A usurpação de identidade comporta muitas vezes a utilização de dispositivos de vigilância (keyloggers) ou outros tipos de malware para intercetar ilegitimamente transmissões não públicas de dados informáticos para, de ou dentro de um sistema informático contendo dados sensíveis, tais como dados de identidade.

Fases	Artigo da Convenção	Exemplos
	Artigo 4º – Interferência em dados	A usurpação de identidade ou o phishing podem danificar, eliminar, deteriorar, alterar ou suprimir dados informáticos. Isto ocorre muitas vezes durante o processo de obtenção de acesso ilegítimo, mediante a instalação de um keylogger para obter dados sensíveis.
	Artigo 5º – Interferência em sistemas	A usurpação de identidade ou o phishing podem entravar o funcionamento de um sistema informático para roubar ou facilitar o roubo de dados de identidade.
	Artigo 7º – Falsidade informática	A usurpação de identidade ou o phishing podem envolver a introdução, alteração, eliminação ou supressão de dados informáticos que resultem em dados não autênticos, com o intuito de que tais dados sejam considerados ou utilizados para fins legais como se fossem autênticos. O phishing é provavelmente a ilustração mais comum de uma burla informática (por exemplo, uma página web forjada de uma instituição financeira) e, consequentemente, é a atividade ilícita mais comummente utilizada para a recolha de dados sensíveis, como os dados de identidade.
Fase 2 – Posse e cessão de dados de identidade	Artigo 6 – Uso indevido de dispositivos	Os dados de identidade roubados – palavras-passe, códigos de acesso, cartões de crédito e outros – podem ser considerados "dispositivos, incluindo um programa informático, concebido e adaptado para permitir cometer qualquer das infrações previstas nos artigos 2º a 5º" da Convenção ou "uma palavra-passe, código de acesso ou dados similares que permitam aceder total ou parcialmente a um sistema informático".
Fase 3 – Utilização de dados de identidade para cometer fraude ou outros crimes	Artigo 8º – Burla informática	A utilização de uma identidade fraudulenta mediante a introdução, alteração, eliminação ou supressão de dados informáticos e/ou a interferência no funcionamento de um sistema informático podem servir para explorar contas bancárias ou cartões de crédito, contrair empréstimos e créditos ou encomendar bens e serviços e pode portanto causar a perda de bens pertencentes a uma pessoa e permitir a outra pessoa obter um benefício económico.

Fases	Artigo da Convenção	Exemplos
Todas as fases	Artigo 11º – Tentativa e cumplicidade	A obtenção, posse e cessão de dados de identidade podem constituir uma tentativa de cometer várias das infrações especificadas na Convenção ou de se tornar cúmplice na sua prática.
	Artigo 13º – Sanções	A usurpação de identidade serve fins criminosos múltiplos, alguns dos quais causam danos graves a indivíduos e a instituições dos setores público e privado. É contudo possível que as sanções previstas pela legislação nacional de algumas Partes em casos de usurpação de identidade sejam demasiado brandas e não permitam tomar em consideração as circunstâncias agravantes. Poderá, assim, ser eventualmente necessário que estas Partes considerem a revisão da sua legislação. Nos termos do artigo 13º, as Partes deverão portanto assegurar que as infrações penais relacionadas com a usurpação de identidade "sejam passíveis de sanções eficazes, proporcionais e dissuasivas, incluindo as penas privativas de liberdade". Para as pessoas coletivas, poderão ser aplicadas sanções penais ou não penais, incluindo as sanções pecuniárias. As Partes podem igualmente tomar em consideração as circunstâncias agravantes, por exemplo se a usurpação de identidade afetar um número significativo de pessoas ou causar perturbação grave ou expuser uma pessoa a perigos.

Declaração do T-CY

O T-CY declara que a presente nota de orientação ilustra o âmbito e os múltiplos elementos da usurpação de identidade e do phishing e as disposições penais aplicáveis.

Portanto, o T-CY pode afirmar que os diferentes aspetos de tais infrações penais estão cobertos pela Convenção de Budapeste.

Nota de orientação sobre ataques contra as infraestruturas de informação críticas[33]

Introdução

Na sua 8ª reunião plenária (dezembro de 2012), o Comité da Convenção sobre o Cibercrime (T-CY) decidiu emitir notas de orientação visando facilitar a utilização e implementação efetivas da Convenção de Budapeste sobre o Cibercrime, nomeadamente à luz dos desenvolvimentos jurídicos, políticos e tecnológicos.[34]

As notas de orientação refletem uma análise da aplicação da Convenção de Budapeste comum a todas as suas Partes.

A presente nota aborda a questão dos ataques a infraestruturas de informação críticas.

A Convenção de Budapeste "recorre a uma linguagem neutra em termos tecnológicos, de modo a que as infrações definidas ao abrigo do direito penal substantivo possam ser aplicáveis quer às tecnologias atuais quer às tecnologias futuras envolvidas".[35] Isto serve para assegurar que as novas formas de malware ou crime sejam sempre cobertas pela Convenção.

Esta Nota de orientação mostra em que medida diferentes artigos da Convenção se aplicam aos ataques a infraestruturas de informação críticas.

Disposições relevantes da Convenção de Budapeste sobre o Cibercrime (STE 185)

As infraestruturas críticas designam em geral os sistemas e os ativos, físicos ou virtuais, indispensáveis à vida de um país e cujo funcionamento incorreto, paragem ou destruição teria um efeito devastador sobre a segurança nacional e a defesa, a segurança económica, a saúde ou a segurança públicas ou qualquer combinação destes elementos. A definição de infraestruturas críticas varia segundo os países. Contudo, para inúmeros países, as infraestruturas críticas englobam a energia, a alimentação, a água, os combustíveis, os transportes, as comunicações, as finanças, a indústria, a defesa e os setores dos serviços públicos e do governo.

---

33. Adotada na 9ª Reunião plenária do T-CY (4-5 junho 2013)
34. Ver o mandato do T-CY (Artigo 46º da Convenção de Budapeste).
35. Parágrafo 36 do Relatório Explicativo

As infraestruturas críticas são frequentemente geridas por sistemas informáticos, nomeadamente os que são conhecidos como sistemas de controlo industriais (SCI) ou sistemas de supervisão, controlo e aquisição de dados (SCADA). Estes sistemas são geralmente designados como infraestruturas de informação críticas.

Segundo fontes privadas e governamentais, ocorre todos os anos um número grande mas desconhecido de ataques a infraestruturas de informação críticas. Estes ataques utilizam as mesmas técnicas que as utilizadas na outra criminalidade eletrónica. A diferença reside no impacto destes ataques sobre a sociedade: podem resultar na retirada de fundos do Tesouro público, interromper o abastecimento de água, perturbar o controlo do tráfego aéreo, etc.

As formas de ataque a infraestruturas de informação críticas, atuais e futuras, são cobertas pelas seguintes secções da Convenção, em função da natureza do ataque. Cada disposição contém um critério de intenção ("sem autorização", "sem intenção fraudulenta", etc.) que as autoridades devem ter em conta ao qualificar uma infração.

Interpretação pelo T-CY da criminalização dos ataques a infraestruturas de informação críticas

Artigos relevantes	**Exemplos**
Artigo 2º – Acesso ilegítimo	Os ataques contra as infraestruturas de informação críticas podem atingir um sistema informático.
Artigo 3º – Interceção ilegítima	Os ataques contra as infraestruturas de informação críticas podem utilizar meios técnicos para intercetar transmissões não públicas de dados informáticos para, de ou dentro de um sistema informático.
Artigo 4º – Interferência em dados	Os ataques contra as infraestruturas de informação críticas podem danificar, eliminar, deteriorar, alterar ou suprimir dados informáticos.
Artigo 5º – Interferência em sistemas	Os ataques contra as infraestruturas de informação críticas podem entravar o funcionamento de um sistema informático; este pode ser, na verdade, o seu objetivo principal.
Artigo 7º – Falsidade informática	Os ataques contra as infraestruturas de informação críticas podem introduzir, alterar, eliminar ou suprimir dados informáticos, resultando em dados não autênticos,

Artigos relevantes	Exemplos
	com o intuito de que tais dados sejam considerados ou utilizados para fins legais como se fossem autênticos.
Artigo 8º – Burla informática	Os ataques contra as infraestruturas de informação críticas podem causar a perda de bens pertencentes a uma pessoa e permitir a outra pessoa obter um benefício económico mediante introdução, alteração, eliminação ou supressão de dados informáticos e/ou a interferência no funcionamento de um sistema informático.
Artigo 11º – Tentativa e cumplicidade	Os ataques contra as infraestruturas de informação críticas podem ser utilizados para tentar cometer infrações especificadas no tratado ou para ser cúmplice na sua prática.
Artigo 13º – Sanções	Os efeitos dos ataques contra as infraestruturas de informação críticas variam (podem variar em países diferentes por razões técnicas, culturais ou outras), mas os governos preocupam-se normalmente com eles quando provocam prejuízos graves ou de grande amplitude. É possível que as sanções previstas pela legislação nacional de algumas Partes em casos de ataques contra infraestruturas de informação críticas sejam demasiado brandas e não permitam tomar em consideração as circunstâncias agravantes, a tentativa ou a cumplicidade. Poderá, assim, ser eventualmente necessário que estas Partes considerem a revisão da sua legislação. Nos termos do artigo 13º, as Partes deverão portanto assegurar que as infrações penais relacionadas com tais ataques "sejam passíveis de sanções eficazes, proporcionais e dissuasivas, incluindo as penas privativas de liberdade". Para as pessoas coletivas, poderão ser aplicadas sanções penais ou não penais, incluindo as sanções pecuniárias.
	As Partes podem igualmente tomar em consideração as circunstâncias agravantes, por exemplo se os ataques contra infraestruturas de informação críticas afetarem um número significativo de sistemas ou os ataques causarem danos consideráveis, incluindo mortes ou ferimentos.

Declaração do T-CY

A lista de artigos relacionados com os ataques contra infraestruturas de informação críticas apresentada acima ilustra as múltiplas infrações que podem ser cometidas por meio destes ataques.

Portanto, o T-CY pode afirmar que os diferentes aspetos de tais ataques estão cobertos pela Convenção de Budapeste.

Nota de orientação sobre as novas formas de malware[36]

Introdução

Na sua 8ª reunião plenária (dezembro de 2012), o Comité da Convenção sobre o Cibercrime (T-CY) decidiu emitir notas de orientação visando facilitar a utilização e implementação efetivas da Convenção de Budapeste sobre o Cibercrime, nomeadamente à luz dos desenvolvimentos jurídicos, políticos e tecnológicos.[37]

As notas de orientação refletem uma análise da aplicação da Convenção de Budapeste comum a todas as suas Partes.

A presente nota aborda a questão das novas formas de malware.

A Convenção de Budapeste "recorre a uma linguagem neutra em termos tecnológicos, de modo a que as infrações definidas ao abrigo do direito penal substantivo possam ser aplicáveis quer às tecnologias atuais quer às tecnologias futuras envolvidas".[38] Isto serve para assegurar que as novas formas de malware ou crime sejam sempre cobertas pela Convenção.

Esta Nota de orientação mostra em que medida diferentes artigos da Convenção se aplicam a novas formas de malware.

Disposições relevantes da Convenção de Budapeste sobre o Cibercrime (STE 185)

Existem atualmente muitas formas de malware (software malicioso). Segundo a Organização para a Cooperação e o Desenvolvimento Económico, malware "é o termo geral para um software introduzido num sistema informático com a finalidade de danificar esse sistema ou outros sistemas ou de os subverter, alterando a forma de utilização pretendida pelos seus utilizadores legítimos."[39] As suas formas mais conhecidas incluem worms, vírus e trojans. As formas atuais de malware têm a capacidade para roubar dados, copiando-os e enviando-os para outro endereço; podem manipular dados; podem entravar a operação de sistemas informáticos, incluindo os que controlam infraestruturas críticas; o *ransomware* pode eliminar, suprimir ou bloquear o acesso aos dados; e malware criado "à medida" pode atacar sistemas informáticos especificados.

---

36. Adotada na 9ª Reunião plenária do T-CY (4-5 junho 2013)
37. Ver o mandato do T-CY (Artigo 46º da Convenção de Budapeste).
38. Parágrafo 36 do Relatório Explicativo
39. http://www.oecd.org/internet/ieconomy/40724457.pdf

Segundo fontes privadas e governamentais, novas e numerosas formas de malware são desenvolvidas e descobertas todos os anos. Estas novas formas variam nos seus objetivos. Tal como as formas mais antigas, as novas formas de malware podem roubar dinheiro, fazer parar redes de abastecimento de água ou ameaçar utilizadores, etc.

O número e variedade de formas de malware são tão vastos que seria impossível, mesmo para as formas conhecidas atualmente, defini-las no quadro da legislação penal. A Convenção sobre o Cibercrime evita deliberadamente termos tais como worms, vírus e trojans. Como as tendências no malware evoluem, a utilização de tais termos numa convenção torná-la-ia rapidamente obsoleta e contraproducente.

É também, obviamente, impossível descrever as formas futuras numa lei.

Por estas razões, é importante concentrarmo-nos nos objetivos e efeitos do malware. Estes já são conhecidos e podem ser alvo de legislação.

Consequentemente, tanto as atuais como as futuras formas de malware estão cobertas pelas seguintes secções da Convenção, em função da ação precisa do malware. Cada disposição contém um critério de intenção ("sem autorização", "sem intenção fraudulenta", etc.) que as autoridades devem ter em conta ao qualificar uma infração.

Interpretação pelo T-CY da criminalização de novas formas de malware

Artigos relevantes	**Exemplos**
Artigo 2º – Acesso ilegítimo	O malware pode ser utilizado para aceder a sistemas informáticos.
Artigo 3º – Interceção ilegítima	O malware pode ser utilizado para intercetar transmissões não públicas de dados informáticos para, de ou dentro de um sistema informático.
Artigo 4º – Interferência em dados	O malware danifica, elimina, deteriora, altera ou suprime dados informáticos.
Artigo 5º – Interferência em sistemas	O malware pode entravar o funcionamento de um sistema informático

Artigos relevantes	Exemplos
Artigo 6º – Uso indevido de dispositivos.	O malware é um dispositivo abrangido pela definição que consta do artigo 6º (as Partes que emitam reservas relativamente ao artigo 6º devem no entanto criminalizar a venda, distribuição ou disponibilização dos dispositivos cobertos por este artigo), pois são concebidos ou adaptados essencialmente para cometer as infrações previstas nos artigos 2º a 5º. Além disso, o artigo tipifica como infração penal a venda, a obtenção para utilização, a importação, distribuição ou outras formas de disponibilização de palavras-passe, códigos de acesso ou dados similares que permitam o acesso a sistemas informáticos. Estes elementos estão frequentemente presentes em procedimentos penais relacionados com malware.
Artigo 7º – Falsidade informática.	O malware pode introduzir, alterar, eliminar ou suprimir dados informáticos, resultando em dados não autênticos, com o intuito de que tais dados sejam considerados ou utilizados para fins legais como se fossem autênticos.
Artigo 8º – Burla informática.	O malware pode causar a perda de bens a uma pessoa e permitir a uma outra pessoa obter um benefício económico mediante a introdução, alteração, eliminação ou supressão de dados informáticos e/ou a interferência no funcionamento de um sistema informático.
Artigo 11º – Tentativa e cumplicidade	O malware pode ser utilizado para tentar cometer várias das infrações especificadas no tratado ou para ser cúmplice na sua prática.

