Minuta do Relatório Explicativo

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.

---

[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

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 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.

<u>Utilização indevida de equipamentos (Artigo 6º)</u>

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 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.

---

[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.

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.

<u>Preservação expedita e divulgação parcial de dados de tráfego (artigo 17º)</u>

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, 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.

---

[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

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.

<u>Divulgação expedita dos dados de tráfego preservados (Artigo 30º)</u>

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[11] (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[12]. 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

[11] Consultar a Declaração Introdutória apresentada pelo CDPC ao Comité de Ministros sobre esta matéria
[12] 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.

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 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).

320. 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)

321. 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.

322. 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.

323. 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)

324. 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.

325. 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.

326. 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)

327. 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)

328. 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.

329. 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).

330. 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.

331. 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.