Artigos relevantes	Exemplos
Artigo 13º – Sanções	Os efeitos das novas formas de malware variam bastante. Algum malware é relativamente trivial, outro é perigoso para as pessoas, para as infraestruturas críticas ou a outros níveis. Os efeitos podem variar segundo os países por razões técnicas, culturais ou outras. É possível que as sanções previstas pela legislação nacional de algumas Partes em casos de ataques de malware sejam demasiado brandas e não permitam tomar em consideração as circunstâncias agravantes, a tentativa ou a cumplicidade. Poderá, assim, ser eventualmente necessário que estas Partes considerem a revisão da sua legislação. Nos termos do artigo 13º, as Partes deverão portanto assegurar que as infrações penais relacionadas com tais ataques "sejam passíveis de sanções eficazes, proporcionais e dissuasivas, incluindo as penas privativas de liberdade". Para as pessoas coletivas, poderão ser aplicadas sanções penais ou não penais, incluindo as sanções pecuniárias. As Partes podem igualmente tomar em consideração as circunstâncias agravantes, por exemplo se os ataques de malware afetarem um número significativo de sistemas ou os ataques causarem danos consideráveis, incluindo mortes ou ferimentos ou danos a infraestruturas críticas.

Declaração do T-CY

A lista acima de artigos relacionados com todas as formas de malware ilustra as múltiplas infrações que podem ser cometidas por meio de tais ataques.

Portanto, o T-CY pode afirmar que os diferentes aspetos de todas as formas de malware estão cobertos pela Convenção de Budapeste.

Nota de orientação sobre acesso transfronteiriço a dados (Artigo 32º)[40]

Introdução

Na sua 8ª sessão plenária (dezembro 2012), o Comité da Convenção sobre o Cibercrime (T-CY) decidiu publicar notas de orientação destinadas a facilitar a utilização e a implementação eficazes da Convenção de Budapeste sobre o Cibercrime, nomeadamente à luz dos desenvolvimentos jurídicos, políticos e tecnológicos.[41]

As notas de orientação refletem uma análise da aplicação da Convenção de Budapeste comum a todas as suas Partes.

A presente Nota trata da questão do acesso transfronteiriço aos dados, de acordo com o artigo 32º da Convenção de Budapeste.[42]

O artigo 32.b constitui uma exceção ao princípio da territorialidade, autorizando em circunstâncias limitadas o acesso transfronteiriço unilateral, sem passar pelo auxílio mútuo. As Partes são convidadas a utilizar mais eficazmente todas as disposições da Convenção de Budapeste relacionadas com a cooperação internacional, nomeadamente o auxílio mútuo.

No conjunto, as práticas e os procedimentos, assim como as condições e as salvaguardas, variam consideravelmente entre as várias Partes. Existem sempre preocupações às quais é preciso responder relativamente aos direitos processuais dos suspeitos, a privacidade e a proteção dos dados pessoais, a base legal do acesso aos dados armazenados em jurisdições estrangeiras ou "na nuvem" e o princípio da soberania nacional.

Esta nota de orientação visa ajudar as Partes a aplicar a Convenção de Budapeste, a corrigir os mal-entendidos relativamente ao acesso transfronteiriço nos termos deste tratado e tranquilizar terceiros.

Ela ajudará assim as Partes a tirar pleno partido do potencial do tratado em matéria de acesso transfronteiriço aos dados.

---

40. Adotada pela 12ª reunião plenária do T-CY (2-3 dezembro 2014)
41. Ver o mandato do T-CY (Artigo 46º da Convenção de Budapeste).
42. A elaboração desta nota de orientação dá seguimento às conclusões do relatório sobre "Acesso transfronteiriço e jurisdição" (T-CY(2012)3), adotado na reunião plenária do T-CY, em dezembro de 2012.
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/TCY2013/TCYreports/TCY_2012_3_transborder_rep_V31public_7Dec12.pdf

Artigo 32º da Convenção de Budapeste

Texto do artigo:

> Artigo 32º – Acesso transfronteiriço aos dados informáticos armazenados, mediante consentimento ou quando sejam acessíveis ao público
>
> Uma Parte poderá, sem autorização de outra Parte:
>
> a aceder a dados informáticos armazenados acessíveis ao público (fonte aberta), independentemente da localização geográfica desses dados; ou
>
> b aceder a, ou receber, através de um sistema informático localizado no seu território, dados informáticos armazenados localizados no território de outra Parte, caso a Parte obtenha o consentimento legal e voluntário da pessoa legalmente autorizada a divulgar-lhe tais dados através de tal sistema informático.

Extrato do Relatório Explicativo:

> 293. Os redatores da Convenção debateram longamente a questão de saber em que circunstâncias deverá ser permitido a uma Parte aceder unilateralmente aos dados informatizados, armazenados no território de uma outra Parte, sem requerer a assistência mútua. Foram examinadas em pormenor todas as situações nas quais se considera admissível que os Estados atuem de forma unilateral, bem como as situações nas quais tal não será aceitável. Os redatores chegaram, pois, à conclusão de que, nesta fase, não seria ainda possível elaborar um regime global, legalmente vinculatório, que regulamentasse esta matéria. Tal deve-se, em parte, à inexistência, até à data, de uma experiência objetiva relativamente a este tipo de situações, ao que se acrescenta o facto de se considerar que a resolução adequada está, frequentemente, ligada à conjuntura do caso em concreto, pelo que se torna difícil estipular regras gerais. Por fim, os redatores decidiram que apenas seriam definidas, ao abrigo do artigo 32º da Convenção, as situações nas quais, por unanimidade, a ação unilateral se mostrasse aceitável. Deste modo, foi acordado que não serão regulamentadas outras situações em relação às quais não tenham sido ainda recolhidos novos dados que permitam ditar a experiência e prosseguir os debates sobre a questão. O parágrafo 3 do artigo 39º determina, assim, que as restantes situações não serão nem autorizadas nem excluídas ao abrigo da presente Convenção.
>
> 294. O artigo 32º (Acesso transfronteiriço a dados informatizados armazenados com autorização ou quando disponíveis ao público) trata duas situações: a primeira, quando os dados acedidos se encontram publicamente disponíveis e, segunda, quando a Parte acedeu a, ou recebeu, dados localizados fora do seu território através de um sistema informático situado no seu território, e obteve

o consentimento legal e voluntário da pessoa autorizada, nos termos da lei, a proceder à divulgação dos dados junto da referida Parte e por meio do dito sistema. A questão de quem é a pessoa "legalmente autorizada" a divulgar os dados poderá variar em função das circunstâncias, da natureza jurídica da pessoa e da respetiva legislação aplicável. Por exemplo, uma mensagem de correio eletrónico de uma dada pessoa poderá ser armazenada num outro país por um fornecedor de serviços, ou a pessoa poderá intencionalmente armazenar os dados num outro país. Estas pessoas poderão, assim, recuperar os dados e, visto que dispõem de uma autoridade legal, proceder voluntariamente à divulgação dos dados junto dos serviços competentes para a aplicação da lei, ou permitir a estes últimos o acesso aos dados em conformidade com as disposições contidas neste artigo.

Interpretação do artigo 32º da Convenção de Budapeste pelo T-CY

Relativamente ao artigo 32.a (Acesso transfronteiriço a dados informáticos armazenados acessíveis ao público (fonte aberta)), não foram levantadas questões específicas e não é de momento necessário que o T-CY dê orientações suplementares.

Considera-se geralmente que as autoridades responsáveis pela aplicação da lei podem consultar os dados acessíveis ao público e que, para este fim, podem registar-se ou subscrever serviços abertos ao público.[43]

Se uma parte de um sítio web público, de um serviço ou similar for fechada ao público, esta parte não é considerada acessível ao público no sentido do artigo 32.a.

Relativamente ao artigo 32.b, as situações típicas poderão incluir:

- Uma mensagem de correio eletrónico de uma pessoa pode ser armazenada noutro país por um fornecedor de serviços, ou uma pessoa pode armazenar intencionalmente dados noutro país. Esta pessoa pode recuperar os dados e, desde que tenha a autoridade jurídica para tal, pode voluntariamente divulgar os dados às autoridades competentes para a aplicação da lei ou permitir que estas acedam aos dados, tal como previsto no artigo.[44]
- Um indivíduo suspeito de tráfico de drogas é legalmente preso enquanto a sua caixa de correio eletrónico, possivelmente com provas de uma infração, está aberta no seu tablet, smartphone ou outro dispositivo. Se o suspeito consentir voluntariamente que a polícia aceda à conta e se

43. A legislação nacional pode, contudo, limitar o acesso a dados publicamente disponíveis ou a sua utilização pelas autoridades responsáveis pela aplicação da lei.
44. Parágrafo 294 do Relatório Explicativo.

esta tiver a certeza de que os dados da caixa de correio estão localizados noutro Estado parte, a polícia pode aceder aos dados, nos termos do artigo 32.b.

Outras situações não são autorizadas nem excluídas.[45]

Relativamente ao artigo 32.b (acesso transfronteiriço com consentimento), o T-CY partilha a seguinte análise:

Considerações e salvaguardas gerais

O artigo 32.b é uma medida a aplicar em investigações e procedimentos criminais específicos no âmbito do artigo 14º.[46]

Como se salientou acima, presume-se que as Partes da Convenção mantêm uma relação de confiança mútua e que o Estado de direito e os princípios dos

45. Parágrafo 293 do Relatório Explicativo. Ver também o artigo 39.3 da Convenção de Budapeste.

46. Artigo 14º – Âmbito de aplicação das disposições processuais

1. Cada Parte adotará as medidas legislativas e outras que se mostrem necessárias para instituir os poderes e os procedimentos previstos na presente Secção, para fins de investigação ou de procedimento criminal específico.
2. Salvo disposição em contrário constante do artigo 21º, cada Parte aplicará os poderes e os procedimentos previstos no n.º 1 do presente artigo:

a. às infrações penais previstas nos artigos 2º a 11º da presente Convenção;
b. a outras infrações penais cometidas através de um sistema informático; e
c. à recolha de meios de prova em suporte eletrónico, relativamente à prática de qualquer infração penal.

3. a Cada Parte poderá reservar-se o direito de só aplicar as medidas previstas no artigo 20º às Infrações ou categorias de Infrações especificadas na reserva, desde que o conjunto de tais Infrações ou categorias de Infrações não seja mais reduzido que o conjunto de Infrações a. que aplica as medidas previstas no artigo 21º. Cada Parte procurará limitar tal reserva por forma a permitir a aplicação mais ampla possível da medida prevista no artigo 20º.

b. Sempre que uma Parte, por força das restrições impostas pela sua legislação vigente à data da adoção da presente Convenção, não se encontrar em condições de aplicar as medidas previstas nos artigos 20º e 21º às comunicações transmitidas num sistema informático de um fornecedor de serviços, que:

i. esteja em funcionamento para benefício de um grupo fechado de utilizadores, e
ii. não utilize as redes públicas de telecomunicações e que não se encontre ligado a outro sistema informático, público ou privado, tal Parte poderá reservar-se o direito de não aplicar essas medidas às referidas comunicações. Cada Parte procurará limitar uma tal reserva por forma a permitir a aplicação mais ampla possível das medidas previstas nos artigos 20º e 21º.

direitos humanos são respeitados, de acordo com o artigo 15º da Convenção de Budapeste.[47]

Os direitos dos indivíduos e os interesses de terceiros devem ser tomados em conta na aplicação desta medida.

Uma Parte requerente poderá portanto considerar informar as autoridades relevantes da Parte requerida.

Sobre a noção de "transfronteiriço" e "localização"

O acesso transfronteiriço consiste em "aceder unilateralmente (isto é, sem passar pelo auxílio judiciário mútuo) aos dados informáticos armazenados no território de outra Parte".[48]

Esta medida só pode ser aplicada entre Partes.

O artigo 32.b menciona "dados informáticos armazenados localizados no território de outra Parte", o que significa que pode ser utilizado quando se sabe onde os dados se encontram.

O artigo 32.b não cobre algumas outras situações em que os dados não estão armazenados no território de outra Parte ou quando não se tem a certeza sobre o seu local de armazenamento. Uma Parte não pode invocar o artigo 32.b para obter a divulgação de dados armazenados no seu próprio território.

---

47. Artigo 15º – Condições e salvaguardas
    1. Cada Parte assegurará que o estabelecimento, a implementação e a aplicação dos poderes e procedimentos previstos na presente secção serão sujeitos às condições e salvaguardas previstas no seu direito interno, o qual deverá garantir uma proteção adequada dos direitos do Homem e das liberdades, designadamente dos direitos estabelecidos em conformidade com as obrigações assumidas pela Parte em aplicação da Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa (1950) e do Pacto Internacional sobre os Direitos Civis e Políticos das Nações Unidas (1966), bem como de outros instrumentos internacionais aplicáveis relativos aos direitos do Homem, e deverá incorporar o princípio da proporcionalidade.
    2. Sempre que tal se mostrar apropriado face à natureza do poder ou do procedimento em causa, as referidas condições e salvaguardadas incluirão, designadamente, um controlo judicial ou outras formas de controlo independente, os fundamentos que justificam a sua aplicação, bem como a delimitação do âmbito de aplicação e a duração do poder ou procedimento em causa.
    3. Na medida em que seja do interesse público, em particular da boa administração da justiça, cada Parte examinará o efeito dos poderes e dos procedimentos previstos na presente secção sobre os direitos, as responsabilidades e os interesses legítimos de terceiros.
48. Parágrafo 293 do Relatório Explicativo da Convenção de Budapeste.

Segundo o artigo 32.b, outras situações "não são nem autorizadas nem excluídas". Assim, em casos nos quais se desconhece ou não se tem a certeza se os dados estão armazenados noutro Estado Parte, as Partes podem ser levadas a avaliar elas mesmas a legitimidade de uma busca ou outro tipo de acesso à luz da sua legislação nacional, dos princípios de direito internacional aplicáveis ou considerações relacionadas com as relações internacionais.

Sobre a noção de "acesso sem a autorização de outra Parte"

O artigo 32.b não impõe a utilização do auxílio mútuo e a Convenção de Budapeste não exige que a outra Parte seja informada. Ao mesmo tempo, a Convenção de Budapeste não exclui a notificação. As Partes podem informar a outra Parte se o considerarem útil.

Sobre a noção de "consentimento"

O artigo 32.b estipula que o consentimento deve ser legal e voluntário, o que significa que a pessoa que fornece o acesso aos dados ou que consente em divulgá-los não pode sofrer constrangimento nem engano.[49]

Segundo certas legislações nacionais, os menores ou as pessoas que sofram de doenças mentais ou outras afeções não poderão também dar o seu consentimento válido.

Na maioria dos Estados Partes, a cooperação no quadro de uma investigação criminal exige um consentimento explícito. Por exemplo, a aceitação das condições gerais de utilização de um serviço on-line pode ser insuficiente para constituir um consentimento explícito, mesmo que estas condições indiquem que os dados podem ser transmitidos às autoridades judiciárias em caso de utilização fraudulenta.

Sobre a legislação aplicável

Em todos os casos, as autoridades competentes para a aplicação da lei devem aplicar as mesmas normas jurídicas na aplicação do artigo 32.b que no seu próprio país. Se o acesso aos dados ou a sua divulgação não forem permitidos no território nacional, o mesmo acontecerá na aplicação do artigo 32.b.

49. Em certos países, o consentimento no sentido de evitar ou reduzir as acusações criminais ou uma pena de prisão constitui também consentimento legal e voluntário.

Presume-se que as Partes da Convenção mantêm uma relação de confiança mútua e que o Estado de direito e os princípios dos direitos humanos são respeitados, de acordo com o artigo 15º da Convenção de Budapeste

Sobre a pessoa autorizada a fornecer o acesso ou a divulgar os dados

Quanto a "quem" é a pessoa "legalmente autorizada" a divulgar os dados, isto pode variar em função das circunstâncias, assim como da legislação e regulamentação em vigor.

Pode por exemplo tratar-se de uma pessoa singular específica que dê acesso à sua conta de correio eletrónico ou a outros dados que tenha armazenado no estrangeiro.[50]

Pode também ser uma pessoa coletiva.

É pouco provável que os fornecedores de serviços preencham as condições para darem um consentimento válido e voluntário para a divulgação dos dados dos seus utilizadores, nos termos do artigo 32º. Normalmente, os fornecedores de serviços são apenas depositários destes dados; não têm o controlo nem a propriedade dos dados e não estão portanto em posição de dar um consentimento válido. As autoridades competentes para a aplicação da lei poderão obviamente procurar obter dados num país estrangeiro por outros métodos, tais como o auxílio judiciário mútuo ou procedimentos aplicáveis em situações de emergência.

Pedidos internos legalmente formulados e o artigo 32.b

O artigo 32.b não se aplica às injunções para produção de provas nem a outros pedidos similares legalmente formulados a nível interno num Estado Parte.

Sobre a localização da pessoa consentindo em fornecer acesso aos dados ou em divulgá-los

A hipótese habitual é que a pessoa que dá acesso aos dados está fisicamente presente no território da Parte requerente.

Contudo, são possíveis múltiplas situações. É possível que a pessoa singular ou coletiva se encontre no território das autoridades competentes para a aplicação da lei do Estado requerente quando consentir em divulgar ou fornecer acesso

50 Ver o exemplo dado no parágrafo 294 do Relatório Explicativo.

efetivo aos dados; ou apenas quando concordar em divulgar mas não ao dar acesso, ou a pessoa pode encontrar-se no país onde os dados estão armazenados ao concordar em divulgar e/ou dar acesso aos mesmos. A pessoa pode também encontrar-se fisicamente num país terceiro ao aceitar cooperar ou ao fornecer acesso efetivo aos dados Se se tratar de uma pessoa coletiva (como uma entidade privada), aquela poderá ser representada simultaneamente no território das autoridades competentes para a aplicação da lei requerentes, no território onde se encontram os dados ou mesmo num país terceiro.

Deve ter-se em conta o facto de que muitas Partes se oporiam – e algumas até poderiam considerar isto uma infração – se uma pessoa que se encontrasse fisicamente no seu território fosse diretamente abordada por autoridades competentes para a aplicação da lei estrangeiras solicitando a sua cooperação.

Declaração do T-CY

O T-CY declara que a presente nota de orientação reflete uma análise do âmbito e elementos do artigo 32º comum a todas as suas Partes.

Nota de orientação sobre o spam[51]

Introdução

Na sua 8ª reunião plenária (dezembro de 2012), o Comité da Convenção sobre o Cibercrime (T-CY) decidiu emitir notas de orientação visando facilitar a utilização e implementação efetivas da Convenção de Budapeste sobre o Cibercrime, nomeadamente à luz dos desenvolvimentos jurídicos, políticos e tecnológicos.[52]

As notas de orientação refletem uma análise da aplicação da Convenção de Budapeste comum a todas as suas Partes.

A presente nota aborda a questão do spam. A Convenção de Budapeste "recorre a uma linguagem neutra em termos tecnológicos, de modo a que as infrações definidas ao abrigo do direito penal substantivo possam ser aplicáveis quer às tecnologias atuais quer às tecnologias futuras envolvidas".[53] Isto serve para assegurar que as novas formas de malware ou crime sejam sempre cobertas pela Convenção.

Esta Nota de orientação mostra em que medida diferentes artigos da Convenção se aplicam ao spam.

Disposições relevantes da Convenção de Budapeste sobre o Cibercrime (STE 185)

O spam é muitas vezes definido como correio eletrónico não solicitado, enviado para um grande número de endereços, sendo a identidade pessoal dos destinatários irrelevante, pois a mensagem é dirigida da mesma forma a muitos outros, sem distinção.

Colocam-se questões distintas sobre os pontos seguintes:

- o conteúdo do spam,
- o ato de enviar o spam, e
- o mecanismo utilizado para transmitir o spam.

O conteúdo do spam pode ser ou não ilegal e, quando é ilegal (tal como a oferta de medicamentos contrafeitos ou ofertas financeiras fraudulentas), a infração poderá ser abrangida pela legislação nacional relevante para essas

51. Adotada na 12ª Reunião plenária do T-CY (2-3 dezembro 2014)
52. Ver o mandato do T-CY (Artigo 46º da Convenção de Budapeste).
53. Parágrafo 36 do Relatório Explicativo

infrações. A ação de transmitir spam (incluindo a transmissão em massa de conteúdos não repreensíveis) poderá constituir uma infração civil ou penal em certas jurisdições.

A Convenção não cobre o spam cujo conteúdo não é ilegal e não causa interferência em sistemas, mas que pode causar incómodos aos utilizadores finais.

As ferramentas utilizadas para transmitir o spam podem ser ilegais nos termos da Convenção de Budapeste e o spam pode estar associado a outras infrações não listadas na tabela abaixo (ver, por exemplo, o artigo 7º).

Tal como para as outras notas de orientação, cada disposição contém um critério de intenção ("sem autorização", "sem intenção fraudulenta", etc.). Em alguns casos de spam, esta intenção pode ser difícil de provar.

Interpretação pelo T-CY das disposições relativas ao spam

Artigos relevantes	**Exemplos**
Artigo 2º – Acesso ilegítimo	O spam pode conter malware que pode aceder ou permitir o acesso a um sistema informático.
Artigo 3º – Interceção ilegítima	O spam pode conter malware, que pode intercetar ilegitimamente ou permitir a interceção ilegítima de transmissões de dados informáticos.
Artigo 4º – Interferência em dados	O spam pode conter malware que pode danificar, eliminar, deteriorar, alterar ou suprimir dados informáticos
Artigo 5º – Interferência em sistemas	A transmissão de spam pode entravar gravemente o funcionamento de um sistema informático. O spam pode conter malware que prejudique gravemente o funcionamento de um sistema informático.
Artigo 6º – Uso indevido de dispositivos	Os dispositivos, tal como definidos no artigo 6º, podem ser utilizados para a transmissão de spam. O spam pode conter dispositivos, tal como definidos no artigo 6º.
Artigo 8º – Burla informática	O spam pode ser utilizado como dispositivo para a introdução, alteração, eliminação ou supressão de dados informáticos ou para a interferência no funcionamento de um sistema informático para obtenção de um benefício económico ilícito.
Artigo 10º – Infrações penais relacionadas com a violação do direito de autor e dos direitos conexos	O spam pode servir para fazer publicidade à venda de produtos contrafeitos, incluindo software e outros bens protegidos por copyright.

Artigos relevantes	Exemplos
Artigo 11º – Tentativa e cumplicidade	O spam e a transmissão de spam podem ser utilizados para tentar cometer várias das infrações especificadas no tratado ou para ser cúmplice na sua prática (tais como falsidade informática, artigo 7º, e burla informática, artigo 8º)
Artigo 13º – Sanções	O spam serve fins criminosos múltiplos, alguns dos quais causam danos graves a indivíduos e a instituições dos setores público e privado. Mesmo que uma Parte não tipifique o spam em si como infração penal, deverá tipificar como infração penal qualquer conduta relacionada com o spam, tais como as infrações acima mencionadas, e poderá considerar circunstâncias agravantes. Nos termos do artigo 13º, as Partes deverão portanto assegurar que as infrações penais relacionadas com o spam "sejam passíveis de sanções eficazes, proporcionais e dissuasivas, incluindo as penas privativas de liberdade". Para as pessoas coletivas, poderão ser aplicadas sanções penais ou não penais, incluindo as sanções pecuniárias

Declaração do T-CY

A lista de artigos acima apresentada ilustra as múltiplas infrações que podem ser cometidas por meio do spam e as infrações relacionadas com o spam.

Portanto, o T-CY pode afirmar que estes aspetos do spam estão cobertos pela Convenção de Budapeste.

Nota de orientação sobre injunções sobre dados relativos aos assinantes (Artigo 18º da Convenção de Budapeste)[54]

Na sua 8ª reunião plenária (dezembro de 2012), o Comité da Convenção sobre o Cibercrime (T-CY) decidiu emitir notas de orientação visando facilitar a utilização e implementação efetivas da Convenção de Budapeste sobre o Cibercrime, nomeadamente à luz dos desenvolvimentos jurídicos, políticos e tecnológicos.[55]

Embora não sejam vinculativas, as notas de orientação refletem uma análise da aplicação da Convenção de Budapeste comum a todas as suas Partes.

A presente Nota[56] trata da questão das injunções sobre dados relativos aos assinantes, nos termos do artigo 18º, isto é, situações nas quais:

- uma pessoa a quem se ordena que comunique dados informáticos especificados está presente no território de um Estado Parte (Artigo 18.1.a);[57]
- um fornecedor de serviços a quem se ordena que comunique dados relativos a assinantes oferece os seus serviços no território da Parte, sem necessariamente estar situado no território em questão (Artigo 18.1.b).

É pertinente publicar uma Nota de orientação sobre estes aspetos do artigo 18º, dado que:

- os dados relativos aos assinantes são os mais frequentemente procurados nas investigações criminais;
- o artigo 18º tem uma competência nacional;
- o crescimento da computação em nuvem e do armazenamento remoto de dados levantou algumas dificuldades às autoridades competentes que desejam acesso a dados informáticos especificados – e em particular aos dados relativos aos assinantes – para conduzir investigações e procedimentos criminais;
- atualmente, as práticas e procedimentos, assim como as condições e salvaguardas para acesso aos dados relativos aos assinantes variam consideravelmente entre as Partes da Convenção;

---

54. Adotada pelo T-CY, no seguimento da 16ª plenária, por procedimento escrito (28 fevereiro 2017)
55. Ver o mandato do T-CY (Artigo 46º da Convenção de Budapeste).
56. Esta Nota de orientação apoia-se nos trabalhos do Grupo sobre as Provas na Cloud do T-CY.
57. É importante recordar que o Artigo 18.1.a da Convenção de Budapeste não se limita a dados relativos aos assinantes e diz respeito a qualquer tipo de dados informáticos especificados. Contudo, esta Nota de orientação apenas trata da comunicação de dados relativos aos assinantes.

– é necessário tratar os problemas que se colocam em matéria de vida privada e proteção de dados pessoais, a base jurídica da jurisdição dos serviços oferecidos no território de uma Parte sem que o fornecedor de serviços se encontre estabelecido nesse território, assim como o acesso a dados armazenados em jurisdições estrangeiras ou em locais desconhecidos e múltiplos "na nuvem".

A notificação e a executoriedade das injunções nacionais contra os fornecedores estabelecidos fora do território de um Estado Parte colocam outros problemas que não podem ser plenamente tratados no quadro de uma nota de orientação. Os Estados Partes podem exigir os dados relativos aos assinantes através do auxílio judiciário mútuo.

O artigo 18º é uma medida a ser aplicada em investigações ou procedimentos criminais específicos no âmbito do artigo 14º da Convenção de Budapeste. As injunções devem portanto ser emitidas em casos específicos relativamente a assinantes especificados.

Artigo 18º da Convenção de Budapeste

Texto da disposição

> Artigo 18º – Injunção
>
> 1 Cada Parte adotará as medidas legislativas e outras que se mostrem necessárias para habilitar as suas autoridades competentes a ordenar:
>
> a. a uma pessoa que se encontre no seu território a comunicar dados informáticos específicos na sua posse ou sob o seu controlo e armazenados num sistema informático ou num suporte de armazenamento de dados informáticos; e
>
> b. a um fornecedor de serviços que preste os seus serviços no território da Parte a comunicar os dados que tenha na sua posse ou sob o seu controlo, relativos aos assinantes e respeitantes a tais serviços.

Extrato do Relatório Explicativo:

> 173. Em virtude do disposto no parágrafo 1(a), uma Parte deverá certificar-se de que as suas autoridades competentes para a aplicação da lei são investidas dos poderes necessários para ordenar a uma pessoa, que esteja no seu território, a apresentação de dados específicos armazenados num sistema informático ou num suporte de armazenamento de dados, que se encontrem na sua posse ou sob o seu controlo. A expressão "posse ou controlo" refere-se à posse física dos dados em questão no seio do território da Parte que emite a ordem, bem como a situações em que os dados a serem produzidos não se encontram na posse

física da pessoa mas sendo possível, contudo, a esta última exercer livremente o seu controlo sobre a produção dos dados a partir do território da Parte emissora da ordem (por exemplo, sob reserva dos privilégios aplicáveis, toda e qualquer pessoa que receba uma ordem de produção relativa à informação armazenada, por sua conta, por meio de um serviço de armazenamento à distância on-line, ficará obrigada a reproduzir a referida informação). Por outro lado, a simples capacidade técnica de aceder a dados armazenados à distância (por exemplo, a capacidade de um utilizador para aceder, através de uma ligação da rede, a dados armazenados à distância que não se encontrem legalmente sob o seu controlo), não constitui necessariamente um "controlo" nos termos a que se refere a presente disposição. Nalguns Estados, o conceito denominado por "posse", de acordo com a lei, cobre a noção de posse física e construtiva, com uma amplitude suficiente para satisfazer este requisito de "posse ou controlo".

Nos termos do parágrafo 1(b), uma Parte deve também instaurar o poder de ordenar a um fornecedor que ofereça serviços no seu território que comunique "dados informáticos específicos na sua posse ou sob o seu controlo". Tal como no parágrafo 1(a), a expressão "posse ou controlo" refere-se a dados relativos ao assinante, materialmente detidos pelo fornecedor de serviços e a dados relativos ao assinante armazenados à distância sob o controlo do fornecedor de serviços (por exemplo, numa instalação de armazenamento de dados à distância fornecida por outra empresa). A expressão "respeitantes a tais serviços" significa que o poder em questão deve servir para obter dados relativos ao assinante ligados aos serviços oferecidos no território da Parte na origem da injunção.[58]

O que são "dados relativos aos assinantes?"

A expressão "dados relativos aos assinantes" é definida no artigo 18.3 da Convenção de Budapeste:

> 3 Para efeitos do presente artigo, a expressão "dados relativos aos assinantes" designa 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 de natureza técnica 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 relativos à faturação e ao pagamento, disponíveis com base num contrato ou num acordo de serviços;

58. Parágrafo 173 do Relatório Explicativo.

c qualquer outra informação sobre a localização do equipamento de comunicação disponível com base num contrato ou num acordo de prestação de serviços.

O parágrafo 177 do Relatório Explicativo nota ainda:

> 177. A expressão "informação relativa ao subscritor" encontra-se definida no parágrafo 3. Em princípio, abrange toda e qualquer informação detida pela administração de um fornecedor de serviços relativamente a um subscritor dos seus serviços. A informação relativa ao subscritor poderá apresentar-se sob a forma de dados informatizados ou qualquer outra forma, tal como um documento em suporte papel. Sendo que a informação relativa ao subscritor nem sempre se apresenta sob a forma de dados informatizados, foi incluída no presente artigo uma disposição especial cujo objetivo é regulamentar este tipo de informação. O termo "subscritor" pressupõe-se englobar um vasto leque de clientes de fornecedores de serviços, desde aqueles que pagam uma tarifa fixa de assinatura, aos que pagam os serviços à medida que os vão utilizando, até aos que usufruem de serviços gratuitos. O referido termo cobre igualmente toda a informação referente a pessoas que se encontram habilitadas a utilizar a conta do subscritor.

A obtenção de dados relativos aos assinantes pode constituir uma interferência menor em termos dos direitos individuais do que a obtenção de dados relativos ao tráfego ou ao conteúdo.

O que é um "fornecedor de serviços"?

A Convenção de Budapeste sobre o Cibercrime aplica um conceito lato de "fornecedor de serviços", que é definido no seu artigo 1.c.

Para os efeitos da presente Convenção:

> c. A expressão "fornecedor de serviços" designa:
>
> i. qualquer entidade pública ou privada que faculte aos utilizadores dos seus serviços a possibilidade de comunicarem através de um sistema informático, e
>
> ii. qualquer outra entidade que processe ou armazene dados informáticos em nome do referido serviço de comunicações ou dos utilizadores desse serviço.

O artigo 18.1.b deve ser aplicado para todo o fornecedor de serviços que ofereça os seus serviços no território da Parte.[59]

Interpretação pelo T-CY do artigo 18º da Convenção de Budapeste sobre dados relativos a assinantes

O âmbito do Artigo 18.1.a

- O âmbito é amplo: uma "pessoa" (que pode incluir um "fornecedor de serviços") que se encontre no território da Parte.
- No que respeita aos dados informáticos, o âmbito é lato, mas não indefinido: todos os dados informáticos "especificados"[2] (daí que o artigo 18.1.a não se restringe aos "dados relativos aos assinantes" e cobre todos os tipos de dados informáticos).
- Os dados informáticos especificados estão na posse dessa pessoa ou, se a pessoa não tiver a sua posse física, controla livremente os dados informáticos transmitidos no quadro do artigo 18.1.a a partir do território do Estado Parte.
- Os dados informáticos especificados encontram-se armazenados num sistema informático ou num meio de armazenamento informático.
- A injunção é emitida e executável pelas autoridades competentes no Estado Parte no qual a injunção é pedida e concedida.

O âmbito do artigo 18.1.b

O âmbito do artigo 18.1.b é mais estreito que o do artigo 18.1.a:

- A subsecção b restringe-se ao "fornecedor de serviços".[60]
- O fornecedor de serviços destinatário da injunção não está necessariamente presente no território, mas oferece os seus serviços no território do Estado Parte.
- Limita-se aos "dados relativos aos assinantes".
- Os dados relativos aos assinantes estão ligados a estes serviços e encontram-se na posse ou sob o controlo do fornecedor de serviços.

---

59. Os instrumentos da União Europeia fazem a distinção entre fornecedores de serviços de comunicações eletrónicas e de serviços na sociedade da Internet. O conceito de "fornecedor de serviços" do Artigo 1.c da Convenção de Budapeste engloba ambos os tipos.
60. O conceito de "pessoa" é mais lato que o de "fornecedor de serviços", embora um "fornecedor de serviços" possa ser "uma pessoa".

Por contraste ao artigo 18.1.a, que se limita no seu campo de aplicação às "pessoas presentes no território do Estado Parte", o artigo 18.1.b mantém o silêncio sobre a localização do fornecedor de serviços. As Partes poderiam aplicar a disposição em circunstâncias nas quais o fornecedor de serviços oferecendo os seus serviços no território do Estado Parte não se encontra nem jurídica nem fisicamente presente no território.

Jurisdição

O artigo 18.1.b limita-se às circunstâncias nas quais a autoridade de justiça penal que emite a injunção tem jurisdição sobre a infração.

Isto pode incluir situações nas quais o assinante é ou era residente ou presente nesse território quando a infração foi cometida.

A presente interpretação do artigo 18º não prejudica as competências mais latas e suplementares previstas na legislação nacional das Partes.

A concordância com esta Nota de orientação não implica o consentimento com a notificação ou a executoriedade extraterritorial de uma injunção nacional emitida por outro Estado nem cria novas obrigações ou relações entre as Partes.

Quais são as características de uma "injunção?

Uma "injunção" (ou ordem de produção), no sentido do artigo 18º, é uma medida nacional que deve ser tomada segundo o direito penal interno. Uma "injunção" é limitada pela competência de adjudicação e execução da Parte na qual a injunção é concedida.

As injunções nos termos do artigo 18º dizem respeito:

> a dados informatizados ou a informações relativas aos subscritores que se encontram na posse ou sob o controlo de uma pessoa singular ou de um fornecedor de serviços. Esta medida é aplicável somente nas situações em que se constate a manutenção, por parte da referida pessoa ou do fornecedor de serviços, de tais dados ou informações. Alguns fornecedores de serviços, por exemplo, não mantêm normalmente quaisquer registos relativos aos subscritores dos seus serviços.[61]

61. Parágrafo 172 do Relatório Explicativo.

O Relatório Explicativo[62] da Convenção de Budapeste menciona as injunções como uma medida flexível, menos intrusiva que a busca ou apreensão ou outros poderes coercivos e afirma ainda que:

> A implementação de um tal mecanismo processual revelar-se-á igualmente benéfico para terceiros, administradores de dados, tais como os fornecedores de serviços da Internet (ISP) que, muitas vezes, estão dispostos a colaborar voluntariamente com as autoridades competentes para a aplicação da lei, fornecendo os dados que se encontram sob o seu controlo mas manifestando a sua preferência pela adoção de uma base jurídica relativa a esta assistência, de modo a ficarem isentos de quaisquer responsabilidades contratuais ou não contratuais eventualmente decorrentes desta divulgação.

Que efeito tem a localização dos dados?

O armazenamento dos dados relativos aos assinantes noutra jurisdição não impede a aplicação do artigo 18º da Convenção de Budapeste, desde que tais dados estejam na posse ou sob o controlo do fornecedor de serviços. O Relatório Explicativo afirma:

- em relação ao artigo 18.1.a, que "a expressão posse ou controlo" refere-se à posse física dos dados em questão no seio do território da Parte que emite a ordem, bem como a situações em que os dados a serem produzidos não se encontram na posse física da pessoa mas sendo possível, contudo, a esta última exercer livremente o seu controlo sobre a produção dos dados a partir do território da Parte emissora da ordem."[63]
- em relação ao artigo 18.1.b, que "a expressão posse ou controlo" refere-se a dados relativos ao assinante, materialmente detidos pelo fornecedor de serviços e a dados relativos ao assinante armazenados à distância sob o controlo do fornecedor de serviços (por exemplo, numa instalação de armazenamento de dados à distância fornecida por outra empresa)."[64]

Relativamente ao artigo 18.1.b, uma situação que pode ocorrer é a de um fornecedor de serviços que tem a sua sede numa jurisdição, mas armazena os dados noutra jurisdição. Os dados podem também ser replicados em várias jurisdições ou deslocar-se entre jurisdições, à discrição do fornecedor de serviços e sem o conhecimento ou controlo do assinante. Os regimes jurídicos

62. Parágrafo 171 do Relatório Explicativo.
63. Parágrafo 173 do Relatório Explicativo. Uma "pessoa" no sentido do artigo 18.1.a da Convenção de Budapeste pode ser uma pessoa singular ou coletiva, nomeadamente um fornecedor de serviços.
64. Parágrafo 173 do Relatório Explicativo.

reconhecem cada vez mais, tanto na esfera do direito penal como em matéria de proteção da vida privada e dos dados, que a localização dos dados não é o fator determinante para estabelecer a competência jurisdicional.

O que significa "prestar serviços no território de uma Parte?"

O crescimento da "computação em nuvem" tem levantado questões sobre quando se considera que um fornecedor de serviços está a oferecer os seus serviços no território da Parte, ficando assim obrigado a obedecer a uma injunção nacional de comunicação de dados relativos aos assinantes. Esta questão tem sido objeto de uma série de interpretações pelos tribunais nas diversas jurisdições, tanto em processos civis como penais.

Relativamente ao artigo 18.1.b, as Partes podem considerar que um fornecedor de serviços está a "prestar os seus serviços no território da Parte" quando:

- o fornecedor de serviços permite às pessoas no território da Parte subscrever os seus serviços[65] (e não bloqueia, por exemplo, o acesso a este tipo de serviços); e
- o fornecedor de serviços estabeleceu uma ligação real e substancial a um Estado Parte. Os fatores relevantes incluem a medida na qual um fornecedor de serviços orienta as suas atividades para estes assinantes (por exemplo, fazendo publicidade local ou anunciando na língua do território da Parte), utiliza os dados relativos aos assinantes (ou os dados de tráfego associados) no decurso das suas atividades, interage com assinantes no Estado Parte e pode, de outras formas, ser considerado como estabelecido no território do Estado Parte.

O simples facto de um fornecedor de serviços utilizar um nome de domínio ou um endereço de correio eletrónico ligado a um país específico não cria o pressuposto de que a sede dos seus negócios fica situada nesse país. Por esse motivo, o requisito de os dados relativos aos assinantes a serem comunicados se relacionarem com os serviços de um fornecedor oferecidos no território da Parte pode ser considerado satisfeito, mesmo que esses serviços sejam fornecidos através de um nome de domínio de topo com código de país referente a outra jurisdição.

65. Note o Parágrafo 183 do Relatório Explicativo: "A expressão "acordo ou contrato de serviços" deverá ser interpretada num sentido lato, incluindo qualquer tipo de relação com base na qual um cliente utilize os serviços prestados pelo fornecedor."

Condições gerais e salvaguardas

Espera-se das Partes da Convenção que mantenham uma relação de confiança mútua, dentro do respeito do artigo 15º da Convenção de Budapeste.

> Artigo 15º – Condições e salvaguardas
>
> 1 – Cada Parte assegurará que o estabelecimento, a implementação e a aplicação dos poderes e procedimentos previstos na presente secção serão sujeitos às condições e salvaguardas previstas no seu direito interno, o qual deverá garantir uma proteção adequada dos direitos do Homem e das liberdades, designadamente dos direitos estabelecidos em conformidade com as obrigações assumidas pela Parte em aplicação da Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa (1950) e do Pacto Internacional sobre os Direitos Civis e Políticos das Nações Unidas (1966), bem como de outros instrumentos internacionais aplicáveis relativos aos direitos do Homem, e deverá incorporar o princípio da proporcionalidade.
>
> 2 – Sempre que tal se mostrar apropriado face à natureza do poder ou do procedimento em causa, as referidas condições e salvaguardadas incluirão, designadamente, um controlo judicial ou outras formas de controlo independente, os fundamentos que justificam a sua aplicação, bem como a delimitação do âmbito de aplicação e a duração do poder ou procedimento em causa.
>
> 3 - Na medida em que seja do interesse público, em particular da boa administração da justiça, cada Parte examinará o efeito dos poderes e dos procedimentos previstos na presente Secção sobre os direitos, as responsabilidades e os interesses legítimos de terceiros.

Aplicação do artigo 18º no que respeita aos dados relativos aos assinantes

A comunicação dos dados relativos aos assinantes, de acordo com o artigo 18º da Convenção de Budapeste, pode portanto ser ordenada se os seguintes critérios forem satisfeitos numa investigação criminal específica e para assinantes especificados:

SE a autoridade de justiça penal tiver competência relativamente à infração;		
E SE o fornecedor de serviços possuir ou controlar os dados relativos aos assinantes;		
E SE		
Artigo 18.1.a A pessoa (o fornecedor de serviços) estiver presente no território da Parte.	OU	Artigo 18.1.b Um Estado Parte considera que um fornecedor de serviços "presta os seus serviços no território da Parte" quando, por exemplo: - o fornecedor de serviços permite às pessoas no território da Parte subscrever os seus serviços (e não bloqueia, por exemplo, o acesso a este tipo de serviços); e - o fornecedor de serviços estabeleceu uma ligação real e substancial a um Estado Parte. Os fatores relevantes incluem a medida na qual um fornecedor de serviços orienta as suas atividades para os seus assinantes (por exemplo, fazendo publicidade local ou anunciando na língua do território da Parte), utiliza os dados relativos aos assinantes (ou os dados de tráfego associados) no decurso das suas atividades, interage com assinantes no Estado Parte e pode, de outras formas, ser considerado como estabelecido no território do Estado Parte.
E SE		
		- Os dados relativos aos assinantes a serem comunicados se relacionarem com os serviços de um fornecedor oferecidos no território da Parte.

Declaração do T-CY

O T-CY declara que a presente nota de orientação reflete uma análise do âmbito e elementos do artigo 18º da Convenção de Budapeste relativamente à comunicação de dados relativos aos assinantes comum a todas as suas Partes.

Nota de orientação sobre o terrorismo[66]

Na sua 8ª reunião plenária (dezembro de 2012), o Comité da Convenção sobre o Cibercrime (T-CY) decidiu emitir notas de orientação visando facilitar a utilização e implementação efetivas da Convenção de Budapeste sobre o Cibercrime, nomeadamente à luz dos desenvolvimentos jurídicos, políticos e tecnológicos.[67]

As notas de orientação refletem uma análise da aplicação da Convenção de Budapeste comum a todas as suas Partes.

Esta Nota de orientação mostra em que medida diferentes artigos da Convenção se poderiam aplicar ao terrorismo.

Muitos países são partes de diversos tratados e estão vinculados pelas resoluções do Conselho de Segurança das Nações Unidas, que exigem a criminalização de diferentes formas de terrorismo, facilitação do terrorismo, apoio ao terrorismo e atos preparatórios de terrorismo. Nos casos de terrorismo, os países apoiam-se muitas vezes em infrações que derivam destes tratados que visam temas específicos, assim como em infrações suplementares tipificadas na legislação nacional.

A Convenção de Budapeste não é um tratado centrado especificamente no terrorismo. Contudo, as infrações materiais visadas na Convenção podem ser transpostas como atos de terrorismo, para facilitar o terrorismo, para apoiar o terrorismo, incluindo financeiramente, ou como atos preparatórios.

Além disso, as ferramentas processuais e de auxílio judiciário internacional mútuo previstas na Convenção são aplicáveis às investigações e procedimentos de terrorismo e relacionados.

O âmbito e os limites são definidos pelos artigos 14.2 e 25.1 da Convenção de Budapeste:

> Artigo 14.2
>
> 2 Salvo disposição em contrário constante do artigo 21º, cada Parte aplicará os poderes e os procedimentos previstos no n.º 1 do presente artigo:
>
> a Às Infrações penais previstas nos artigos 2º a 11º da presente Convenção;
>
> b A outras Infrações penais cometidas através de um sistema informático; e

66. Adotado pelo T-CY na sequência da 16.ª reunião plenária por procedimento escrito (28 de fevereiro de 2017).
67. Ver o mandato do T-CY (Artigo 46º da Convenção de Budapeste).

c À recolha de meios de prova em suporte eletrónico, relativamente à prática de qualquer infração penal.

Artigo 25.1.

"As Partes concederão entre si o auxílio mútuo mais amplo possível para efeitos de investigações ou de procedimentos relativamente a Infrações penais relacionadas com sistemas e dados informáticos, ou para efeitos de recolha de provas sob a forma eletrónica relativamente a uma infração penal."

Ver também os artigos 23 e 27.1 da Convenção de Budapeste, assim como outras Notas de orientação, tais como as que abordam os ataques contra infraestruturas críticas ou ataques por negação de serviço distribuído.

Disposições relevantes da Convenção de Budapeste sobre o Cibercrime (STE 185)

Disposições processuais

Os poderes processuais da Convenção (artigos 14º-21º) podem ser utilizados numa investigação ou procedimento criminal em qualquer tipo de caso, conforme previsto no artigo 14º.

De facto, as medidas processuais específicas podem ser muito úteis, por exemplo em casos de terrorismo, se um sistema informático tiver sido utilizado para cometer ou facilitar uma infração ou se as provas da infração estiverem armazenadas em formato eletrónico ou se um suspeito puder ser identificado através dos dados relativos ao assinante, nomeadamente um endereço IP (Internet Protocol). Assim, em casos de terrorismo, as Partes podem recorrer à conservação expedita dos dados informáticos armazenados, injunções, ordens de busca e apreensão dos dados informáticos armazenados e a outras ferramentas para recolher provas eletrónicas em investigações e procedimentos relacionados com o terrorismo no âmbito acima exposto.

Disposições sobre o auxílio judiciário internacional mútuo

Os poderes de cooperação internacional da Convenção (artigos 23º-35º) têm um âmbito similar.

Assim as Partes devem assegurar a conservação expedita dos dados informáticos armazenados, injunções, ordens de busca e apreensão dos dados informáticos armazenados e outras ferramentas, assim como outras disposições de cooperação internacional, a fim de cooperar com outras Partes em investigações e procedimentos de terrorismo e relacionados com o terrorismo no âmbito acima exposto.

Disposições do direito penal substantivo

Por fim, tal como notado acima, os terroristas e grupos terroristas podem perpetrar atos criminalizados pela Convenção para alcançar os seus fins.

Artigos relevantes	Exemplos
Artigo 2º – Acesso ilegítimo	Um sistema informático pode ser ilegitimamente acedido para obter dados de identificação pessoal (por exemplo, informação sobre funcionários governamentais para os visar para um ataque).
Artigo 3º – Interceção ilegítima	As transmissões não públicas de dados informáticos para, de ou dentro de um sistema informático podem ser ilegalmente interc-etadas para obter informação sobre a localização de uma pessoa (a fim de a atacar)
Artigo 4º – Interferência em dados	Os dados informáticos podem ser danificados, eliminados, deterio-rados, alterados ou suprimidos (por exemplo, fichas médicas hos-pitalares podem ser alteradas, tornando-se perigosamente incor-retas, ou a interferência no sistema de controlo de tráfego aéreo pode afetar a segurança dos voos).
Artigo 5º – Interferência em sistemas	O funcionamento de um sistema informático pode ser entravado para fins terroristas (por exemplo, entravar um sistema que arma-zene registos da bolsa de valores pode torná-los inexatos ou entra-var o funcionamento de infraestruturas críticas)
Artigo 6º – Uso indevido de dispositivos	A venda, a obtenção para utilização, a importação, a distribuição, ou outros atos de disponibilização de palavras-passe, códigos de acesso ou dados similares que permitam aceder a sistemas informáticos podem facilitar um ataque terrorista (podendo, por exemplo, levar a danos na rede nacional de energia elétrica).
Artigo 7º – Falsidade informática	Os dados informáticos (por exemplo, os dados utilizados nos pas-saportes eletrónicos) podem ser introduzidos, alterados, eliminados ou suprimidos, resultando em dados não autênticos, com o intuito de que tais dados sejam considerados ou utilizados para fins legais como se fossem autênticos.
Artigo 8º – Burla informática	Os dados informáticos podem ser introduzidos, alterados, elimina-dos ou suprimidos e/ou pode ocorrer interferência no funciona-mento de um sistema informático, provocando a perda de bens a outras pessoas (por exemplo, um ataque ao sistema bancário de um país pode provocar a perda de bens a várias vítimas).
Artigo 11º – Tentativa e cumplicidade	As infrações penais especificadas no tratado podem assumir a forma de tentativa ou cumplicidade, para servir os fins do terrorismo.

Artigos relevantes	Exemplos
Artigo 12º – Responsabilidade das pessoas coletivas	As infrações penais cobertas pelos artigos 2º-11º da Convenção, para servir os fins do terrorismo, podem ser cometidas por pessoas coletivas, que seriam declaradas responsáveis nos termos do artigo 12º.
Artigo 13º – Sanções	As infrações penais cobertas pela Convenção podem constituir uma ameaça para os indivíduos e a sociedade, especialmente quando os crimes são dirigidos contra sistemas cruciais para a vida do dia-a-dia, por exemplo os transportes públicos, os sistemas bancários ou a infraestrutura hospitalar. Os efeitos podem variar nos diferentes países, em função também do seu grau de interconectividade e da sua dependência de tais sistemas. É contudo possível que as sanções previstas pela legislação nacional de algumas Partes em casos de atos ligados ao terrorismo, relativamente aos artigos 2º-11º, sejam demasiado brandas e não permitam tomar em consideração as circunstâncias agravantes, a tentativa ou a cumplicidade. Poderá, assim, ser eventualmente necessário que estas Partes considerem a revisão da sua legislação. Nos termos do artigo 13º, as Partes deverão portanto assegurar que as infrações penais relacionadas com tais atos "sejam passíveis de sanções eficazes, proporcionais e dissuasivas, incluindo as penas privativas de liberdade". As Partes podem igualmente tomar em consideração as circunstâncias agravantes, por exemplo se tais atos afetarem um número significativo de sistemas ou os ataques causarem danos consideráveis, incluindo mortes ou ferimentos ou danos a infraestruturas críticas.

Outras infrações cobertas pela Convenção mas não especificamente mencionadas acima, nomeadamente a produção de materiais ligados à exploração infantil ou o tráfico de propriedade intelectual roubada, podem também ser cometidas em associação com o terrorismo.

Para as Partes da Convenção de Budapeste que são também Partes do Protocolo adicional relativo à criminalização de atos de natureza racista e xenófoba praticados através de sistemas informáticos (STE 189)[68], há dois artigos do Protocolo que são relevantes, pois podem relacionar-se com a radicalização e

68. http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

o extremismo violento, que podem conduzir ao terrorismo. Estes são o artigo 4º do Protocolo, sobre ameaça com motivação racista e xenófoba, e o artigo 6º, cobrindo a negação, minimização grosseira, aprovação ou justificação do genocídio ou dos crimes contra a humanidade.

Declaração do T-CY

O T-CY pode afirmar que as infrações substantivas abordadas pela Convenção podem também constituir atos de terrorismo, tal como definido na legislação aplicável.

As infrações substantivas visadas na Convenção podem ser cometidas para facilitar o terrorismo, para o apoiar, incluindo financeiramente, ou para preparar os atos terroristas.

As ferramentas processuais e de auxílio judiciário mútuo previstas na Convenção podem ser utilizadas para investigar o terrorismo, a sua facilitação e o apoio ou atos preparatórios do terrorismo.

Nota de orientação sobre aspetos da interferência eleitoral por meio de sistemas informáticos cobertos pela Convenção de Budapeste[69]

Introdução

Na sua 8ª reunião plenária (dezembro 2012), o Comité da Convenção sobre o Cibercrime (T-CY) decidiu emitir notas de orientação visando facilitar a utilização e implementação efetivas da Convenção de Budapeste sobre o Cibercrime, nomeadamente à luz dos desenvolvimentos do direito, política e tecnologia.[70]

As notas de orientação refletem uma análise da aplicação da Convenção de Budapeste partilhada por todas as suas Partes.

A interferência em eleições através de ciberatividades maliciosas contra os computadores e dados utilizados em eleições e campanhas eleitorais compromete a realização de eleições livres, justas e transparentes e a confiança na democracia. As operações de desinformação, tais como as vividas em particular desde 2016, podem recorrer a tais práticas e ter o mesmo efeito. Os procedimentos eleitorais nacionais poderão ter que ser adaptados às realidades da sociedade da informação e os sistemas informáticos utilizados para as eleições e as campanhas eleitorais devem ser tornados mais seguros.

Neste contexto, é preciso intensificar esforços no sentido de processar judicialmente estas interferências sempre que constituam uma infração penal: uma resposta eficaz da justiça penal pode dissuadir ações de interferência eleitoral e tranquilizar o eleitorado quanto à utilização das tecnologias da informação e comunicação nas eleições.

A presente nota aborda a forma como os artigos da Convenção podem aplicar-se a aspetos da interferência eleitoral por meio de sistemas informáticos.

As infrações penais substantivas definidas na Convenção podem ser cometidas como atos de interferência eleitoral ou como atos preparatórios, facilitadores desta interferência.

Além disso, estão disponíveis as ferramentas dos procedimentos nacionais e do auxílio judiciário mútuo internacional da Convenção para investigações e processos judiciais ligados à interferência eleitoral. O âmbito e os limites dos

69. Adotada pela 21ª sessão plenária do T-CY (8 julho 2019)
70. Ver o mandato do T-CY (Artigo 46º da Convenção de Budapeste).

poderes procedimentais e das ferramentas de cooperação internacional são definidos pelos artigos 14.2 e 25.1 da Convenção de Budapeste:

> Artigo 14.2
>
> 2 Salvo disposição em contrário constante do artigo 21º, cada Parte aplicará os poderes e procedimentos referidos no n.º 1:
>
> a às infrações penais em conformidade com o disposto nos artigos 2º a 11º da presente Convenção;
>
> b a outras infrações penais cometidas por meio de um sistema informático; e
>
> c à recolha de provas eletrónicas de qualquer infração penal.
>
> Artigo 25.1
>
> As Partes concederão entre si o auxílio mútuo mais amplo possível para efeitos de investigações ou de procedimentos relativos a infrações penais relacionadas com sistemas e dados informáticos, ou para efeitos de recolha de provas sob a forma eletrónica de uma infração penal.

Os poderes e procedimentos previstos na Convenção estão submetidos às condições e salvaguardas do artigo 15º.

Disposições relevantes da Convenção de Budapeste sobre o Cibercrime (STE 185)

Disposições procedimentais

Os poderes e procedimentos previstos na Convenção (artigos 14º a 21º) podem ser aplicados no quadro de um inquérito ou processo penal específico em qualquer tipo de interferência eleitoral, tal como disposto no artigo 14º.

As medidas procedimentais específicas podem ser muito úteis nos inquéritos penais em matéria de interferência eleitoral. Por exemplo, neste tipo de casos, em que um sistema informático pode ser utilizado para cometer ou facilitar uma infração, a prova desta infração pode ser guardada sob forma eletrónica ou um suspeito poder ser identificável graças a informações sobre o assinante, incluindo um endereço IP. Da mesma forma, o financiamento político ilegal pode ser rastreável através da conservação de correio eletrónico, comunicações de voz entre conspiradores podem ser captadas no seguimento de uma interceção devidamente autorizada e a utilização abusiva de dados pode ser ilustrada por pistas eletrónicas.

Assim, nos inquéritos penais sobre interferência eleitoral, as Partes podem servir-se dos seus poderes para ordenar a conservação rápida dos dados

informáticos guardados, injunções para produção de provas, busca e apreensão de dados informáticos guardados, assim como de outras ferramentas que permitem a recolha das provas eletrónicas necessárias para os fins de investigação e processamento penal destas infrações relacionadas com a interferência eleitoral.

Disposições sobre auxílio judiciário mútuo internacional

Os poderes previstos pela Convenção em matéria de cooperação internacional (artigos 23º a 35º) são de um âmbito similar e poderão ajudar as Partes em investigações sobre a interferência eleitoral.

Assim, as Partes implementarão as ações necessárias – conservação rápida dos dados informáticos guardados, injunções para produção de provas, busca e apreensão de dados informáticos guardados, bem como outras disposições de cooperação internacional.

Disposições do direito penal substantivo

Por fim, como notámos acima, a interferência eleitoral pode envolver os seguintes tipos de comportamento (quando desprovidos de fundamento legal) criminalizados pela Convenção sobre o Cibercrime. O T-CY sublinha que os comportamentos abaixo são apenas exemplos – isto é, uma vez que a interferência eleitoral é um fenómeno que está a assumir maiores proporções, poderá manifestar-se de muitas formas não enumeradas abaixo. Contudo, o T-CY espera que a Convenção sobre o Cibercrime seja suficientemente flexível para as englobar.

Artigos relevantes	**Exemplos**
Artigo 2º – Acesso ilegítimo	Um sistema informático pode ser ilegalmente utilizado para obter informações sensíveis ou confidenciais relativas a candidatos, campanhas, partidos políticos ou eleitores.
Artigo 3º – Interceção ilegítima	Ao efetuar transmissões não públicas para, de ou no interior de um sistema informático, os dados informáticos podem ser intercetados ilegalmente para obter informações sensíveis ou confidenciais relativas a candidatos, campanhas, partidos políticos ou eleitores.
Artigo 4º – Interferência em dados	Os dados informáticos podem ser danificados, apagados, deteriorados, alterados ou suprimidos para modificar sítios web, alterar as bases de dados de eleitores ou falsificar os resultados das eleições, por exemplo manipulando as máquinas de votação.

Artigos relevantes	Exemplos
Artigo 5º – Interferência em sistemas	O funcionamento dos sistemas informáticos utilizados nas eleições ou campanhas eleitorais pode ser entravado para interferir nas mensagens da campanha, entravar a inscrição dos eleitores, desativar os dispositivos de voto ou impedir a contagem dos votos através de ataques de negação de serviço, software malicioso (malware) ou outros meios.
Artigo 6º – Uso abusivo de dispositivos	A venda, a obtenção para utilização, importação, a distribuição ou outras formas de disponibilização de palavras-passe, códigos de acesso ou dados similares permitindo o acesso a um sistema informático podem facilitar a interferência eleitoral (por exemplo, roubo de dados sensíveis de candidatos políticos, partidos ou campanhas).
Artigo 7º – Falsidade informática	Dados informáticos (por exemplo, os dados das listas eleitorais) podem ser introduzidos, alterados, apagados ou suprimidos de forma que os dados não autênticos são tomados em conta ou utilizados para fins legais como se fossem autênticos. Por exemplo, certos países exigem que as campanhas eleitorais façam divulgações públicas da sua situação financeira. A falsificação de dados informáticos poderá dar a impressão de divulgações incorretas ou esconder fontes duvidosas de fundos de campanha.
Artigo 11º – Tentativa e cumplicidade	A tentativa de cometer qualquer uma das infrações definidas no tratado ou qualquer ato de cumplicidade por auxílio ou instigação, tendo em vista exercer uma interferência eleitoral.
Artigo 12º – Responsabilidade de pessoas coletivas	As infrações cobertas pelos artigos 2º-11º da Convenção podem ser cometidas visando exercer uma interferência eleitoral por pessoas coletivas que poderiam ser consideradas responsáveis nos termos do artigo 12º.

Artigos relevantes	Exemplos
Artigo 13º – Sanções e medidas	As infrações abrangidas pela Convenção podem constituir uma ameaça para os indivíduos e a sociedade, especialmente quando as infrações são dirigidas contra fundamentos da vida política como as eleições. Os atos criminosos e os seus efeitos podem diferir de país para país, mas a interferência eleitoral pode minar a confiança nos processos democráticos, alterar o resultado de uma eleição, obrigar a organizar um segundo escrutínio com os custos e as eventuais perturbações que isso comporta, ou causar violência física entre membros dos vários partidos políticos e as comunidades. Uma Parte pode prever no seu direito interno uma sanção demasiado leve para atos visados nos artigos 2º
	a 11º cometidos no quadro de eleições e pode não autorizar a tomada em conta de circunstâncias agravantes ou de tentativa, instigação ou cumplicidade. Neste caso, a Parte referida deveria considerar introduzir alterações na sua legislação nacional. As Partes devem assegurar, nos termos do artigo 13º, que as infrações penais ligadas a estes atos "sejam passíveis de sanções eficazes, proporcionais e dissuasivas, incluindo as penas privativas de liberdade." As Partes podem igualmente considerar circunstâncias agravantes, por exemplo se tais atos afetarem de forma significativa uma eleição ou causarem mortes ou ferimentos ou danos materiais significativos.

Declaração do T-CY

O T-CY concorda que as infrações substantivas definidas na Convenção são igualmente suscetíveis de constituir atos de interferência eleitoral, tal como definidos na legislação aplicável, isto é, atos atentatórios de eleições livres, justas e transparentes.

As infrações substantivas definidas na Convenção podem ser cometidas com a finalidade de facilitar, participar em, ou preparar atos de interferência eleitoral.

As ferramentas procedimentais e de auxílio judiciário mútuo da Convenção podem ser utilizadas para investigar a interferência eleitoral, a sua facilitação, a participação na mesma ou os atos preparatórios dessa interferência.

Nota de orientação sobre aspetos do *ransomware* abrangidos pela Convenção de Budapeste[71]

Introdução

Na sua 8.ª reunião plenária (dezembro de 2012), o Comité da Convenção sobre o Cibercrime (TCY) decidiu publicar notas de orientação destinadas a facilitar a utilização e a implementação eficazes da Convenção sobre o Cibercrime, nomeadamente à luz dos desenvolvimentos jurídicos, políticos e tecnológicos[72].

As Notas de orientação refletem uma análise da aplicação da Convenção de Budapeste comum a todas as suas Partes.

Há décadas que os infratores cometem diferentes formas de cibercrime para extorquir resgates de organizações e indivíduos. Por exemplo, o roubo e a subsequente ameaça de divulgação pública de dados pessoais ou de outras informações sensíveis para coagir ao pagamento de resgates ainda prevalecem. No entanto, ao longo da última década, surgiram formas mais complexas de *ransomware* e infrações conexas. Estas envolvem a encriptação de dados ou sistemas informáticos, bloqueando assim os utilizadores, seguida de pedidos de resgate em troca do restabelecimento (a promessa de) do acesso. Os infratores podem também ameaçar divulgar informações sensíveis ou pessoais, numa tentativa de obter, mais eficazmente, os pagamentos das vítimas.

Tais infrações de *ransomware* são possíveis porque a tecnologia permite:

- uma encriptação forte dos dados ou sistemas informáticos das vítimas;
- a utilização de sistemas de comunicação difíceis de rastrear para enviar pedidos de pagamento de resgate, bem como ferramentas de desencriptação;
- o pagamento de resgates de uma forma difícil de rastrear, por exemplo através de moedas virtuais que sãomais fáceis de ocultar do que as moedas fiduciárias tradicionais.

Os ataques "WannaCry" e "NotPetya" de 2016/2017 afetaram computadores e atraíram uma grande atenção em todo o mundo. A pandemia de COVID-19, a partir de 2020, conduziu a uma maior dependência das sociedades das tecnologias da informação e da comunicação, aumentando as oportunidades de exploração para fins criminosos. Esta situação contribuiu para um novo

71. Adotado pela 27.ª sessão plenária do T-CY (29-30 de novembro de 2022).
72. Ver o mandato do T-CY (Artigo 46.º da Convenção de Budapeste).

aumento das infrações de *ransomware*. Alegadamente, os ataques contra os sistemas informáticos dos hospitais conduziram à morte de doentes. Além disso, as infrações de *ransomware* contra infraestruturas críticas causaram a declaração de uma emergência nacional na Costa Rica em abril de 2022. A utilização de *ransomware* é agora considerada uma forma grave de cibercrime que afeta os interesses fundamentais dos indivíduos, das empresas, das sociedades e dos governos.

Por conseguinte, na sua 26.ª sessão plenária (10-11 de maio de 2022), o T-CY decidiu elaborar uma Nota de orientação para mostrar de que forma os aspetos das infrações de *ransomware* são criminalizados ao abrigo das disposições de direito penal substantivo da Convenção sobre o Cibercrime e de que modo os poderes e as disposições processuais em matéria de cooperação internacional deste tratado podem ser utilizados para investigar, processar judicialmente e cooperar contra infrações de *ransomware*.

As presentes Notas de orientação fazem igualmente referência ao Segundo Protocolo Adicional à Convenção sobre o Cibercrime (STCE 224) que proporcionará instrumentos adicionais para "reforçar a cooperação e a divulgação de provas sob a forma eletrónica" às Partes neste Protocolo assim que este entrar em vigor.

As anteriores Notas de orientação do T-CY sobre *malware*, *botnets*, usurpação de identidade e ataques a infraestruturas críticas continuam também a ser pertinentes no que diz respeito às infrações de *ransomware*.

Infrações de *ransomware*

O *ransomware* é um tipo de *malware* concebido para recusar o acesso de um utilizador aos seus dados informáticos ou ao seu sistema informático através da encriptação desses dados ou sistemas. É depois solicitado ao utilizador visado que pague um resgate pelo restabelecimento (a promessa de) do acesso aos dados ou ao sistema.

As infrações de *ransomware* envolvem normalmente:

Atos preparatórios, incluindo:

- a produção, venda, obtenção ou qualquer outra forma de colocação à disposição de *ransomware*, ou seja, de um "dispositivo" na aceção do artigo 6.º da Convenção sobre o Cibercrime;
- a produção, venda, obtenção ou qualquer outra forma de colocação à disposição de outros dispositivos, na aceção do artigo 6.º, que sejam

utilizados na preparação de infrações de *ransomware*, tais como *malware* para obter acesso não autorizado aos sistemas de vítimas, ou *botnets* para a distribuição de *ransomware*;

- a obtenção de listas de distribuição ou outras informações pertinentes sobre os alvos. Alguns desses atos preparatórios podem constituir, eles próprios, infrações ou podem ser considerados como tentativa ou cumplicidade em crimes de *ransomware*, como a exfiltração de bases de dados que utilizam dispositivos de vigilância (*keyloggers*), a utilização de *botnets* ou a usurpação de identidade[73].

Distribuição ou instalação de *ransomware*, incluindo:

- através de e-mails com anexos que contenham o *malware* ou visando os utilizadores de aplicações de mensagens com hiperligações incorporadas nas mensagens. Incentivar os utilizadores a acederem a esses anexos ou hiperligações – e, por conseguinte, a instalarem o *malware* – pode ser ainda mais facilitado através de engenharia social ou de outras técnicas de usurpação de identidade;
- através do acesso remoto a um sistema informático.

Encriptação do sistema informático, ou de partes do mesmo, ou dos dados através de *ransomware*, impedindo assim o utilizador de aceder aos dados ou sistema ou de os utilizar de qualquer outra forma.

Solicitar, obter e transferir o pagamento de resgate, incluindo:

- solicitar o resgate em troca do (promessa de) restabelecimento do acesso aos dados e/ou ao sistema, o que equivale a extorsão ou chantagem, mas eventualmente também a outras infrações;
- comunicação entre o infrator e o alvo através de meios de comunicação de rastreio difícil, incluindo a utilização de TOR. As ferramentas de desencriptação também podem ser comunicadas desta forma;
- obtenção do resgate de uma forma que dificulte o seu rastreio, em geral, sob a forma de criptomoeda, frequentemente seguida do branqueamento dos produtos para ocultar ainda mais a identidade do autor do crime e dos respetivos produtos.

Desde 2021, o mercado de *ransomware* está cada vez mais organizado e profissional, oferecendo um modelo de negócio frequentemente designado como "*ransomware* como um serviço" (*ransomware-as-a-service* – ou RaaS)

73. Ver Notas de orientação (coe.int) pertinentes.

para cometer infrações de *ransomware*. Este modelo de negócio deu origem a criminosos informáticos, que incluem serviços independentes, como negociar pagamentos, prestar assistência às vítimas na realização de pagamentos e alguns serviços que oferecem um centro de ajuda disponível 24 horas por dia 7 dias por semana para acelerar os pagamentos de resgate e ajuda a restabelecer os sistemas ou dados encriptados.

Disposições relevantes da Convenção sobre o Cibercrime (STCE 185)

Criminalização das infrações relacionadas com *ransomware*

Ao abrigo da Convenção sobre o Cibercrime, cada Parte adotará as medidas legislativas e outras que se revelem necessárias para estabelecer determinadas infrações penais, em conformidade com o seu direito interno, quando cometidas intencional e ilegitimamente. Os artigos seguintes e as infrações correspondentes ao abrigo do direito interno das Partes que aplicam a Convenção serão pertinentes para as investigações e processos penais relativos a infrações de *ransomware*.

Artigos pertinentes	**Exemplos**
Artigo 2.º – Acesso ilícito	As infrações de *ransomware* envolvem o acesso ilícito a um sistema informático de uma vítima e, por conseguinte, uma infração penal nos termos do artigo 2.º.
Artigo 3.º – Interceção ilícita	As variantes de *ransomware* podem incluir a capacidade de intercetar transmissões não públicas de dados informáticos para, de ou dentro de um sistema informático. A obtenção de informações sobre os alvos ou de credenciais de acesso pode também envolver o crime de interceção ilícita.
Artigo 4.º – Interferência nos dados	O *ransomware* é especificamente concebido para interferir nos dados informáticos, pelo que a sua utilização constitui uma infração penal nos termos do artigo 4.º.
Artigo 5.º – Interferência no sistema	O *ransomware* pode ser concebido para interferir no funcionamento de um sistema informático, pelo que a sua utilização constitui uma infração penal nos termos do artigo 5.º.

Artigos pertinentes	**Exemplos**
Artigo 6.º – Uso abusivo de dispositivos	O *ransomware* é um *malware* e, por conseguinte, um dispositivo "concebido ou adaptado essencialmente para permitir a prática de qualquer das infrações definidas em conformidade com os artigos 2.º a 5.º". Assim, a "produção, a venda, a obtenção para utilização, a importação, a distribuição, ou outras formas de colocação à disposição" de *ransomware* constitui uma infração penal nos termos do artigo 6.º.
Artigo 7.º – Falsidade informática	A fim de obter acesso ilícito aos sistemas das vítimas, os intervenientes no *ransomware* utilizam frequentemente o *phishing* e outras técnicas de engenharia social – que, em certos casos, podem constituir falsidade informática – que criam dados não autênticos com a intenção de que estes sejam considerados ou utilizados para fins legais como se fossem autênticos.
Artigo 8.º – Burla informática	As infrações de *ransomware* provocam a perda de bens ao interferir com dados informáticos e/ou o funcionamento de um sistema informático com a intenção fraudulenta ou com dolo, com vista a obter, ilegitimamente, um benefício económico.
Artigo 11.º – Tentativa e cumplicidade	As infrações previstas no tratado podem assumir a forma de tentativa e cumplicidade para servir infrações relacionadas com *ransomware*. Podem implicar o envolvimento de diferentes pessoas, por exemplo, na produção, obtenção ou qualquer outra forma de colocação à disposição de *ransomware*, ou na obtenção de informações sobre os alvos.
Artigo 12.º – Responsabilidade das pessoas coletivas	As infrações de *ransomware* abrangidas pelos artigos 2.º a 11.º da Convenção, tal como acima descrito, podem ser realizadas por pessoas coletivas, que seriam declaradas responsáveis nos termos do artigo 12.º.

Artigos pertinentes	Exemplos
Artigo 13.º – Sanções	As infrações relacionadas com *ransomware* que são crimes abrangidos pela Convenção podem representar uma ameaça significativa para as pessoas e para a sociedade, em especial quando os crimes são dirigidos contra infraestruturas críticas de informação e constituem um risco significativo para a vida ou a segurança de qualquer pessoa singular. Por conseguinte, nos termos do artigo 13.º, as Partes deverão assegurar que as infrações penais relacionadas com tais atos "sejam passíveis de sanções eficazes, proporcionais e dissuasivas, incluindo as penas privativas de liberdade". Tal inclui a garantia de que, ao abrigo do seu direito interno, as sanções disponíveis são apropriadas tendo em conta a ameaça que o *ransomware* representa e têm em conta toda a gama de responsabilidade penal, nomeadamente com base na tentativa e cumplicidade na atividade criminosa. As Partes podem igualmente considerar penas mais graves quando existam circunstâncias agravantes, por exemplo, se esses atos afetarem significativamente o funcionamento de infraestruturas críticas ou provocarem a morte ou lesões corporais de uma pessoa singular ou danos materiais significativos.

Por conseguinte, as infrações de *ransomware* podem incluir condutas que devem ser criminalizadas nos termos dos artigos 2.º a 8.º, bem como nos termos do artigo 11.º (tentativa e cumplicidade), e que podem também envolver a responsabilidade das pessoas coletivas nos termos do artigo 12.º da Convenção sobre o Cibercrime.

As atividades de *ransomware* podem abranger um vasto leque de outras infrações ao abrigo do direito penal interno.

Disposições processuais

Nos termos da Convenção sobre o Cibercrime, "[c]ada Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes a" tomar determinadas medidas processuais para investigar as infrações em conformidade com os artigos 2.º a 11.º da Convenção e recolher provas sob forma eletrónica (ver artigo 14.º da Convenção). Estas podem também ser utilizadas para investigações e processos penais relacionados com infrações de *ransomware*.

Artigos pertinentes	Exemplos
Artigo 14º – Âmbito de aplicação das disposições processuais	Os poderes processuais da Convenção (artigos 16.º a 21.º) podem ser utilizados numa investigação ou processo penal específico, não só no que diz respeito às infrações acima referidas ao abrigo da Convenção, mas também no que se refere à recolha de provas sob forma eletrónica de qualquer outra infração relacionada com *ransomware*, tal como definida no direito interno de uma Parte.
Artigo 15.º – Condições e salvaguardas	Estas condições e salvaguardas aplicam-se igualmente às investigações e processos penais relacionados com infrações de *ransomware*.
Artigo 16.º – Preservação expedita de dados informáticos armazenados	Este poder pode ser utilizado para a preservação expedita de dados informáticos armazenados em computadores no tocante a infrações de *ransomware*, incluindo, por exemplo, dados sobre a fonte ou o percurso da distribuição do *ransomware* ou de comunicações que solicitem um resgate ou forneçam ferramentas de desencriptação, se for caso disso. Este poder pode também ser utilizado para ordenar a preservação de outros dados relacionados com infrações de *ransomware*, tais como comunicações entre suspeitos ou dados armazenados por suspeitos que possam constituir prova de tais infrações.
Artigo 17.º – Preservação expedita e divulgação parcial de dados de tráfego	Este poder pode ser utilizado para obter, de forma expedita, uma quantidade suficiente de dados de tráfego para identificar outros fornecedores de serviços e o percurso através do qual foram transmitidas comunicações relacionadas com infrações de *ransomware*.
Artigo 18.º – Injunção	Nos termos do artigo 18.º, as injunções podem ser utilizadas para ordenar a uma pessoa a produção de dados informáticos armazenados, relacionados com infrações de *ransomware*. Tal pode incluir fornecedores de serviços, instituições financeiras, nomeadamente fornecedores de serviços e plataformas de ativos virtuais, e outras pessoas singulares ou coletivas. Estas injunções são fundamentais para a obtenção, por exemplo, de informações sobre subscritores de fornecedores relacionadas com contas e infraestruturas associadas ao *ransomware*.

Artigos pertinentes	Exemplos
Artigo 19.º – Busca e apreensão de dados informáticos armazenados	As disposições em matéria de busca e apreensão nos termos do artigo 19.º podem ser utilizadas para a busca e apreensão de dados informáticos armazenados relacionados com infrações de *ransomware*.
Artigo 20.º – Recolha em tempo real de dados relativos ao tráfego	Os poderes previstos no artigo 20.º podem ser utilizados para a recolha em tempo real de dados relativos ao tráfego relacionados com infrações de *ransomware*.
Artigo 21.º – Interceção de dados relativos ao conteúdo	Os poderes previstos no artigo 21.º podem ser utilizados para a interceção de determinados dados relativos ao conteúdo e relacionados com infrações de *ransomware*, como, por exemplo, comunicações entre suspeitos.

Assim, em investigações ou processos penais relacionados com infrações de *ransomware*, as Partes podem recorrer à preservação expedita dos dados informáticos armazenados, injunções, ordens de busca e apreensão dos dados informáticos armazenados e outras ferramentas para recolher provas sob a forma eletrónica.

Disposições em matéria de cooperação internacional

Artigos pertinentes	Exemplos
Princípios e procedimentos gerais relativos à cooperação internacional ao abrigo do artigo 23.º a 28.º	Os princípios e procedimentos gerais para a cooperação internacional previstos nos artigos 23.º a 28.º da Convenção – ou seja, em matéria de extradição, assistência mútua e outros – são igualmente aplicáveis às infrações relacionadas com *ransomware*. O artigo 26.º pode ser particularmente útil na medida em que uma Parte que esteja na posse de informação valiosa sobre infrações de *ransomware* obtida através das suas próprias investigações pode, dentro dos limites do seu direito interno, transmitir essa informação à outra Parte sem pedido prévio (ver ponto 260 do Relatório Explicativo da Convenção sobre o Cibercrime). Nos termos do artigo 23.º e do artigo 25.º, n.º 1, as Partes na Convenção devem cooperar entre si, em conformidade com o disposto nos artigos 23.º a 28.º, "da forma mais ampla possível para efeitos de investigações ou de procedimentos relativos a infrações penais relacionadas com sistemas e dados informáticos" e para "efeitos de recolha de provas sob a forma eletrónica de uma infração penal".
Disposições específicas relativas à cooperação ao abrigo dos artigos 29.º a 35.º.	As disposições específicas do capítulo III da Convenção estão disponíveis para a cooperação internacional e a recolha de provas relacionadas com infrações de *ransomware*: – Artigo 29.º – Preservação expedita de dados informáticos armazenados – Artigo 30.º – Divulgação expedita dos dados de tráfego preservados – Artigo 31° – Assistência mútua relativamente ao acesso a dados informáticos armazenados – Artigo 32.º – Acesso transfronteiriço aos dados informáticos armazenados, mediante consentimento ou quando sejam acessíveis ao público – Artigo 33.° – Assistência mútua relativa à recolha de dados de tráfego em tempo real – Artigo 34.° – Assistência mútua em matéria de interceção de dados de conteúdo – Artigo 35.º – Rede 24/7

Tendo em conta que as infrações de *ransomware* envolvem normalmente infratores, alvos e vítimas, fornecedores de serviços, instituições financeiras ou sistemas informáticos em várias jurisdições, a utilização eficaz destas disposições de cooperação internacional é particularmente importante.

Segundo Protocolo Adicional à Convenção sobre o Cibercrime (STCE 224)

Em 12 de maio de 2022, o Segundo Protocolo Adicional à Convenção sobre o Cibercrime (STCE 224) foi aberto para assinatura. Uma vez em vigor, este instrumento dotará as Partes de instrumentos adicionais para "o reforço da cooperação e da divulgação de provas sob a forma eletrónica". Estes serão pertinentes e, em alguns casos, altamente relevantes para as investigações e processos penais relacionados com infrações de *ransomware*, e incluem:

- Artigo 6.º – Pedido de informação sobre o registo de nomes de domínio diretamente a uma entidade de outra Parte que preste serviços de registo de nomes de domínio;
- Artigo 7.º – Divulgação de informação sobre subscritores através da cooperação direta com um fornecedor de serviços de outra Parte;
- Artigo 8.º – Execução de injunções de outra Parte para a apresentação expedita de informação sobre subscritores e dados de tráfego;
- Artigo 9.º – Divulgação expedita de dados informáticos armazenados em caso de emergência;
- Artigo 10.º – Assistência mútua de emergência;
- Artigo 11.º – Videoconferência;
- Artigo 12.º – Equipas de investigação conjuntas e investigações conjuntas.

O âmbito de aplicação do presente Protocolo é, mais uma vez, abrangente, na medida em que se aplica não só às infrações penais relacionadas com sistemas e dados informáticos, mas também à recolha de provas sob forma eletrónica de qualquer infração penal (ver artigo 2.º, n.º 1, alínea a)).

As condições e as salvaguardas do artigo 13.º asseguram que o estabelecimento, a execução e a aplicação dos poderes e procedimentos previstos no presente Protocolo estejam sujeitos às condições e salvaguardas previstas no direito interno de cada Parte, que devem assegurar a proteção adequada dos direitos humanos e das liberdades. Além disso, tendo em conta 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 garantam, assim, que os dados pessoais podem ser transferidos quando se recorre a essas formas expeditas de cooperação.

Declaração do T-CY

O T-CY acorda que:

- as infrações relacionadas com ataques de *ransomware* podem incluir condutas que devem ser criminalizadas nos termos dos artigos 2.º a 8.º, bem como nos termos do artigo 11.º (tentativa e cumplicidade), e que podem envolver a responsabilidade das pessoas coletivas nos termos do artigo 12.º da Convenção sobre o Cibercrime;
- as medidas processuais e os instrumentos de cooperação internacional da Convenção podem ser utilizados para investigar e processar judicialmente os ataques de *ransomware* e infrações conexas, bem como a sua facilitação e participação nessas infrações ou atos preparatórios;
- o Segundo Protocolo Adicional à Convenção sobre o Cibercrime, uma vez em vigor, dotará as suas Partes de instrumentos adicionais para o reforço da cooperação e da divulgação de provas sob a forma eletrónica relacionadas com ataques de *ransomware*.

Nota de Orientação sobre o Âmbito dos poderes processuais e das disposições em matéria de cooperação internacional da Convenção de Budapeste[74]

1. Introdução

Na sua 8ª sessão plenária (dezembro 2012), o Comité da Convenção sobre o Cibercrime (T-CY) decidiu publicar Notas de Orientação destinadas a facilitar a utilização e a implementação eficazes da Convenção de Budapeste sobre o Cibercrime, nomeadamente à luz dos desenvolvimentos jurídicos, políticos e tecnológicos[75]. As Notas de Orientação refletem uma análise da aplicação da Convenção de Budapeste comum a todas as suas Partes.

A presente nota aborda o âmbito dos poderes processuais nacionais e das disposições em matéria de cooperação internacional da Convenção sobre o Cibercrime (STE 185), bem como do seu Segundo Protocolo Adicional relativo ao reforço da cooperação e divulgação de provas sob a forma eletrónica (STCE 224).

Embora o texto da Convenção sobre o Cibercrime seja bastante claro que os poderes processuais e as disposições em matéria de cooperação internacional são aplicáveis não só ao cibercrime (artigos 2.º a 11.º da Convenção), mas também a "outras infrações cometidas por meio de um sistema informático"; e para "efeitos de recolha de provas sob a forma eletrónica de uma infração penal" (ver artigo 14.º, n.º 2, alíneas b) e c), e artigos 23.º e 25.º STE 185), e embora tal seja confirmado de novo no Segundo Protocolo Adicional à Convenção (ver artigo 2.º do STCE 224), este âmbito nem sempre é plenamente compreendido, e a legislação de alguns países limita a aplicação dos poderes processuais ou das disposições em matéria de cooperação internacional a um conjunto de cibercrimes.

Por conseguinte, o T-CY decidiu que uma Nota de Orientação que sublinhe a forma como as principais disposições processuais e de cooperação internacional poderiam ser aplicadas não só às infrações contra e por meio de sistemas informáticos, mas também a uma série de infrações, teria benefícios práticos e estratégicos.

74. Adotado pela 28.ª sessão plenária do T-CY (27-28 de junho de 2023).
75. Ver o mandato do T-CY (artigo 46.º da Convenção de Budapeste).

2. Disposições relevantes da Convenção sobre o Cibercrime (STE 185)

2.1 Disposições processuais

Nos termos da Convenção sobre o Cibercrime, "[c]ada Parte adotará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes a" tomar as medidas processuais estabelecidas nos artigos 16.º a 21.º da Convenção:

- Artigo 16.º – Preservação expedita de dados informáticos armazenados
- Artigo 17.º – Preservação expedita e divulgação parcial de dados de tráfego
- Artigo 18.º – Injunção
- Artigo 19.º – Busca e apreensão de dados informáticos armazenados
- Artigo 20.º – Recolha em tempo real de dados relativos ao tráfego
- Artigo 21.º – Interceção de dados relativos ao conteúdo

Estas medidas estão sujeitas às condições e salvaguardas previstas no artigo 15.º.

O âmbito destas medidas processuais é definido no artigo 14.º:

> **Artigo 14.º – Âmbito de aplicação das disposições processuais**
>
> 1 Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para instituir os poderes e os procedimentos previstos na presente secção, para fins de investigação ou de procedimento criminal específico.
>
> 2 Salvo disposição em contrário constante do artigo 21.°, cada Parte aplicará os poderes e procedimentos referidos no n.º 1:
>
> a) às infrações penais previstas nos artigos 2.º a 11.º da presente Convenção;
>
> b) a outras infrações penais cometidas por meio de um sistema informático; e
>
> c) à recolha de provas sob a forma eletrónica, relativamente à prática de qualquer infração penal.
>
> 3 a) Cada Parte poderá reservar-se o direito de só aplicar as medidas previstas no artigo 20.º às infrações ou categorias de infrações especificadas na reserva, desde que o conjunto de tais infrações ou categorias de infrações não seja mais reduzido que o conjunto de infrações a que aplica as medidas previstas no artigo 21.º. Cada Parte procurará limitar tal reserva por forma a permitir a aplicação mais ampla possível da medida prevista no artigo 20.º.
>
> b) Sempre que uma Parte, por força das restrições impostas pela sua legislação vigente à data da adoção da presente Convenção, não se encontrar

em condições de aplicar as medidas previstas nos artigos 20.º e 21.º às comunicações transmitidas num sistema informático de um fornecedor de serviços, que:

i. esteja em funcionamento para benefício de um grupo fechado de utilizadores, e

ii. não utilize redes públicas de telecomunicações e não esteja ligado a outro sistema informático, quer seja público ou privado, essa Parte pode reservar-se o direito de não aplicar essas medidas às referidas comunicações. Cada Parte procurará limitar uma tal reserva por forma a permitir a aplicação mais ampla possível das medidas previstas nos artigos 20.º e 21.º.

Por conseguinte, nos termos do artigo 14.º, n.º 2, da Convenção, os poderes processuais são aplicáveis à recolha de provas sob a forma eletrónica de qualquer infração penal. Fica, deste modo, "assegurada a obtenção ou recolha de provas sob a forma eletrónica relativamente a uma infração penal, em virtude da aplicação dos poderes e procedimentos estabelecidos na presente Secção" da Convenção (n.º 141 do Relatório Explicativo da Convenção).

O artigo 14.º, n.º 3, prevê exceções a este vasto âmbito de aplicação e permite às Partes restringir o âmbito de poderes mais intrusivos (recolha em tempo real de dados relativos ao tráfego ao abrigo do artigo 20.º e interceção de dados relativos ao conteúdo nos termos do artigo 21.º)[76].

Consequentemente, as autoridades competentes podem ordenar a preservação dos dados, ordenar a produção de dados, buscar ou apreender dados informáticos armazenados, encomendar ou efetuar a recolha em tempo real de dados relativos ao tráfego ou a interceção de dados relativos ao conteúdo[77] em investigações criminais específicas relacionadas com qualquer infração cometida ao abrigo do direito nacional, incluindo, por exemplo[78]:

- corrupção;
- contrafação de medicamentos ou outras ameaças à saúde pública, incluindo infrações relacionadas com a COVID-19;
- diferentes formas de abuso infantil;

76. Ver reservas e declarações das Partes no que se refere ao artigo 14.º.
77. Tal como indicado nos artigos 20.º e 21.º da Convenção, podem aplicar-se restrições aos poderes de recolha em tempo real de dados relativos ao tráfego e à interceção de dados relativos ao conteúdo, como a limitação a uma série de infrações graves.
78. Ver também as referências a seguir relativas aos tratados internacionais pertinentes que abrangem algumas destas infrações.

- diferentes formas de violência doméstica e violência contra as mulheres;
- diferentes formas de crimes económicos e financeiros;
- infrações relacionadas com droga;
- fraude;
- rapto;
- manipulação de competições desportivas;
- branqueamento de capitais e financiamento do terrorismo;
- homicídio;
- infrações relacionadas com o crime organizado;
- violação e outras formas de violência sexual;
- terrorismo;
- genocídio, crimes contra a humanidade, crimes de guerra e outros crimes internacionais;
- tráfico de seres humanos;
- xenofobia e racismo e outras formas criminosas de discurso de ódio.

2.2 Disposições em matéria de cooperação internacional

O âmbito abrangente dos poderes processuais nacionais é alargado aos princípios e medidas relacionados com a cooperação internacional (Capítulo III da Convenção). Os artigos 23.º e 25.º esclarecem que a cooperação não só é possível para efeitos de investigações ou processos relativos a infrações penais relacionadas com sistemas informáticos e dados informatizados, mas também para a recolha de provas sob a forma eletrónica de qualquer infração penal:

> **Artigo 23.º – Princípios gerais relativos à cooperação internacional**
>
> As Partes cooperarão entre si, em conformidade com as disposições do presente capítulo, em aplicação dos instrumentos internacionais pertinentes sobre a cooperação internacional em matéria penal, de acordos celebrados com base nas legislações uniformes ou recíprocas, e do seu direito interno, na medida mais ampla possível, para efeitos de investigações ou de procedimentos relativos a infrações penais relacionadas com sistemas informáticos e dados informatizados, ou para recolher provas sob a forma eletrónica de uma infração penal.
>
> **Artigo 25.º – Princípios gerais relativos à assistência mútua**
>
> 1 As Partes concederão entre si a assistência mútua mais ampla possível para efeitos de investigações ou de procedimentos relativos a infrações penais

relacionadas com sistemas informáticos e dados informatizados, ou para efeitos de recolha de provas sob a forma eletrónica de uma infração penal.

O n.º 243 do Relatório Explicativo da Convenção confirma que:

> "a cooperação deverá estender-se a todas as infrações penais relacionadas com sistemas informáticos e dados informatizados (isto é, as infrações incluídas no artigo 14°, n.º 2, alíneas a e b), bem como à recolha de provas sob a forma eletrónica de uma dada infração penal. Tal significa que, tanto nos casos de infrações cometidas por meio da utilização de um sistema informático, como nos casos de infrações comuns não cometidas através da utilização de um sistema informático (por exemplo, um homicídio) mas que envolvam provas sob a forma eletrónica, serão pois aplicáveis os termos constantes do Capítulo III."

As Partes podem limitar este âmbito abrangente no que diz respeito à assistência mútua referente à recolha em tempo real de dados relativos ao tráfego (artigo 33.º) e à assistência mútua em matéria de interceção de dados relativos ao conteúdo (artigo 34.º). Além disso, a cooperação internacional pode estar sujeita a condições, tais como requisitos de dupla criminalidade[79] ou motivos de recusa, em conformidade com os artigos 25.º, n.º 4, 27.º, n.º 4 e 27.º, n.º 5 da Convenção[80].

Os princípios e medidas para a cooperação internacional relativos às infrações enunciadas na Convenção e outras infrações penais cometidas por meio de um sistema informático, bem como a recolha de provas sob a forma eletrónica de qualquer outra infração penal, estão previstos nos artigos 23.º a 35.º[81] da Convenção:

- Artigo 23.° – Princípios gerais relativos à cooperação internacional;
- Artigo 25.° – Princípios gerais relativos à assistência mútua;
- Artigo 26.º – Informação espontânea;

79. Ver o artigo 29.º, n.º 4 da Convenção.
Tal como referido no n.º 259 do Relatório Explicativo da Convenção, "...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".
80. O artigo 27.º, n.º 5 da Convenção refere-se aos motivos para o adiamento da execução de um pedido.
81. Nota: A obrigação de extradição ao abrigo do "Artigo 24.º – Extradição" somente será aplicável "às infrações penais definidas em conformidade com o disposto nos artigos 2.º a 11.º da Convenção, que sejam passíveis de punição em virtude da legislação adotada por ambas as Partes envolvidas, por meio da privação da liberdade por um período máximo de, pelo menos, um ano ou através da aplicação de uma pena mais grave".

- Artigo 27.º – Procedimentos relativos aos pedidos de assistência mútua na ausência de acordos internacionais aplicáveis;
- Artigo 28.º – Confidencialidade e restrição de utilização
- Artigo 29.º – Preservação expedita de dados informáticos armazenados;
- Artigo 30.º – Divulgação expedita dos dados de tráfego preservados;
- Artigo 31.° – Assistência mútua relativamente ao acesso a dados informáticos armazenados;
- Artigo 32.º – Acesso transfronteiriço aos dados informáticos armazenados, mediante consentimento ou quando sejam acessíveis ao público;
- Artigo 33.° – Assistência mútua relativa à recolha em tempo real de dados relativos ao tráfego;
- Artigo 34.° – Assistência mútua em matéria de interceção de dados relativos ao conteúdo;
- Artigo 35.º – Rede 24/7.

As Partes na Convenção podem utilizar estas medidas e princípios para cooperar entre si na medida mais abrangente possível para efeitos de investigações ou processos e de recolha de provas sob a forma eletrónica de qualquer infração penal, e solicitar a preservação dos dados, o acesso aos dados armazenados, a recolha em tempo real de dados relativos ao tráfego ou a interceção de dados relativos ao conteúdo[82], ou o acesso aos dados informatizados armazenados transfronteiriços, com o consentimento ou sempre que estejam disponíveis ao público, no que diz respeito a qualquer infração penal e nas condições previstas no Capítulo III da Convenção.

3. Disposições relevantes do Segundo Protocolo Adicional (STCE 224)

Em 12 de maio de 2022, o Segundo Protocolo Adicional à Convenção sobre o Cibercrime (STCE 224) foi aberto para assinatura. Uma vez em vigor, este instrumento dotará as Partes de instrumentos adicionais para "o reforço da cooperação e da divulgação de provas sob a forma eletrónica".

82. Tal como indicado nos artigos 20.º e 21.º da Convenção, podem aplicar-se restrições aos poderes de recolha em tempo real de dados relativos ao tráfego e à interceção de dados relativos ao conteúdo, como a limitação a uma série de infrações graves. No que diz respeito aos artigos 33.º e 34.º relativos à cooperação internacional, "Cada Parte concederá a assistência pelo menos no que diz respeito às infrações penais relativamente às quais seria possível a recolha, ao nível interno, em tempo real dos dados relativos ao tráfego em caso semelhante" (artigo 33.º, n.º 2), no tocante à interceção de dados relativos ao conteúdo "As Partes concederão assistência mútua, na medida em que é permitido pelos tratados e pelas legislações aplicáveis" (artigo 34.º).

O âmbito de aplicação do presente Protocolo é, mais uma vez, abrangente, e aplica-se não só às infrações penais relacionadas com sistemas informáticos e dados informatizados, mas também à recolha de provas sob forma eletrónica de qualquer infração penal:

> **Artigo 2.º – Âmbito de aplicação**
>
> 1 Salvo disposição em contrário no presente Protocolo, as medidas descritas no presente Protocolo são aplicáveis:
>
> a) entre as Partes na Convenção que são Partes no presente Protocolo, em investigações ou processos penais específicos relativos a infrações penais relacionadas com sistemas informáticos e dados informatizados e com a recolha de provas sob a forma eletrónica de uma infração penal; e
>
> b) entre as Partes no Primeiro Protocolo que são Partes no presente Protocolo, em investigações ou processos penais específicos relativos a infrações penais estabelecidas nos termos do Primeiro Protocolo.

As medidas previstas no presente Protocolo são as seguintes:

- Artigo 6.º – Pedido de informação sobre o registo de nomes de domínio diretamente a uma entidade de outra Parte que preste serviços de registo de nomes de domínio;
- Artigo 7.º – Divulgação de informação sobre subscritores através da cooperação direta com um fornecedor de serviços de outra Parte;
- Artigo 8.º – Execução de injunções de outra Parte para a apresentação expedita de informação sobre subscritores e dados de tráfego;
- Artigo 9.º – Divulgação expedita de dados informáticos armazenados em caso de emergência;
- Artigo 10.º – Assistência mútua de emergência;
- Artigo 11.º – Videoconferência;
- Artigo 12.º – Equipas de investigação conjuntas e investigações conjuntas.

Estas medidas estão sujeitas às condições e salvaguardas previstas nos artigos 13.º e 14.º do STCE 224.

Por conseguinte, as autoridades competentes das Partes no presente Protocolo podem – sujeitas às reservas e declarações autorizadas nos termos do artigo 19.º do STCE 224 – solicitar informação relativa ao registo do nome do domínio, ordenar a divulgação de informação sobre subscritores, executar injunções relativas a informação sobre subscritores e dados de tráfego, cooperar em situações de emergência, recorrer a videoconferência ou criar equipas de investigação conjuntas ou realizar investigações conjuntas relacionadas com

investigações criminais ou processos relativos a infrações penais referentes a sistemas informáticos e dados informatizados, bem como com a recolha de provas sob forma eletrónica de qualquer infração.

4. Sinergias entre a Convenção sobre o Cibercrime e outros tratados

As competências processuais internas e os princípios e medidas de cooperação internacional também podem ser utilizados para recolher provas sob a forma eletrónica relacionadas com infrações previstas noutros acordos internacionais em que os Estados sejam Partes, sob reserva das condições pertinentes acima referidas[83]. Esses acordos podem incluir os relativos à corrupção[84]; contrafação de medicamentos ou de outras ameaças à saúde pública[85]; abuso infantil[86]; violência doméstica e violência contra mulheres[87]; infrações relacionadas com droga[88]; manipulação de competições desportivas[89]; branqueamento de capitais e financiamento do terrorismo[90]; infrações relacionadas com o crime organizado[91];

83. Tais como requisitos de dupla criminalidade ou motivos de recusa, em conformidade com os artigos 25.º, n.º 4 e 27.º, n.º 4 da Convenção.
84. Por exemplo, a conduta criminal referida na Convenção de Direito Penal sobre a Corrupção (STE 173) do Conselho da Europa ou na Convenção das Nações Unidas contra a Corrupção.
85. Por exemplo, a conduta criminal referida na Convenção do Conselho da Europa relativa à contrafação de medicamentos e infrações semelhantes que constituem uma ameaça para a saúde pública (STCE 211)
86. Por exemplo, a conduta criminosa referida na Convenção do Conselho da Europa para a Proteção das Crianças contra a Exploração Sexual e os Abusos Sexuais (STCE 201)
87. Por exemplo, a conduta criminal referida na Convenção do Conselho da Europa para a Prevenção e o Combate à Violência Contra as Mulheres e a Violência Doméstica (STCE 210)
88. Por exemplo, a conduta criminosa referida nas Convenções das Nações Unidas relativas ao Controlo da Droga
89. Por exemplo, a conduta criminosa referida na Convenção do Conselho da Europa relativa à Manipulação das Competições Desportivas (STCE 215)
90. Por exemplo, a conduta criminosa referida na Convenção do Conselho da Europa relativa ao Branqueamento, Deteção, Apreensão e Perda dos Produtos do Crime e ao Financiamento do Terrorismo (STCE 198)
91. Por exemplo, a conduta criminosa referida na Convenção das Nações Unidas contra a Criminalidade Organizada Transnacional e seus Protocolos.

terrorismo[92]; tráfico de seres humanos[93] ou genocídio, crimes contra a humanidade, crimes de guerra e outros crimes internacionais[94].

No que se refere às Partes no Primeiro Protocolo Adicional à Convenção sobre o Cibercrime no que diz respeito à xenofobia e ao racismo através de sistemas informáticos (STE 189)[95], o artigo 8.º, n.º 2, estabelece que "As Partes tornarão extensível a aplicação das medidas estabelecidas nos artigos 14.º a 21.º e 23.º a 35.º da Convenção aos artigos 2.º a 7.º do presente Protocolo".

Em 2018, o T-CY recomendou que as Partes na Convenção de Lanzarote contra a Exploração Sexual e os Abusos Sexuais de Crianças (STCE 201) e da Convenção de Istambul para a Prevenção e o Combate à Violência Contra as Mulheres e a Violência Doméstica (STCE 210) fossem encorajadas a "introduzir os poderes processuais dos artigos 16.º a 21.º da Convenção de Budapeste no direito interno e a considerar a possibilidade de se tornarem Partes na Convenção de Budapeste para facilitar a cooperação internacional em matéria de provas sob a forma eletrónica (artigos 23.º a 35.º da Convenção de Budapeste) em relação à violência sexual contra crianças e à violência contra mulheres e violência doméstica"[96].

5. Declaração do T-CY

O T-CY concorda que as disposições em matéria de direito processual e os princípios e medidas de cooperação internacional da Convenção sobre o Cibercrime são aplicáveis não apenas às infrações relacionadas com sistemas informáticos e dados informatizados, mas também à recolha de provas sob a forma eletrónica de qualquer infração penal. Este vasto âmbito aplica-se igualmente às medidas do Segundo Protocolo Adicional da Convenção.

Este âmbito permite ainda sinergias entre a Convenção de Budapeste e outros acordos internacionais.

---

92. Por exemplo, a conduta criminosa referida na Convenção do Conselho da Europa para a Prevenção do Terrorismo (STCE 196) e seus Protocolos.
93. Por exemplo, a conduta criminosa referida na Convenção do Conselho da Europa relativa à Luta contra o Tráfico de Seres Humanos (STCE 197)
94. Por exemplo, a conduta referida na Convenção para a Prevenção e Repressão do Crime de Genocídio de 1948, nas quatro Convenções de Genebra sobre o Direito Humanitário Internacional e nos seus Protocolos Adicionais de 1949, ou no Estatuto de Roma do Tribunal Penal Internacional.
95. Protocolo adicional à Convenção sobre o Cibercrime relativo à incriminação de atos de natureza racista e xenófoba praticados através de sistemas informáticos (STE 189)
96. Ver o estudo do T-CY de mapeamento da ciberviolência https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914

PREMS 108923

POR

www.coe.int

O Conselho da Europa é a principal organização de defesa dos direitos humanos no continente. Integra 46 Estados membros, incluindo todos os membros da União Europeia. Todos os Estados membros do Conselho da Europa assinaram a Convenção Europeia dos Direitos do Homem, um tratado que visa proteger os direitos humanos, a democracia e o Estado de direito. O Tribunal Europeu dos Direitos do Homem controla a implementação da Convenção nos Estados membros.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE