Projecto do Cibercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

25 de Março de 2010

Legislação do cyber crime

PORTUGAL

Este perfil legislativo foi preparado no âmbito do Projecto do Cibercrime do Conselho da Europa, tendo em vista a partilha de informação sobre legislação na área do cibercrime e a avaliação do presente estado de implementação da Convenção do Cibercrime na legislação nacional. Não reflecte necessariamente posições oficiais do país referido nem do Conselho da Europa.

Comentários podem ser mandados para:

Economic Crime Division
Directorate General of Human Rights and Legal Affairs
Council of Europe, Strasbourg, France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int
www.coe.int/cybercrime

País:	**Portugal**
Assinatura da Convenção:	23.11.2001
Ratificação/acessão:	24.03.2010
Disposições da Convenção	***Correspondentes disposições/soluções na legislação nacional*** *(por favor, cite ou sumarie brevemente; por favor, anexe os extractos que considere relevantes, como anexo)*
Capítulo I – Terminologia	

Artigo 1.º - Definições	**Artigo 2º - Definições**
Para efeitos da presente Convenção, entende-se por: a) «*Sistema informático*», um equipamento ou conjunto de equipamentos interligados ou relacionados entre si que asseguram, isoladamente ou em conjunto, pela execução de um programa, o tratamento automatizado de dados; b) «*Dados informáticos*», qualquer representação de factos, informações ou conceitos numa forma adequada para o processamento informático, incluindo um programa que permita a um sistema informático executar uma função; c) «Prestador *de serviços*»: i. Qualquer entidade pública ou privada que faculte aos utilizadores dos seus serviços a possibilidade de comunicarem por meio de um sistema informático; ii. Qualquer outra entidade que processe ou armazene dados informáticos em nome desse serviço de comunicações ou dos seus utilizadores. d) «D*ados de tráfego*», quaisquer dados informáticos relativos a uma comunicação efectuada por meio de um sistema informático, que foram gerados por um sistema informático enquanto elemento da cadeia de comunicação, e indicam a origem, o destino, o trajecto, a hora, a data, o tamanho e a duração da comunicação, ou o tipo de serviço subjacente.	Para efeitos da presente lei, considera-se: *a*) «Sistema informático», qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção; *b*) «Dados informáticos», qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função; *c*) «Dados de tráfego», os dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente; *d*) «Fornecedor de serviço», qualquer entidade, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático, bem como qualquer outra entidade que trate ou armazene dados informáticos em nome e por conta daquela entidade fornecedora de serviço ou dos respectivos utilizadores; *e*) «Intercepção», o acto destinado a captar informações contidas num sistema informático, através de dispositivos electromagnéticos, acústicos, mecânicos ou outros; *f*) «Topografia», uma série de imagens ligadas entre si, independentemente do modo como são fixadas ou codificadas, que representam a configuração tridimensional das camadas que compõem um produto semicondutor e na qual cada imagem reproduz o desenho, ou parte dele, de uma superfície do produto semicondutor, independentemente da fase do respectivo fabrico; *g*) «Produto semicondutor», a forma final ou intermédia de qualquer produto, composto por um substrato que inclua uma camada de material semicondutor e constituído por uma ou várias camadas de matérias condutoras, isolantes ou semicondutoras, segundo uma disposição conforme a uma configuração tridimensional e destinada a cumprir, exclusivamente ou não, uma função electrónica.

Capítulo II - Medidas a adoptar a nível nacional ***Secção 1 .- Direito penal material***	
Artigo 2.º – Acesso ilícito Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracção penal nos termos do seu direito interno, quando praticado intencionalmente, o acesso ilícito a um sistema informático no seu todo ou a parte dele. Para que se verifique a infracção penal, qualquer uma das Partes pode exigir que ela seja cometida por meio da violação das medidas de segurança com intenção de obter dados informáticos ou com qualquer outra intenção, ou ainda que esteja relacionada com um sistema informático conectado a outro sistema informático.	**Artigo 6º - Acesso ilegítimo** 1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias. 2 - Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior. 3 - A pena é de prisão até 3 anos ou multa se o acesso for conseguido através de violação de regras de segurança. 4 - A pena é de prisão de 1 a 5 anos quando: *a*) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; ou *b*) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado. 5 - A tentativa é punível, salvo nos casos previstos no nº 2. 6 - Nos casos previstos nos nºs 1, 3 e 5 o procedimento penal depende de queixa.
Artigo 3.º – Intercepção ilícita Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracção penal nos termos do seu Direito interno, quando praticada intencionalmente, a intercepção não autorizada, através de meios técnicos, de transmissões não públicas de dados informáticos, para, de ou dentro de um sistema informático, incluindo as radiações electromagnéticas emitidas por um sistema informático que transporte esses dados informáticos. Para que se verifique a infracção penal, qualquer uma das Partes pode exigir que ela seja cometida por meio da violação das medidas de segurança com intenção de obter dados informáticos ou com qualquer outra intenção, ou ainda que esteja relacionada com um sistema informático conectado a outro sistema informático.	**Artigo 7º - Intercepção ilegítima** 1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, e através de meios técnicos, interceptar transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinadas ou dele provenientes, é punido com pena de prisão até 3 anos ou com pena de multa. 2 - A tentativa é punível. 3 - Incorre na mesma pena prevista no nº 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no mesmo número.

Artigo 4.º – Dano provocado nos dados 1. Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracções penais nos termos do seu Direito interno, quando praticados intencionalmente, a danificação, o apagamento, a deterioração, a alteração ou supressão não autorizados de dados informáticos. 2. Qualquer uma das Partes pode reservar-se o direito de exigir que o comportamento descrito no n.º 1 do presente artigo tenha de ter acarretado danos graves.	**Artigo 4º - Dano relativo a programas ou outros dados informáticos** 1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afectar a capacidade de uso, é punido com pena de prisão até 3 anos ou pena de multa. 2 - A tentativa é punível. 3 - Incorre na mesma pena do n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas nesse número. 4- Se o dano causado for de valor elevado, a pena é de prisão até 5 anos ou de multa até 600 dias. 5 - Se o dano causado for de valor consideravelmente elevado, a pena é de prisão de 1 a 10 anos. 6 - Nos casos previstos nos nºs 1, 2 e 4 o procedimento penal depende de queixa.
Artigo 5.º – Sabotagem informática Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracção penal nos termos do seu Direito interno, quando praticada intencionalmente, a perturbação grave, não autorizada, do funcionamento de um sistema informático mediante inserção, transmissão, danificação, eliminação, deterioração, alteração ou supressão de dados informáticos.	**Artigo 5º - Sabotagem informática** 1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático, é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias. 2 - Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior. 3 - Nos casos previstos no número anterior, a tentativa não é punível. 4 - A pena é de prisão de 1 a 5 anos se o dano emergente da perturbação for de valor elevado. 5 - A pena é de prisão de 1 a 10 anos se: *a*) O dano emergente da perturbação for de valor consideravelmente elevado;

	b) A perturbação causada atingir de forma grave ou duradoura um sistema informático que apoie uma actividade destinada a assegurar funções sociais críticas, nomeadamente as cadeias de abastecimento, a saúde, a segurança e o bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos.
Artigo 6.º – Utilização indevida de dispositivos 1. Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracções penais nos termos do seu Direito interno, quando praticadas intencional e ilicitamente: a) A produção, venda, aquisição para efeitos de utilização, importação, distribuição, ou outras formas de disponibilização de: i) Um dispositivo, incluindo um programa informático, concebido ou adaptado antes de mais para permitir a prática de uma das infracções previstas nos artigos 2.º a 5.º supra; ii) Uma palavra-passe, um código de acesso ou dados similares que permitem aceder, no todo ou em parte, a um sistema informático, com a intenção de os utilizar para cometer qualquer uma das infracções previstas nos artigos 2.º a 5.º supra; e b) A posse de um dos elementos referidos na alínea a) (i) ou (ii), desde que utilizados com a intenção de cometer qualquer uma das infracções previstas nos artigos 2.º a 5.º. Qualquer uma das Partes pode exigir que para existir responsabilidade criminal nos termos do seu Direito interno tenha de se verificar um determinado número desses elementos. 2. O presente artigo não pode ser interpretado no sentido de determinar que existe responsabilidade criminal nos casos em que a finalidade da produção, venda, obtenção para utilização, importação, distribuição ou outras formas de disponibilização referidas no n.º 1 do presente artigo não é a prática de uma das infracções previstas nos artigos 2.º a 5.º da presente Convenção, mas antes a realização de testes autorizados ou a protecção de um sistema informático.	**Artigo 3º - Falsidade informática** 4- Quem importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, sobre o qual tenha sido praticada qualquer das acções prevista no nº 2, é punido com pena de prisão de 1 a 5 anos. **Artigo 4º - Dano relativo a programas ou outros dados informáticos** 3 - Incorre na mesma pena do n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas nesse número. **Artigo 5º - Sabotagem informática** 2 - Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior. **Artigo 6º - Acesso ilegítimo** 2 - Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior. **Artigo 7º - Intercepção ilegítima** 3 - Incorre na mesma pena prevista no nº 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no mesmo número.

3. Cada Parte pode reservar-se o direito de não aplicar o n. º 1 do presente artigo, desde que essa reserva não diga respeito à venda, distribuição ou qualquer outra forma de disponibilização dos elementos referidos no n.º 1, a), (ii) do presente artigo.	
Artigo 7.º – Falsificação informática Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracções penais nos termos do seu direito interno, quando praticadas intencional e ilicitamente, a introdução, a alteração, o apagamento ou a supressão de dados informáticos dos quais resultem dados não autênticos, com o intuito de que esses dados sejam considerados ou utilizados para fins legais como se fossem autênticos, quer sejam ou não directamente legíveis e inteligíveis. Qualquer uma das Partes pode exigir que para existir responsabilidade criminal tem de haver intenção fraudulenta ou outra intenção criminosa semelhante.	**Artigo 3º - Falsidade informática** 1 - Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão até 5 anos ou multa de 120 a 600 dias. 2- Quando as acções descritas no número anterior incidirem sobre os dados registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, a pena é de 1 a 5 anos de prisão. 3 - Quem, actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar documento produzido a partir de dados informáticos que foram objecto dos actos referidos no nº 1 ou cartão ou outro dispositivo no qual se encontrem registados ou incorporados os dados objecto dos actos referidos no número anterior, é punido com as penas previstas num e noutro número, respectivamente. 4- Quem importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, sobre o qual tenha sido praticada qualquer das acções prevista no nº 2, é punido com pena de prisão de 1 a 5 anos. 5 - Se os factos referidos nos números anteriores forem praticados por funcionário no exercício das suas funções, a pena é de prisão de 2 a 5 anos.
Artigo 8.º - Burla informática Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracção penal nos termos do seu direito interno, quando praticado intencional e ilicitamente, o prejuízo patrimonial	**Artigo 221º - Burla informática e nas comunicações** 1 - Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, interferindo no resultado de tratamento de dados ou mediante estruturação incorrecta de programa informático, utilização incorrecta ou incompleta de dados, utilização de dados sem

causado a outra pessoa por meio de: a) Qualquer introdução, alteração, apagamento ou supressão de dados informáticos; b) Qualquer interferência no funcionamento de um sistema informático, com intenção de obter para si ou para outra pessoa um benefício económico ilegítimo	autorização ou intervenção por qualquer outro modo não autorizada no processamento, é punido com pena de prisão até 3 anos ou com pena de multa. 2 - A mesma pena é aplicável a quem, com intenção de obter para si ou para terceiro um benefício ilegítimo, causar a outrem prejuízo patrimonial, usando programas, dispositivos electrónicos ou outros meios que, separadamente ou em conjunto, se destinem a diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações. 3 - A tentativa é punível. 4 - O procedimento criminal depende de queixa. 5 - Se o prejuízo for: a) De valor elevado, o agente é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias; b) De valor consideravelmente elevado, o agente é punido com pena de prisão de 2 a 8 anos. 6 - É correspondentemente aplicável o disposto no artigo 206º.
Artigo 9.º – Infracções relativas à pornografia infantil 1. Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracções penais nos termos do seu direito interno, quando praticadas de forma intencional e ilegítima, as seguintes condutas: a) Produção de pornografia infantil com o propósito de a divulgar através um sistema informático; b) Oferta ou disponibilização de pornografia infantil através de um sistema informático; c) Difusão ou transmissão de pornografia infantil através de um sistema informático; d) Obtenção para si ou para outra pessoa de pornografia infantil através de um sistema informático; e) Posse de pornografia infantil num sistema informático ou num dispositivo de armazenamento de dados informáticos. 2. Para efeitos do n.º 1, a expressão «pornografia infantil» deverá abranger todo o material pornográfico que represente visualmente: a) Um menor envolvido em comportamentos sexualmente explícitos; b) Uma pessoa com aspecto de menor envolvida em comportamentos	**Artigo 176º - Pornografia de menores** 1 - Quem: *a*) Utilizar menor em espectáculo pornográfico ou o aliciar para esse fim; *b*) Utilizar menor em fotografia, filme ou gravação pornográficos, independentemente do seu suporte, ou o aliciar para esse fim; *c*) Produzir, distribuir, importar, exportar, divulgar, exibir ou ceder, a qualquer título ou por qualquer meio, os materiais previstos na alínea anterior; *d*) Adquirir ou detiver materiais previstos na alínea *b*) com o propósito de os distribuir, importar, exportar, divulgar, exibir ou ceder; é punido com pena de prisão de um a cinco anos. 2 - Quem praticar os actos descritos no número anterior profissionalmente ou com intenção lucrativa é punido com pena de prisão de um a oito anos. 3 - Quem praticar os actos descritos nas alíneas *c*) e *d*) do n.º 1 utilizando material pornográfico com representação realista de menor é punido com pena de prisão até dois anos. 4 - Quem adquirir ou detiver os materiais previstos na alínea *b*) do n.º 1 é punido com pena de prisão até um ano ou com pena de multa. 5 - A tentativa é punível.

sexualmente explícitos; c) Imagens realistas de um menor envolvido em comportamentos sexualmente explícitos. 3. Para efeitos do n.º 2, a expressão «menor» deverá abranger qualquer pessoa com menos de 18 anos de idade. Qualquer uma das Partes pode impor um limite de idade inferior, não podendo, contudo, ser fixado abaixo dos 16 anos. 4. Cada Parte pode reservar-se o direito de não aplicar, no todo ou em parte, o disposto nas alíneas d) e e) do n.º 1 e nas alíneas b) e c) do n.º 2.	
Título 4 – Infracções respeitantes a violações do direito de autor e direitos conexos	
Artigo 10.º – Infracções respeitantes a violações do direito de autor e dos direitos conexos 1. Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracções penais nos termos do seu direito interno, as violações do direito de autor, tal como estas se encontram definidas na lei dessa Parte com base nas obrigações que a mesma assumiu ao abrigo da Convenção de Berna para a Protecção das Obras Literárias e Artísticas, revista pelo Acto de Paris de 24 de Julho de 1971, do Acordo sobre os Aspectos dos Direitos de Propriedade Intelectual relacionados com o Comércio e do Tratado da OMPI sobre o Direito de Autor, com excepção de quaisquer direitos morais reconhecidos por essas Convenções, quando tais actos são praticados de forma intencional, para fins comerciais e por meio de um sistema informático. 2. Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracções penais nos termos do seu direito interno as violações dos direitos conexos tal como estas se encontram definidas na lei dessa Parte com base nas obrigações que a mesma assumiu ao abrigo da Convenção Internacional para a Protecção dos Artistas Intérpretes ou Executantes, dos Produtores de Fonogramas e dos Organismos de Radiodifusão (Convenção de Roma), do Acordo sobre os Aspectos dos Direitos de Propriedade Intelectual relacionados com o	**Lei do Cibercrime** **Artigo 8º - Reprodução ilegítima de programa protegido** 1 - Quem ilegitimamente reproduzir, divulgar ou comunicar ao público um programa informático protegido por lei é punido com pena de prisão até 3 anos ou com pena de multa. 2 - Na mesma pena incorre quem ilegitimamente reproduzir topografia de um produto semicondutor ou a explorar comercialmente ou importar, para estes fins, uma topografia ou um produto semicondutor fabricado a partir dessa topografia. 3 - A tentativa é punível. **Decreto-Lei nº 252/94, de 20 de Outubro** **Artigo 14º - Tutela Penal** 1 – Um programa de computador é penalmente protegido contra a reprodução não autorizada. 2 – É aplicável ao programa de computador o disposto no nº 1 do Artigo 9º da Lei nº 109/91, de 17 de Agosto. (esta lei foi revogada e substituída pela Lei nº 109/2009, sendo o Artigo 9º, nº 1 substituído pelo novo Artigo 8º, nº 1) **Lei nº 45/85, 17 de Setembro, alterada pela Lei nº 16/2008 (*Código de Direito de Autor*)**

Comércio e do Tratado da OMPI sobre Interpretações ou Execuções e Fonogramas, com excepção de quaisquer direitos morais reconhecidos por essas Convenções, quando tais actos são praticados de forma intencional, para fins comerciais e por meio de um sistema informático. 3. Qualquer Parte pode, em circunstâncias claramente definidas, reservar-se o direito de não estabelecer a responsabilidade criminal nos termos dos números 1 e 2 do presente artigo, desde que se encontrem disponíveis outros meios eficazes e essa reserva não prejudique as obrigações internacionais assumidas por essa Parte no quadro dos instrumentos internacionais referidos nos números 1 e 2 do presente artigo.	**Artigo 195º - Usurpação** 1 - Comete o crime de usurpação quem, sem autorização do autor ou do artista, do produtor de fonograma e videograma ou do organismo de radiodifusão, utilizar uma obra ou prestação por qualquer das formas previstas neste Código. 2 - Comete também o crime de usurpação: *a*) Quem divulgar ou publicar abusivamente uma obra ainda não divulgada nem publicada pelo seu autor ou não destinada a divulgação ou publicação, mesmo que a apre sente como sendo do respectivo autor, quer se proponha ou não obter qualquer vantagem económica; *b*) Quem coligir ou compilar obras publicadas ou inéditas sem autorização do autor; *c*) Quem, estando autorizado a utilizar uma obra, prestação de artista, fonograma, videograma ou emissão radiodifundida, exceder os limites da autorização concedida, salvo nos casos expressamente previstos neste Código. 3 - Será punido com as penas previstas no artigo 197º o autor que, tendo transmitido, total ou parcialmente, os respectivos direitos ou tendo autorizado a utilização da sua obra por qualquer dos modos previstos neste Código, a utilizar directa ou indirectamente com ofensa dos direitos atribuídos a outrem. **Artigo 196º - Contrafacção** 1 - Comete o crime de contrafacção quem utilizar, como sendo criação ou prestação sua, obra, prestação de artista, fonograma, videograma ou emissão de radiodifusão que seja mera reprodução total ou parcial de obra ou prestação alheia, divulgada ou não divulgada, ou por tal modo semelhante que não tenha individualidade própria. 2 - Se a reprodução referida no número anterior representar apenas parte ou fracção da obra ou prestação, só essa parte ou fracção se considera como contrafacção. 3 - Para que haja contrafacção não é essencial que a reprodução seja feita pelo mesmo processo que o original, com as mesmas dimensões ou com o mesmo formato 4 - Não importam contrafacção: *a*) A semelhança entre traduções, devidamente autorizadas, da mesma obra ou entre fotografias, desenhos, gravuras ou outra forma de representação do mesmo objecto, se, apesar das semelhanças decorrentes da identidade do objecto, cada

	uma das obras tiver individualidade própria; *b*) A reprodução pela fotografia ou pela gravura efectuada só para o efeito de documentação da crítica artística. **Artigo 199º - Aproveitamento de obra contrafeita ou usurpada** 1 - Quem vender, puser à venda, importar, exportar ou por qualquer modo distribuir ao público obra usurpada ou contrafeita ou cópia não autorizada de fonograma ou videograma, quer os respectivos exemplares tenham sido produzidos no País quer no estrangeiro, será punido com as penas previstas no artigo 197º 2 - A negligência é punível com multa até 50 dias. **Artigo 218º - Tutela penal** 1 - Quem, não estando autorizado, neutralizar qualquer medida eficaz de carácter tecnológico, sabendo isso ou tendo motivos razoáveis para o saber, é punido com pena de prisão até 1 ano ou com pena de multa até 100 dias. 2 - A tentativa é punível com multa até 25 dias. **Artigo 224º - Tutela penal** 1 - Quem, não estando autorizado, intencionalmente, sabendo ou tendo motivos razoáveis para o saber, pratique um dos seguintes actos: *a*) Suprima ou altere qualquer informação para a gestão electrónica de direitos; *b*) Distribua, importe para distribuição, emita por radiodifusão, comunique ou ponha à disposição do público obras, prestações ou produções protegidas, das quais tenha sido suprimida ou alterada, sem autorização, a informação para a gestão electrónica dos direitos, sabendo que em qualquer das situações indicadas está a provocar, permitir, facilitar ou dissimular a violação de direitos de propriedade intelectual; é punido com pena de prisão até 1 ano ou com pena de multa até 100 dias. 2 - A tentativa é punível com multa até 25 dias.
Artigo 11.º – Tentativa, auxílio ou instigação 1. Cada Parte deverá adoptar as medidas legislativas e outras que se	**Código Penal Português** **Artigo 22º - Tentativa**

revelem necessárias para classificar como infracções penais, nos termos do seu direito interno, o auxílio ou a instigação à prática de qualquer uma das infracções previstas nos artigos 2.º a 10.º da presente Convenção, quando praticados intencionalmente tendo em vista a prática dessa infracção. 2. Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracção penal, nos termos do seu direito interno, a tentativa deliberada de praticar qualquer uma das infracções previstas nos artigos 3.º a 5.º , 7.º, 8.º e nas alíneas a) e c) do n.º 1 do artigo 9.º da presente Convenção. 3. Cada Parte pode reservar-se o direito de não aplicar, no todo ou em parte, o disposto no n.º 2 do presente artigo.	1 - Há tentativa quando o agente praticar actos de execução de um crime que decidiu cometer, sem que este chegue a consumar -se. 2 - São actos de execução: *a*) Os que preencherem um elemento constitutivo de um tipo de crime; *b*) Os que forem idóneos a produzir o resultado típico; ou *c*) Os que, segundo a experiência comum e salvo circunstâncias imprevisíveis, forem de natureza a fazer esperar que se lhes sigam actos das espécies indicadas nas alíneas anteriores. **Artigo 23º - Punibilidade da tentativa** 1 - Salvo disposição em contrário, a tentativa só é punível se ao crime consumado respectivo corresponder pena superior a três anos de prisão. 2 - A tentativa é punível com a pena aplicável ao crime consumado, especialmente atenuada. 3 - A tentativa não é punível quando for manifesta a inaptidão do meio empregado pelo agente ou a inexistência do objecto essencial à consumação do crime. **Artigo 27º - Cumplicidade** 1 - É punível como cúmplice quem, dolosamente e por qualquer forma, prestar auxílio material ou moral à prática por outrem de um facto doloso. 2 - É aplicável ao cúmplice a pena fixada para o autor, especialmente atenuada.
Artigo 12.º – Responsabilidade das pessoas colectivas 1. Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para garantir que as pessoas colectivas possam ser consideradas responsáveis pelas infracções penais previstas na presente Convenção, cometidas em seu benefício por qualquer pessoa singular, agindo individualmente ou enquanto membro de um órgão da pessoa colectiva, que nelas ocupem uma posição de liderança, com base: a) Nos poderes de representação conferidos pela pessoa colectiva; b) Na autoridade para tomar decisões em nome da pessoa colectiva; c) Na autoridade para exercer o controlo no seio da pessoa colectiva. 2. Para além dos casos já previstos no n.º 1 do presente artigo, cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para garantir que uma pessoa colectiva possa ser considerada responsável	**Artigo 9º - Responsabilidade penal das pessoas colectivas e entidades equiparadas** As pessoas colectivas e entidades equiparadas são penalmente responsáveis pelos crimes previstos na presente lei nos termos e limites do regime de responsabilização previsto no Código Penal.

sempre que a falta de vigilância ou controlo por parte de uma pessoa singular referida no n.º 1 possibilite a prática de uma das infracções previstas na presente Convenção em benefício da referida pessoa colectiva por uma pessoa singular que aja sob a sua autoridade. 3. De acordo com os princípios jurídicos da Parte, a responsabilidade de uma pessoa colectiva pode ser penal, civil ou administrativa. Essa responsabilidade não exclui a responsabilidade criminal das pessoas singulares que tenham cometido a infracção.	
Artigo 13.º – Sanções e medidas 1. Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para assegurar que as infracções penais estabelecidas nos termos dos artigos 2.º a 11.º sejam puníveis com sanções eficazes, proporcionais e dissuasivas, incluindo com penas privativas de liberdade. 2. Cada Parte deverá assegurar que as pessoas colectivas consideradas responsáveis nos termos do artigo 12.º sejam objecto de sanções ou medidas, de natureza penal e não penal, eficazes, proporcionais e dissuasivas, incluindo sanções pecuniárias.	
Secção 2 – Direito processual	
Artigo 14.º – Âmbito de aplicação das disposições processuais 1. Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para instituir os poderes e os procedimentos previstos na presente Secção, para efeitos de investigação ou de procedimento criminal específicos. 2. Salvo disposição em contrário do artigo 21.º, cada Parte deverá aplicar os poderes e os procedimentos previstos no n.º 1 do presente artigo: a) Às infracções penais previstas nos artigos 2.º a 11.º da presente Convenção; b) A outras infracções penais cometidas por meio de um sistema informático; e c) À obtenção de prova electrónica da prática de qualquer infracção penal.	**Artigo 11º - Âmbito de aplicação das disposições processuais** 1 - Com excepção do disposto nos artigos 18º e 19º, as disposições processuais previstas no presente capítulo aplicam -se a processos relativos a crimes: *a*) Previstos na presente lei; *b*) Cometidos por meio de um sistema informático; ou *c*) Em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico. 2 - As disposições processuais previstas no presente capítulo não prejudicam o regime da Lei nº 32/2008, de 17 de Julho.

3.a) Cada Parte pode reservar-se o direito de só aplicar as medidas previstas no artigo 20.º às infracções ou categorias de infracções especificadas na reserva, desde que o conjunto dessas infracções ou categorias de infracções não seja mais reduzido que o conjunto de infracções a que aplica as medidas previstas no artigo 21.º. Cada Parte deverá considerar a possibilidade de restringir a dita reserva de modo a permitir que a aplicação da medida prevista no artigo 20.º seja a mais ampla possível. b) Sempre que por força das restrições impostas pela sua legislação vigente à data da adopção da presente Convenção não possa aplicar as medidas previstas nos artigos 20.º e 21.º às comunicações que se processam no interior de um sistema informático de um prestador de serviços, que: i) tenha sido implementado para um grupo fechado de utilizadores; e ii) nem utilize as redes de telecomunicações públicas nem esteja interligado a outro sistema informático, público ou privado, uma Parte pode reservar-se o direito de não aplicar essas medidas às referidas comunicações. Cada Parte deverá considerar a possibilidade de restringir a dita reserva de modo a permitir que a aplicação das medidas previstas nos artigos 20.º e 21.º.	
rtigo 15.º – Condições e Garantias 1. Cada Parte deverá assegurar que o estabelecimento, a implementação e a aplicação dos poderes e procedimentos previstos na presente Secção respeitem as condições e garantias previstas no seu Direito interno, o qual deverá garantir uma protecção adequada dos direitos humanos e das liberdades, designadamente dos direitos estabelecidos em conformidade com as obrigações assumidas pela Parte em virtude da Convenção do Conselho da Europa de 1950 para a Protecção dos Direitos do Homem e das Liberdades Fundamentais e do Pacto Internacional sobre os Direitos Civis e Políticos das Nações Unidas de 1966, bem como de outros instrumentos internacionais aplicáveis em matéria de direitos humanos, e deverá incorporar o princípio da proporcionalidade. 2. Sempre que tal se justifique, em razão da natureza do poder ou do procedimento em causa, as referidas condições e garantias deverão incluir, designadamente, um controlo judicial ou outras formas de controlo	

independente, os fundamentos que justificam a sua aplicação, bem como a delimitação do âmbito de aplicação e a duração do poder ou procedimento em causa. 3. Na medida em que seja do interesse público, em particular, da boa administração da justiça, cada Parte deverá ter em consideração o impacto dos poderes e dos procedimentos previstos na presente Secção nos direitos, nas responsabilidades e nos interesses legítimos de terceiros.	
Artigo 16.º - Conservação expedita de dados informáticos armazenados 1. Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para que as suas autoridades competentes possam ordenar ou de outra modo impor a conservação expedita de dados informáticos específicos, incluindo de dados de tráfego armazenados por meio de um sistema informático, sobretudo quando existam motivos para crer que em relação a esses dados existe o sério risco de perda ou alteração. 2. Sempre que aplicar o disposto no n.º 1 supra através de uma injunção que impõe a uma pessoa a conservação dos dados informáticos específicos armazenados que tem na sua posse ou sob o seu controlo, uma Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para obrigar essa pessoa a conservar e a proteger a integridade dos referidos dados pelo tempo que for necessário, até um prazo máximo de 90 dias, para permitir que as autoridades competentes obtenham a sua divulgação. Qualquer uma das Partes pode prever a possibilidade dessa injunção ser subsequentemente renovada. 3. Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para obrigar a pessoa responsável pelos dados informáticos, ou qualquer outra pessoa encarregue de os conservar, a manterem a confidencialidade da aplicação dos referidos procedimentos durante o prazo previsto no seu direito interno. Os artigos 14.º e 15.º regulamentam os poderes e procedimentos referidos no presente artigo	**Artigo 12º - Preservação expedita de dados** 1 - Se no decurso do processo for necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos armazenados num sistema informático, incluindo dados de tráfego, em relação aos quais haja receio de que possam perder-se, alterar-se ou deixar de estar disponíveis, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que preserve os dados em causa. 2 - A preservação pode também ser ordenada pelo órgão de polícia criminal mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, devendo aquele, neste último caso, dar notícia imediata do facto à autoridade judiciária e transmitir -lhe o relatório previsto no artigo 253º do Código de Processo Penal. 3 - A ordem de preservação discrimina, sob pena de nulidade: *a*) A natureza dos dados; *b*) A sua origem e destino, se forem conhecidos; e *c*) O período de tempo pelo qual deverão ser preservados, até um máximo de três meses. 4 - Em cumprimento de ordem de preservação que lhe seja dirigida, quem tenha disponibilidade ou controlo sobre esses dados, designadamente o fornecedor de serviço, preserva de imediato os dados em causa, protegendo e conservando a sua integridade pelo tempo fixado, de modo a permitir à autoridade judiciária competente a sua obtenção, e fica obrigado a assegurar a confidencialidade da aplicação da medida processual. 5 - A autoridade judiciária competente pode ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea *c*) do nº 3, desde que se verifiquem os respectivos requisitos de admissibilidade, até ao limite máximo de um ano.

Artigo 17.º – Conservação expedita e divulgação parcial de dados de tráfego 1. Em relação aos dados de tráfego que devem ser conservados em conformidade com o artigo 16.º, cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para: a) Assegurar a conservação expedita dos dados de tráfego quer tenha sido um, quer tenham sido vários os prestadores de serviço envolvidos na transmissão dessa comunicação; b) Assegurar que um volume suficiente de dados de tráfego seja de imediato transmitido à autoridade competente da Parte ou a qualquer pessoa designada por essa autoridade, para permitir que a Parte identifique os prestadores de serviços e o trajecto da comunicação. 2. Os artigos 14.º e 15.º regulamentam os poderes e procedimentos referidos no presente artigo.	**Artigo 13º - Revelação expedita de dados de tráfego** Tendo em vista assegurar a preservação dos dados de tráfego relativos a uma determinada comunicação, independentemente do número de fornecedores de serviço que nela participaram, o fornecedor de serviço a quem essa preservação tenha sido ordenada nos termos do artigo anterior indica à autoridade judiciária ou ao órgão de polícia criminal, logo que o souber, outros fornecedores de serviço através dos quais aquela comunicação tenha sido efectuada, tendo em vista permitir identificar todos os fornecedores de serviço e a via através da qual aquela comunicação foi efectuada.
Artigo 18.º – Injunção de comunicar 1. Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para conferir poder às suas autoridades competentes para ordenarem: a) A uma pessoa que se encontre no seu território que disponibilize os dados informáticos específicos que estejam na sua posse ou sob o seu controlo e que estão armazenados num sistema informático ou num dispositivo de armazenamento de dados informáticos; e b) A um prestador de serviços que preste os seus serviços no território da Parte que disponibilize os dados dos assinantes relacionados com esses serviços que estejam na sua posse ou sob o seu controlo. 2. Os artigos 14.º e 15.º regulamentam os poderes e procedimentos referidos no presente artigo. 3. Para efeitos do presente artigo, entende-se por «dados relativos aos assinantes» quaisquer informações que um prestador de serviços possua sobre os assinantes dos seus serviços, sob a forma de dados informáticos ou sob qualquer outra forma, distintas dos dados de tráfego ou de conteúdo e que	**Artigo 14º - Injunção para apresentação ou concessão do acesso a dados** 1- Se no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados que os comunique ao processo ou que permita o acesso aos mesmos, sob pena de punição por desobediência. 2 - A ordem referida no número anterior identifica os dados em causa. 3 - Em cumprimento da ordem descrita nos nºs 1 e 2, quem tenha disponibilidade ou controlo desses dados comunica esses dados à autoridade judiciária competente ou permite, sob pena de punição por desobediência, o acesso ao sistema informático onde os mesmos estão armazenados. 4 - O disposto no presente artigo é aplicável a fornecedores de serviço, a quem pode ser ordenado que comuniquem ao processo dados relativos aos seus clientes ou assinantes, neles se incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida pelo fornecedor de serviços, e que permita determinar: *a*) O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço;

permitam determinar: c) O tipo de serviço de comunicação utilizado, as medidas técnicas adoptadas a esse respeito e a duração do serviço; d) A identidade, o endereço postal ou geográfico e o número de telefone do assinante e qualquer outro número de acesso, os dados referentes à facturação e ao pagamento, disponíveis com base num contrato ou num acordo de serviços; e) Qualquer outra informação sobre a localização do equipamento de comunicação disponível com base num contrato ou num acordo de prestação de serviços.	*b*) A identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à facturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; ou *c*) Qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços. 5 - A injunção prevista no presente artigo não pode ser dirigida a suspeito ou arguido nesse processo. 6 - Não pode igualmente fazer-se uso da injunção prevista neste artigo quanto a sistemas informáticos utilizados para o exercício da advocacia, das actividades médica e bancária e da profissão de jornalista. 7 - O regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 182º do Código de Processo Penal é aplicável com as necessárias adaptações.
Artigo 19.º – Busca e apreensão de dados informáticos armazenados 1. Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes a efectuar buscas ou de outro modo aceder: a) A um sistema informático, ou a parte do mesmo, bem como aos dados informáticos nele armazenados; e b) A um suporte informático de dados que permita armazenar dados informáticos no seu território. 2. Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para assegurar que, sempre que as suas autoridades efectuem buscas ou de outro modo acedam a um determinado sistema informático ou a parte dele, em conformidade com o disposto na alínea a) do n.º 1 do presente artigo, e caso existam motivos para crer que os dados procurados estão armazenados noutro sistema informático ou em parte dele, situado no seu território, e que é possível aceder legalmente a esses dados ou que eles estão disponíveis através do primeiro sistema, as autoridades são capazes de rapidamente alargar a busca ou o acesso equivalente ao outro sistema. 3. Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes a apreender ou de outro modo reter os dados informáticos aos quais se teve acesso nos termos do	**Artigo 15º - Pesquisa de dados informáticos** 1 - Quando no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente autoriza ou ordena por despacho que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência. 2 - O despacho previsto no número anterior tem um prazo de validade máximo de 30 dias, sob pena de nulidade. 3 - O órgão de polícia criminal pode proceder à pesquisa, sem prévia autorização da autoridade judiciária, quando: *a*) A mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado; *b*) Nos casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa. 4 - Quando o órgão de polícia criminal proceder à pesquisa nos termos do número anterior: *a*) No caso previsto na alínea *b*), a realização da diligência é, sob pena de nulidade, imediatamente comunicada à autoridade judiciária competente e por esta apreciada em ordem à sua validação;

n.º 1 ou 2 do presente artigo. Essas medidas incluem o poder de: c) Apreender ou de outro modo reter um sistema informático ou parte do mesmo, ou um suporte informático de dados; d) Efectuar e reter uma cópia desses dados informáticos; e) Preservar a integridade dos dados informáticos pertinentes armazenados; f) Tornar esses dados informáticos inacessíveis ou retirá-los do sistema informático acedido. 4. Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes a impor a qualquer pessoa que conheça o funcionamento do sistema informático ou as medidas aplicadas para proteger os dados informáticos nele contidos , que forneça de forma ponderada todas as informações necessárias para permitir a aplicação das medidas previstas no n.º 1 e 2 do presente artigo. 5. Os artigos 14.º e 15.º regulamentam os poderes e procedimentos referidos no presente artigo.	*b*) Em qualquer caso, é elaborado e remetido à autoridade judiciária competente o relatório previsto no artigo 253º do Código de Processo Penal. 5 - Quando, no decurso de pesquisa, surgirem razões para crer que os dados procurados se encontram noutro sistema informático, ou numa parte diferente do sistema pesquisado, mas que tais dados são legitimamente acessíveis a partir do sistema inicial, a pesquisa pode ser estendida mediante autorização ou ordem da autoridade competente, nos termos dos nºs 1 e 2. 6 - À pesquisa a que se refere este artigo são aplicáveis, com as necessárias adaptações, as regras de execução das buscas previstas no Código de Processo Penal e no Estatuto do Jornalista. **Artigo 16º - Apreensão de dados informáticos** 1 - Quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontrados dados ou documentos informáticos necessários à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a apreensão dos mesmos. 2 - O órgão de polícia criminal pode efectuar apreensões, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo anterior, bem como quando haja urgência ou perigo na demora. 3 - Caso sejam apreendidos dados ou documentos informáticos cujo conteúdo seja susceptível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo titular ou de terceiro, sob pena de nulidade esses dados ou documentos são apresentados ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto. 4 - As apreensões efectuadas por órgão de polícia criminal são sempre sujeitas a validação pela autoridade judiciária, no prazo máximo de 72 horas. 5 - As apreensões relativas a sistemas informáticos utilizados para o exercício da advocacia e das actividades médica e bancária estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no Código de Processo Penal e as relativas a sistemas informáticos utilizados para o exercício da profissão de jornalista estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no Estatuto do Jornalista.

	6 - O regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 182º do Código de Processo Penal é aplicável com as necessárias adaptações. 7 - A apreensão de dados informáticos, consoante seja mais adequado e proporcional, tendo em conta os interesses do caso concreto, pode, nomeadamente, revestir as formas seguintes: *a*) Apreensão do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respectiva leitura; *b*) Realização de uma cópia dos dados, em suporte autónomo, que será junto ao processo; *c*) Preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos; ou *d*) Eliminação não reversível ou bloqueio do acesso aos dados. 8 - No caso da apreensão efectuada nos termos da alínea *b*) do número anterior, a cópia é efectuada em duplicado, sendo uma das cópias selada e confiada ao secretário judicial dos serviços onde o processo correr os seus termos e, se tal for tecnicamente possível, os dados apreendidos são certificados por meio de assinatura digital. **Artigo 17º - Apreensão de correio electrónico e registos de comunicações de natureza semelhante** Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal.
Artigo 20.º – Recolha, em tempo real, de dados de tráfego 1. Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes a: a) Recolher ou registar, através da aplicação dos meios técnicos existentes no seu território; e	**Artigo 18º - Intercepção de comunicações** 1 - É admissível o recurso à intercepção de comunicações em processos relativos a crimes: *a*) Previstos na presente lei; ou *b*) Cometidos por meio de um sistema informático ou em relação aos

b) Obrigar um prestador de serviços, no âmbito da sua capacidade técnica, a: i) Recolher ou registar, através da aplicação dos meios técnicos existentes no seu território, ou ii) Cooperar com as autoridades competentes e a dar-lhes assistência na recolha ou no registo, em tempo real, dos dados de tráfego associados a comunicações específicas transmitidas no seu território através de um sistema informático. 2. Quando uma Parte, por força dos princípios estabelecidos no seu Direito interno, não puder adoptar as medidas enunciadas na alínea a) do n.º 1 do presente artigo, pode, em alternativa, adoptar as medidas legislativas e outras que se revelem necessárias para assegurar a recolha ou o registo, em tempo real, dos dados de tráfego associados a comunicações específicas transmitidas no seu território através da aplicação de meios técnicos existentes nesse território. 3. Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para obrigar um prestador de serviços a manter a confidencialidade do exercício de um dos poderes previstos no presente artigo, bem como de qualquer informação a esse respeito. 4. Os artigos 14.º e 15.º regulamentam os poderes e procedimentos referidos no presente artigo.	quais seja necessário proceder à recolha de prova em suporte electrónico, quando tais crimes se encontrem previstos no artigo 187º do Código de Processo Penal. 2 - A intercepção e o registo de transmissões de dados informáticos só podem ser autorizados durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público. 3 - A intercepção pode destinar -se ao registo de dados relativos ao conteúdo das comunicações ou visar apenas a recolha e registo de dados de tráfego, devendo o despacho referido no número anterior especificar o respectivo âmbito, de acordo com as necessidades concretas da investigação. 4 - Em tudo o que não for contrariado pelo presente artigo, à intercepção e registo de transmissões de dados informáticos é aplicável o regime da intercepção e gravação de conversações ou comunicações telefónicas constante dos artigos 187º, 188º e 190º do Código de Processo Penal.
Artigo 21.º – Intercepção de dados de conteúdo 1. Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes, relativamente a um conjunto de infracções graves a definir no âmbito do seu Direito interno, a: c) Recolher ou registar, através da aplicação dos meios técnicos existentes no seu território; d) Obrigar um prestador de serviços, no âmbito da sua capacidade técnica, a: i) Recolher ou registar, através da aplicação dos meios técnicos existentes no seu território, ou a	**Artigo 18º - Intercepção de comunicações** 1 - É admissível o recurso à intercepção de comunicações em processos relativos a crimes: *a*) Previstos na presente lei; ou *b*) Cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico, quando tais crimes se encontrem previstos no artigo 187º do Código de Processo Penal. 2 - A intercepção e o registo de transmissões de dados informáticos só podem ser autorizados durante o inquérito, se houver razões para crer que a diligência é

ii) Cooperar com as autoridades competentes e a dar-lhes assistência na recolha ou no registo, em tempo real, dos dados de conteúdo de comunicações específicas feitas no seu território, transmitidas através de um sistema informático. 2. Quando uma Parte, por força dos princípios estabelecidos no seu Direito interno, não puder adoptar as medidas enunciadas na alínea a) do n.º 1 do presente artigo, pode, em alternativa, adoptar as medidas legislativas e outras que se revelem necessárias para assegurar a recolha ou o registo, em tempo real, dos dados de conteúdo de comunicações específicas feitas no seu território, transmitidas através de um sistema informático nesse território. 3. Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para obrigar um prestador de serviços a manter a confidencialidade do exercício de um dos poderes previstos no presente artigo, bem como de qualquer informação a esse respeito. 4. Os artigos 14.º e 15.º regulamentam os poderes e procedimentos referidos no presente artigo.	indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público. 3 - A intercepção pode destinar -se ao registo de dados relativos ao conteúdo das comunicações ou visar apenas a recolha e registo de dados de tráfego, devendo o despacho referido no número anterior especificar o respectivo âmbito, de acordo com as necessidades concretas da investigação. 4 - Em tudo o que não for contrariado pelo presente artigo, à intercepção e registo de transmissões de dados informáticos é aplicável o regime da intercepção e gravação de conversações ou comunicações telefónicas constante dos artigos 187º, 188º e 190º do Código de Processo Penal.
Secção 3 – Jurisdição	
Artigo 22.º – Jurisdição 1. Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para estabelecer a sua competência relativamente à prática de qualquer infracção penal prevista nos artigos 2.º a 11.º da presente Convenção, sempre que a infracção seja cometida: a) no seu território; ou b) a bordo de um navio arvorando o pavilhão dessa Parte; c) a bordo de uma aeronave registada nos termos das leis dessa Parte; d) por um dos seus nacionais, se a infracção for punível nos termos do direito penal vigente no local onde foi praticada, ou se for cometida em local que não se encontra sob a jurisdição territorial de qualquer Estado. 2. Cada Parte pode reservar-se o direito de não aplicar, ou de apenas aplicar em casos e condições específicas, as regras de competência jurisdicional	**Lei do Cibercrime** **Artigo 27º - Aplicação no espaço da lei penal portuguesa e competência dos tribunais portugueses** 1 - Para além do disposto no Código Penal em matéria de aplicação no espaço da lei penal portuguesa, e salvo tratado ou convenção internacional em contrário, para efeitos da presente lei, a lei penal portuguesa é ainda aplicável a factos: *a*) Praticados por Portugueses, se aos mesmos não for aplicável a lei penal de nenhum outro Estado; *b*) Cometidos em benefício de pessoas colectivas com sede em território português; *c*) Fisicamente praticados em território português, ainda que visem sistemas informáticos localizados fora desse território; ou *d*) Que visem sistemas informáticos localizados em território português,

definidas nas alíneas b) a d) do n.º 1 do presente artigo ou qualquer parte dessas alíneas. 3. Cada Parte deverá adoptar as medidas legislativas que se revelem necessárias para estabelecer a sua jurisdição sobre as infracções referidas no n.º 1 do artigo 24.º da presente Convenção, sempre que o presumível autor da infracção se encontre no seu território e não seja extraditado para outra Parte apenas com base na sua nacionalidade, após um pedido de extradição. 4. A presente Convenção não exclui nenhuma jurisdição penal exercida por uma Parte em conformidade com o seu Direito interno. 5. Sempre que várias Partes reivindiquem a jurisdição sobre uma presumível infracção prevista na presente Convenção, as Partes interessadas deverão, se for caso disso, consultar-se para decidir qual é a jurisdição mais adequada para efeitos de exercício da acção penal.	independentemente do local onde esses factos forem fisicamente praticados. 2 - Se, em função da aplicabilidade da lei penal portuguesa, forem simultaneamente competentes para conhecer de um dos crimes previstos na presente lei os tribunais portugueses e os tribunais de outro Estado membro da União Europeia, podendo em qualquer um deles ser validamente instaurado ou prosseguido o procedimento penal com base nos mesmos factos, a autoridade judiciária competente recorre aos órgãos e mecanismos instituídos no seio da União Europeia para facilitar a cooperação entre as autoridades judiciárias dos Estados membros e a coordenação das respectivas acções, por forma a decidir qual dos dois Estados instaura ou prossegue o procedimento contra os agentes da infracção, tendo em vista centralizá-lo num só deles. 3 - A decisão de aceitação ou transmissão do procedimento é tomada pela autoridade judiciária competente, tendo em conta, sucessivamente, os seguintes elementos: *a*) O local onde foi praticada a infracção; *b*) A nacionalidade do autor dos factos; e *c*) O local onde o autor dos factos foi encontrado. 4 - São aplicáveis aos crimes previstos na presente lei as regras gerais de competência dos tribunais previstas no Código de Processo Penal. 5 - Em caso de dúvida quanto ao tribunal territorialmente competente, designadamente por não coincidirem o local onde fisicamente o agente actuou e o local onde está fisicamente instalado o sistema informático visado com a sua actuação, a competência cabe ao tribunal onde primeiro tiver havido notícia dos factos. **Código Penal** **Artigo 4º - Aplicação no espaço - princípio geral** Salvo tratado ou convenção internacional em contrário, a lei penal portuguesa é aplicável a factos praticados: *a*) Em território português, seja qual for a nacionalidade do agente; ou *b*) A bordo de navios ou aeronaves portugueses. **Artigo 5º - Factos praticados fora do território português** 1 - Salvo tratado ou convenção internacional em contrário, a lei penal portuguesa é ainda aplicável a factos cometidos fora do território nacional:

	a) Quando constituírem os crimes previstos nos artigos 221.º, 262.º a 271.º, 308.º a 321.º e 325.º a 345.º; *b*) Contra portugueses, por portugueses que viverem habitualmente em Portugal ao tempo da sua prática e aqui forem encontrados; *c*) Quando constituírem os crimes previstos nos artigos 159º a 161º, 171º, 172º, 175º, 176º e 278º a 280º, desde que o agente seja encontrado em Portugal e não possa ser extraditado ou entregue em resultado de execução de mandado de detenção europeu ou de outro instrumento de cooperação internacional que vincule o Estado Português; *d*) Quando constituírem os crimes previstos nos artigos 144.º, 163.º e 164.º, sendo a vítima menor, desde que o agente seja encontrado em Portugal e não possa ser extraditado ou entregue em resultado de execução de mandado de detenção europeu ou de outro instrumento de cooperação internacional que vincule o Estado Português; *e*) Por portugueses, ou por estrangeiros contra portugueses, sempre que: *i*) Os agentes forem encontrados em Portugal; *ii*) Forem também puníveis pela legislação do lugar em que tiverem sido praticados, salvo quando nesse lugar não se exercer poder punitivo; e *iii)* Constituírem crime que admita extradição e esta não possa ser concedida ou seja decidida a não entrega do agente em execução de mandado de detenção europeu ou de outro instrumento de cooperação internacional que vincule o Estado Português; *f*) Por estrangeiros que forem encontrados em Portugal e cuja extradição haja sido requerida, quando constituírem crimes que admitam a extradição e esta não possa ser concedida ou seja decidida a não entrega do agente em execução de mandado de detenção europeu ou de outro instrumento de cooperação internacional que vincule o Estado Português; *g*) Por pessoa colectiva ou contra pessoa colectiva que tenha sede em território português. 2 - A lei penal portuguesa é ainda aplicável a factos cometidos fora do território nacional que o Estado Português se tenha obrigado a julgar por tratado ou convenção internacional. **Artigo 6º - Restrições à aplicação da lei portuguesa** 1 - A aplicação da lei portuguesa a factos praticados fora do território nacional só tem lugar quando o agente não tiver sido julgado no país da prática do facto ou

	se houver subtraído ao cumprimento total ou parcial da condenação. 2 - Embora seja aplicável a lei portuguesa, nos termos do número anterior, o facto é julgado segundo a lei do país em que tiver sido praticado sempre que esta seja concretamente mais favorável ao agente. A pena aplicável é convertida naquela que lhe corresponder no sistema português, ou, não havendo correspondência directa, naquela que a lei portuguesa previr para o facto. 3 - O regime do número anterior não se aplica aos crimes previstos nas alíneas *a*) e *b*) do n.º 1 do artigo anterior. **Artigo 7º - Lugar da prática do facto** 1 - O facto considera -se praticado tanto no lugar em que, total ou parcialmente, e sob qualquer forma de comparticipação, o agente actuou, ou, no caso de omissão, devia ter actuado, como naquele em que o resultado típico ou o resultado não compreendido no tipo de crime se tiver produzido. 2 - No caso de tentativa, o facto considera -se igualmente praticado no lugar em que, de acordo com a representação do agente, o resultado se deveria ter produzido.
Capítulo III – Cooperação internacional	
Artigo 24.º – Extradição 1. a) O presente artigo aplica-se à extradição entre as Partes para as infracções penais previstas nos artigos 2.º a 11.º da presente Convenção, desde que sejam puníveis, nos termos da legislação das duas Partes interessadas, com uma pena privativa de liberdade de duração máxima não inferior a um ano ou com uma pena mais grave. b) Nos casos em que seja aplicável uma pena mínima diferente, nos termos de um acordo celebrado com base em legislação uniforme ou recíproca ou de um tratado de extradição aplicável entre duas ou mais Partes, incluindo a Convenção Europeia de Extradição (STE n.º 24), dever-se-á aplicar a pena mínima prevista nesse tratado ou acordo. 2. As infracções penais descritas no n.º 1 do presente artigo deverão ser consideradas como estando incluídas em qualquer tratado de extradição existente entre as Partes como infracções passíveis de extradição. As Partes comprometem-se a incluir essas infracções em qualquer tratado de extradição que venha a ser celebrado entre elas como infracções passíveis de extradição.	

3. Sempre que uma Parte receber um pedido de extradição proveniente de outra Parte com a qual não celebrou nenhum tratado de extradição e fizer depender a extradição da existência de um tratado, pode considerar a presente Convenção como constituindo a base legal para a extradição relativamente às infracções penais previstas no n.º 1 do presente artigo. 4. As Partes que não façam depender a extradição da existência de um tratado deverão reconhecer entre si as infracções penais referidas no n.º 1 do presente artigo como infracções passíveis de extradição. 5. A extradição fica sujeita às condições previstas na lei da Parte requerida ou nos tratados de extradição aplicáveis, incluindo os motivos pelos quais a Parte requerida pode recusar a extradição. 6. Se a extradição por uma das infracções penais previstas no n.º 1 do presente artigo for recusada apenas com base na nacionalidade da pessoa procurada ou porque a Parte requerida considera ter competência relativamente a essa infracção, a Parte requerida deverá, a pedido da Parte requerente, apresentar o caso às suas autoridades competentes para fins de procedimento criminal e informar oportunamente a Parte requerente do resultado definitivo. Essas autoridades deverão tomar a sua decisão e conduzir as investigações e o procedimento nas mesmas condições que para qualquer outra infracção de natureza idêntica, nos termos da lei dessa Parte. 7 a) Na falta de tratado, cada Parte deverá, no momento da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, comunicar ao Secretário-Geral do Conselho da Europa o nome e a morada de cada autoridade responsável pela elaboração ou recepção dos pedidos de extradição ou de detenção provisória; b) O Secretário-Geral do Conselho da Europa deverá criar e manter actualizado um registo das autoridades assim designadas pelas Partes. Cada Parte deverá assegurar que os dados constantes do registo estão sempre correctos.	
Artigo 25.º – Princípios gerais relativos ao auxílio judiciário mútuo	**Artigo 20º - Âmbito da cooperação internacional** As autoridades nacionais competentes cooperam com as autoridades estrangeiras

1. As Partes deverão conceder-se mutuamente o mais amplo auxílio possível para efeitos de investigação ou de procedimento relativos a infracções penais relacionadas com sistemas e dados informáticos, ou para efeitos de recolha de provas sob a forma electrónica de uma infracção penal. 2. Cada Parte deverá adoptar, igualmente, as medidas legislativas e outras que se revelem necessárias para cumprir as obrigações enunciadas nos artigos 27.º a 35.º. 3. Em caso de urgência, cada Parte pode efectuar os pedidos de auxílio judiciário mútuo ou as comunicações conexas, através de meios de comunicação expeditos, nomeadamente por fax ou correio electrónico, desde que esses meios assegurem níveis de segurança e autenticação adequados (incluindo a encriptação, se necessário), com confirmação oficial posterior se o Estado requerido o exigir. O Estado requerido deverá aceitar e responder ao pedido através de qualquer um desses meios de comunicação expeditos. 4. Salvo disposição expressa em contrário prevista nos artigos do presente Capítulo, o auxílio judiciário mútuo fica sujeito às condições previstas na lei da Parte requerida ou nos tratados de auxílio mútuo aplicáveis, incluindo os motivos pelos quais a Parte requerida pode recusar a cooperação. A Parte requerida não deverá exercer o seu direito de recusa de auxílio judiciário mútuo relativamente às infracções previstas nos artigos 2.º a 11.º apenas com o fundamento de que o pedido se reporta a uma infracção considerada como uma infracção de natureza fiscal. 5. Sempre que, em conformidade com o disposto no presente Capítulo, a Parte requerida estiver autorizada a fazer depender o auxílio judiciário mútuo da existência de dupla incriminação, considera-se que esta condição está preenchida se a conduta que constitui a infracção, relativamente à qual o auxílio mútuo é pedido, for qualificada como infracção penal pelo direito interno dessa Parte, independentemente de nos termos do seu direito interno a infracção pertencer ou não à mesma categoria de infracções ou obedecer ou não à mesma terminologia que as previstas no direito interno da Parte requerente.	competentes para efeitos de investigações ou procedimentos respeitantes a crimes relacionados com sistemas ou dados informáticos, bem como para efeitos de recolha de prova, em suporte electrónico, de um crime, de acordo com as normas sobre transferência de dados pessoais previstas na Lei n.º 67/98, de 26 de Outubro.
Artigo 26.º – Informação espontânea	

1. Qualquer Parte pode, nos limites previstos no seu Direito interno e não e sem pedido prévio, transmitir a uma outra Parte informações obtidas no âmbito das suas próprias investigações, sempre que considerar que a transmissão dessas informações pode ajudar a Parte destinatária a iniciar ou a efectuar investigações ou procedimentos relativos a infracções penais previstas na presente Convenção, ou sempre que considerar que ela pode dar origem a um pedido de cooperação formulado por essa Parte nos termos do presente Capítulo. 2. Antes de transmitir essas informações, a Parte transmissora pode solicitar que o seu carácter confidencial seja preservado ou que só sejam utilizadas em determinadas condições. Se não puder satisfazer o pedido, a Parte destinatária deverá informar a outra Parte de tal facto, a qual deverá, então, decidir se as informações em causa devem, mesmo assim, ser fornecidas. Se a Parte destinatária aceitar as informações nas condições estipuladas, fica obrigada a observá-las.	
Artigo 27.º - Procedimentos relativos aos pedidos de auxílio mútuo na falta de acordos internacionais aplicáveis 1. Na falta de um tratado de auxílio mútuo ou de um acordo assente em legislação uniforme ou recíproca em vigor entre a Parte requerente e a Parte requerida, aplica-se o disposto nos números 2 a 9 do presente artigo. Existindo esse tratado, acordo ou legislação, só se aplica o disposto no presente artigo se, em vez deles, as Partes envolvidas decidirem aplicar o presente artigo, no todo ou em parte. 2 a) Cada Parte deverá designar uma ou mais autoridades centrais encarregues de enviar os pedidos de auxílio mútuo ou de lhes responder, de os executar ou de os transmitir às autoridades competentes com vista à sua execução; b) As autoridades centrais deverão comunicar directamente entre si; c) Cada Parte deverá, no momento em que assinar ou depositar o seu instrumento de ratificação, aceitação, aprovação ou adesão, comunicar ao Secretário-Geral do Conselho da Europa o nome e endereço das autoridades designadas nos termos do presente número;	

d) O Secretário-Geral do Conselho da Europa deverá criar e manter actualizado um registo das autoridades centrais designadas pelas Partes. Cada Parte deverá assegurar que os dados constantes do registo estão sempre correctos. 3. Os pedidos de auxílio mútuo referidos no presente artigo deverão ser executados em conformidade com os procedimentos especificados pela Parte requerente, salvo se forem incompatíveis com a legislação da Parte requerida. 4. Para além dos motivos de recusa previstos no n.º 4 do artigo 25.º, a Parte requerida pode recusar o auxílio mútuo se considerar que: e) O pedido respeita a uma infracção de natureza política ou com ela conexa; ou que f) A execução do pedido pode prejudicar a sua soberania, segurança, ordem pública ou outros interesses essenciais. 5. A Parte requerida pode adiar a execução do pedido sempre que ela prejudique as investigações ou os procedimentos criminais levados a cabo pelas suas autoridades. 6. Antes de recusar ou adiar o auxílio, a Parte requerida deverá, se for caso disso, após consulta com a Parte requerente, verificar se o pedido pode ser parcialmente executado ou sujeito às condições que considere necessárias. 7. A Parte requerida deverá de imediato informar a Parte requerente do resultado da execução do pedido de auxílio. Qualquer recusa ou adiamento do pedido deverão ser fundamentados. A Parte requerida também deverá informar a Parte requerente de quaisquer motivos que impossibilitem a execução do pedido ou que conduzam a um atraso significativo da mesma. 8. A Parte requerente pode solicitar à Parte requerida que preserve a confidencialidade de qualquer pedido apresentado nos termos do presente Capítulo bem como do respectivo conteúdo, a menos que a sua execução exija o contrário. Caso não possa respeitar o pedido de confidencialidade, a Parte requerida deverá de imediato informar a Parte requerente, a qual decide depois se o pedido deve, ainda assim, ser executado.	

9.a) Nos casos urgentes, as autoridades judiciárias da Parte requerente podem enviar directamente às autoridades judiciárias da Parte requerida os pedidos de auxílio mútuo ou as comunicações com eles relacionadas. Nesses casos, dever-se-á ao mesmo tempo e por intermédio da autoridade central da Parte requerente enviar uma cópia à autoridade central da Parte requerida. b) Qualquer pedido ou comunicação nos termos do presente número podem ser efectuados por intermédio da Organização Internacional de Polícia Criminal (Interpol). c) Quando um pedido é efectuado nos termos da alínea a) do presente artigo e a autoridade não é competente para executá-lo, deverá esta última transmiti-lo à autoridade nacional competente e informar directamente a Parte requerente de tal facto. d) As autoridades competentes da Parte requerente podem enviar directamente às autoridades competentes da Parte requerida os pedidos ou as comunicações nos termos do presente número que não envolvam medidas coercivas. e) Cada Parte pode, no momento em que assinar ou depositar o seu instrumento de ratificação, aceitação, aprovação ou adesão, informar o Secretário-Geral do Conselho da Europa que, por razões de eficácia, os pedidos feitos nos termos do presente número deverão ser dirigidos à sua autoridade central.	
Artigo 28.º – Confidencialidade e restrição de utilização 1. Na falta de um tratado de auxílio mútuo ou de um acordo assente em legislação uniforme ou recíproca em vigor entre a Parte requerente e a Parte requerida, aplica-se o disposto no presente artigo. Existindo esse tratado, acordo ou legislação, só se aplica o disposto no presente artigo se, em vez deles, as Partes envolvidas decidirem aplicar o presente artigo, no todo ou em parte. 2. A Parte requerida pode sujeitar a comunicação de informações ou de material em resposta a um pedido às seguintes condições: a) É mantida a confidencialidade dessas informações e desse material nos casos em que o pedido de auxílio mútuo não puder ser cumprido sem o preenchimento dessa condição, ou b) Essas informações e esse material não são utilizados para investigações ou procedimentos diversos dos indicados no pedido.	

3. Se não puder satisfazer uma das condições enunciadas no n.º 2 do presente artigo, a Parte requerente deverá de imediato informar a Parte requerida, a qual decide depois se a informação deve, ainda assim, ser transmitida. Se aceitar essa condição, a Parte requerente fica obrigada a observá-la. 4. Qualquer Parte que forneça informações ou material sujeitos a uma das condições enunciadas no n.º 2 do presente artigo pode exigir da outra Parte uma explicação sobre a utilização dada a essas informações ou a esse material.	
Artigo 29.º – Conservação expedita de dados informáticos armazenados 1. Uma Parte pode solicitar a outra Parte que ordene ou, de outro modo, imponha a conservação expedita de dados armazenados através de um sistema informático situado no território dessa outra Parte, e relativamente aos quais a Parte requerente pretende efectuar um pedido de auxílio mútuo tendo em vista a busca ou outro acesso semelhante, a apreensão ou outro tipo de retenção semelhante, ou a divulgação dos dados. 2. Um pedido de conservação feito nos termos do n.º 1 do presente artigo deverá especificar: d) A autoridade que solicita a conservação; e) A infracção que constitui o objecto da investigação ou do procedimento criminal, bem como um breve resumo dos respectivos factos; f) Os dados informáticos armazenados que devem ser conservados e a relação entre estes e a infracção; g) Todas as informações disponíveis que permitam identificar o responsável pelos dados informáticos armazenados ou a localização do sistema informático; h) A necessidade da conservação; e i) A intenção da Parte de apresentar um pedido de auxílio tendo em vista a busca ou outro acesso semelhante, a apreensão ou outro tipo de retenção semelhante, ou a divulgação de dados informáticos armazenados.	**Artigo 22º - Preservação e revelação expeditas de dados informáticos em cooperação internacional** 1 - Pode ser solicitada a Portugal a preservação expedita de dados informáticos armazenados em sistema informático aqui localizado, relativos a crimes previstos no artigo 11º, com vista à apresentação de um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação dos mesmos. 2 - A solicitação especifica: *a*) A autoridade que pede a preservação; *b*) A infracção que é objecto de investigação ou procedimento criminal, bem como uma breve exposição dos factos relacionados; *c*) Os dados informáticos a conservar e a sua relação com a infracção; *d*) Todas as informações disponíveis que permitam identificar o responsável pelos dados informáticos ou a localização do sistema informático; *e*) A necessidade da medida de preservação; e *f*) A intenção de apresentação de um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação dos dados. 3 - Em execução de solicitação de autoridade estrangeira competente nos termos dos números anteriores, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que os preserve. 4 - A preservação pode também ser ordenada pela Polícia Judiciária mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, sendo aplicável, neste último caso, o disposto no nº 4 do artigo anterior. 5 - A ordem de preservação especifica, sob pena de nulidade:

3. Após ter recebido o pedido de outra Parte, a Parte requerida deverá tomar todas as medidas adequadas para proceder, de forma expedita, à conservação dos dados especificados, em conformidade com o seu direito interno. Para efeitos de execução de um pedido, o requisito da dupla incriminação não é exigido como condição para essa conservação. 4. Uma Parte que imponha o requisito da dupla incriminação como condição para executar um pedido de auxílio mútuo tendo em vista a busca ou outro acesso semelhante, a apreensão ou outro tipo de retenção semelhante, ou a divulgação dos dados, pode, em relação a outras infracções que não as estabelecidas em conformidade com o disposto nos artigos 2.º a 11.º da presente Convenção, reservar-se o direito de recusar o pedido de conservação nos termos do presente artigo nos casos em que tenha motivos para crer que, no momento da divulgação, o requisito da dupla incriminação não pode ser preenchido. 5. Além disso, um pedido de conservação só pode ser recusado se a Parte requerida considerar que: c) o pedido respeita a uma infracção de natureza política ou com ela conexa; ou que d) a execução do pedido pode prejudicar a sua soberania, segurança, ordem pública ou outros interesses essenciais. 6. Quando, no seu entender, a conservação não assegurar a futura disponibilização dos dados ou comprometer ou de outro modo prejudicar a confidencialidade das investigações efectuadas pela Parte requerente, a Parte requerida deverá de imediato informar a Parte requerente, a qual decide depois se o pedido deve, ainda assim, ser executado. 7. Qualquer conservação efectuada em resposta ao pedido referido no n.º 1 do presente artigo é válida por um período não inferior a 60 dias, de modo a permitir que a Parte requerente possa apresentar um pedido tendo em vista a busca ou outro acesso semelhante, a apreensão ou outro tipo de retenção semelhante, ou a divulgação dos dados. Após a recepção desse pedido, os dados deverão continuar a ser conservados até que haja uma decisão sobre o pedido.	*a*) A natureza dos dados; *b*) Se forem conhecidos, a origem e o destino dos mesmos; e *c*) O período de tempo pelo qual os dados devem ser preservados, até um máximo de três meses. 6 - Em cumprimento de ordem de preservação que lhe seja dirigida, quem tem disponibilidade ou controlo desses dados, designadamente o fornecedor de serviço, preserva de imediato os dados em causa pelo período de tempo especificado, protegendo e conservando a sua integridade. 7 - A autoridade judiciária competente, ou a Polícia Judiciária mediante autorização daquela autoridade, podem ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea *c*) do nº 5, desde que se verifiquem os respectivos requisitos de admissibilidade, até ao limite máximo de um ano. 8 - Quando seja apresentado o pedido de auxílio referido no nº 1, a autoridade judiciária competente para dele decidir determina a preservação dos dados até à adopção de uma decisão final sobre o pedido. 9 - Os dados preservados ao abrigo do presente artigo apenas podem ser fornecidos: *a*) À autoridade judiciária competente, em execução do pedido de auxílio referido no nº 1, nos mesmos termos em que poderiam sê -lo, em caso nacional semelhante, ao abrigo dos artigos 13º a 17º; *b*) À autoridade nacional que emitiu a ordem de preservação, nos mesmos termos em que poderiam sê -lo, em caso nacional semelhante, ao abrigo do artigo 13º. 10 - A autoridade nacional à qual, nos termos do número anterior, sejam comunicados dados de tráfego identificadores de fornecedor de serviço e da via através dos quais a comunicação foi efectuada, comunica -os rapidamente à autoridade requerente, por forma a permitir a essa autoridade a apresentação de nova solicitação de preservação expedita de dados informáticos. 11 - O disposto nos nºs 1 e 2 aplica -se, com as devidas adaptações, aos pedidos formulados pelas autoridades portuguesas. **Artigo 23º - Motivos de recusa** 1 - A solicitação de preservação ou revelação expeditas de dados informáticos é recusada quando: *a*) Os dados informáticos em causa respeitarem a infracção de natureza política ou infracção conexa segundo as concepções do direito português; *b*) Atentar contra a soberania, segurança, ordem pública ou outros

	interesses da República Portuguesa, constitucionalmente definidos; *c*) O Estado terceiro requisitante não oferecer garantias adequadas de protecção dos dados pessoais. 2 - A solicitação de preservação expedita de dados informáticos pode ainda ser recusada quando houver fundadas razões para crer que a execução de pedido de auxílio judiciário subsequente para fins de pesquisa, apreensão e divulgação de tais dados será recusado por ausência de verificação do requisito da dupla incriminação.
Artigo 30.º – Divulgação expedita de dados de tráfego conservados 1. Quando, no decurso da execução de um pedido de conservação de dados de tráfego relativos a uma determinada comunicação, formulado nos termos do artigo 29.º, verificar que um prestador de serviços noutro Estado participou na transmissão da comunicação, a Parte requerida deverá transmitir rapidamente à Parte requerente dados de tráfego suficientes para identificar esse prestador de serviços bem como o trajecto utilizado para a transmissão da comunicação. 2. A divulgação de dados de tráfego nos termos do n.º 1 só pode ser recusada se a Parte requerida considerar que: i. o pedido respeita a uma infracção de natureza política ou com ela conexa; ou que ii. a execução do pedido pode prejudicar a sua soberania, segurança, ordem pública ou outros interesses essenciais.	**Artigo 22º - Preservação e revelação expeditas de dados informáticos em cooperação internacional** 1 - Pode ser solicitada a Portugal a preservação expedita de dados informáticos armazenados em sistema informático aqui localizado, relativos a crimes previstos no artigo 11º, com vista à apresentação de um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação dos mesmos. 2 - A solicitação especifica: *a*) A autoridade que pede a preservação; *b*) A infracção que é objecto de investigação ou procedimento criminal, bem como uma breve exposição dos factos relacionados; *c*) Os dados informáticos a conservar e a sua relação com a infracção; *d*) Todas as informações disponíveis que permitam identificar o responsável pelos dados informáticos ou a localização do sistema informático; *e*) A necessidade da medida de preservação; e *f*) A intenção de apresentação de um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação dos dados. 3 - Em execução de solicitação de autoridade estrangeira competente nos termos dos números anteriores, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que os preserve. 4 - A preservação pode também ser ordenada pela Polícia Judiciária mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, sendo aplicável, neste último caso, o disposto no nº 4 do artigo anterior. 5 - A ordem de preservação especifica, sob pena de nulidade: *a*) A natureza dos dados; *b*) Se forem conhecidos, a origem e o destino dos mesmos; e *c*) O período de tempo pelo qual os dados devem ser preservados, até um

	máximo de três meses. 6 - Em cumprimento de ordem de preservação que lhe seja dirigida, quem tem disponibilidade ou controlo desses dados, designadamente o fornecedor de serviço, preserva de imediato os dados em causa pelo período de tempo especificado, protegendo e conservando a sua integridade. 7 - A autoridade judiciária competente, ou a Polícia Judiciária mediante autorização daquela autoridade, podem ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea *c*) do nº 5, desde que se verifiquem os respectivos requisitos de admissibilidade, até ao limite máximo de um ano. 8 - Quando seja apresentado o pedido de auxílio referido no nº 1, a autoridade judiciária competente para dele decidir determina a preservação dos dados até à adopção de uma decisão final sobre o pedido. 9 - Os dados preservados ao abrigo do presente artigo apenas podem ser fornecidos: *a*) À autoridade judiciária competente, em execução do pedido de auxílio referido no nº 1, nos mesmos termos em que poderiam sê -lo, em caso nacional semelhante, ao abrigo dos artigos 13º a 17º; *b*) À autoridade nacional que emitiu a ordem de preservação, nos mesmos termos em que poderiam sê -lo, em caso nacional semelhante, ao abrigo do artigo 13º. 10 - A autoridade nacional à qual, nos termos do número anterior, sejam comunicados dados de tráfego identificadores de fornecedor de serviço e da via através dos quais a comunicação foi efectuada, comunica -os rapidamente à autoridade requerente, por forma a permitir a essa autoridade a apresentação de nova solicitação de preservação expedita de dados informáticos. 11 - O disposto nos nºs 1 e 2 aplica -se, com as devidas adaptações, aos pedidos formulados pelas autoridades portuguesas. **Artigo 23º - Motivos de recusa** 1 - A solicitação de preservação ou revelação expeditas de dados informáticos é recusada quando: *a*) Os dados informáticos em causa respeitarem a infracção de natureza política ou infracção conexa segundo as concepções do direito português; *b*) Atentar contra a soberania, segurança, ordem pública ou outros interesses da República Portuguesa, constitucionalmente definidos; *c*) O Estado terceiro requisitante não oferecer garantias adequadas de protecção dos dados pessoais. 2 - A solicitação de preservação expedita de dados informáticos pode ainda ser recusada quando houver fundadas razões para crer que a execução de pedido de

	auxílio judiciário subsequente para fins de pesquisa, apreensão e divulgação de tais dados será recusado por ausência de verificação do requisito da dupla incriminação.
Artigo 31.º – Auxílio mútuo para o acesso a dados informáticos armazenados 1. Uma Parte pode solicitar a outra Parte a busca ou outro acesso semelhante, a apreensão ou outro tipo de retenção semelhante, bem como a divulgação de dados armazenados através de um sistema informático situado no território dessa outra Parte, incluindo os dados conservados em conformidade com o artigo 29.º. 2. A Parte requerida deverá cumprir o pedido aplicando os instrumentos internacionais, os acordos e a legislação referidos no artigo 23.º e respeitando as disposições pertinentes do presente Capítulo. 3. O pedido deverá ser cumprido o mais rapidamente possível sempre que: a) haja motivos para crer que os dados relevantes são especialmente susceptíveis de se perderem ou de serem alterados; b) os instrumentos, os acordos e a legislação referidos no n.º 2 prevejam uma cooperação célere.	**Artigo 24º - Acesso a dados informáticos em cooperação internacional** 1 - Em execução de pedido de autoridade estrangeira competente, a autoridade judiciária competente pode proceder à pesquisa, apreensão e divulgação de dados informáticos armazenados em sistema informático localizado em Portugal, relativos a crimes previstos no artigo 11º, quando se trata de situação em que a pesquisa e apreensão são admissíveis em caso nacional semelhante. 2 - A autoridade judiciária competente procede com a maior rapidez possível quando existam razões para crer que os dados informáticos em causa são especialmente vulneráveis à perda ou modificação ou quando a cooperação rápida se encontre prevista em instrumento internacional aplicável. 3 - O disposto no nº 1 aplica -se, com as devidas adaptações, aos pedidos formulados pelas autoridades judiciárias portuguesas.
Artigo 32.º – Acesso transfronteiriço a dados armazenados num computador, mediante consentimento ou quando se trate de dados acessíveis ao público Uma Parte pode, sem autorização de uma outra Parte: a) aceder a dados informáticos acessíveis ao público (fonte aberta), independentemente da sua localização geográfica; b) através de um sistema informático situado no seu território, aceder a dados informáticos no território de uma outra Parte, ou recebê-los, se obtiver o consentimento legal e voluntário da pessoa com legitimidade para lhe divulgar os dados através desse sistema informático.	**Artigo 25º - Acesso transfronteiriço a dados informáticos armazenados quando publicamente disponíveis ou com consentimento** As autoridades estrangeiras competentes, sem necessidade de pedido prévio às autoridades portuguesas, de acordo com as normas sobre transferência de dados pessoais previstas na Lei nº 67/98, de 26 de Outubro, podem: *a*) Aceder a dados informáticos armazenados em sistema informático localizado em Portugal, quando publicamente disponíveis; *b*) Receber ou aceder, através de sistema informático localizado no seu território, a dados informáticos armazenados em Portugal, mediante consentimento legal e voluntário de pessoa legalmente autorizada a divulgá-los.

Artigo 33.º – Auxílio mútuo para a recolha, em tempo real, de dados de tráfego 1. As Partes deverão conceder-se mutuamente auxílio para a recolha, em tempo real, de dados de tráfego relativos a comunicações específicas transmitidas no seu território por meio de um sistema informático. Sem prejuízo do disposto no n.º 2, o auxílio deverá ser concedido nas condições e de acordo com os procedimentos previstos no direito interno. 2. Cada Parte deverá conceder esse auxílio pelo menos em relação às infracções penais relativamente às quais, em casos internos semelhantes, seria possível efectuar a recolha, em tempo real, de dados de tráfego.	**Artigo 26º - Intercepção de comunicações em cooperação internacional** 1 - Em execução de pedido da autoridade estrangeira competente, pode ser autorizada pelo juiz a intercepção de transmissões de dados informáticos realizadas por via de um sistema informático localizado em Portugal, desde que tal esteja previsto em acordo, tratado ou convenção internacional e se trate de situação em que tal intercepção seja admissível, nos termos do artigo 18º, em caso nacional semelhante. 2 - É competente para a recepção dos pedidos de intercepção a Polícia Judiciária, que os apresentará ao Ministério Público, para que os apresente ao juiz de instrução criminal da comarca de Lisboa para autorização. 3 - O despacho de autorização referido no artigo anterior permite também a transmissão imediata da comunicação para o Estado requerente, se tal procedimento estiver previsto no acordo, tratado ou convenção internacional com base no qual é feito o pedido. 4 - O disposto no nº 1 aplica -se, com as devidas adaptações, aos pedidos formulados pelas autoridades judiciárias portuguesas.
Artigo 34.º – Auxílio mútuo para a intercepção de dados de conteúdo As Partes deverão conceder-se mutuamente auxílio para a recolha ou o registo, em tempo real, de dados relacionados com o conteúdo de comunicações específicas transmitidas através de um sistema informático, na medida em que os seus tratados e respectivo direito interno em vigor o permitam.	**Artigo 26º - Intercepção de comunicações em cooperação internacional** 1 - Em execução de pedido da autoridade estrangeira competente, pode ser autorizada pelo juiz a intercepção de transmissões de dados informáticos realizadas por via de um sistema informático localizado em Portugal, desde que tal esteja previsto em acordo, tratado ou convenção internacional e se trate de situação em que tal intercepção seja admissível, nos termos do artigo 18º, em caso nacional semelhante. 2 - É competente para a recepção dos pedidos de intercepção a Polícia Judiciária, que os apresentará ao Ministério Público, para que os apresente ao juiz de instrução criminal da comarca de Lisboa para autorização. 3 - O despacho de autorização referido no artigo anterior permite também a transmissão imediata da comunicação para o Estado requerente, se tal procedimento estiver previsto no acordo, tratado ou convenção internacional com base no qual é feito o pedido. 4 - O disposto no nº 1 aplica -se, com as devidas adaptações, aos pedidos formulados pelas autoridades judiciárias portuguesas.
Artigo 35.º – Rede 24/7 1. Cada Parte deverá designar um ponto de contacto que deverá estar disponível 24 horas por dia, sete dias por semana, a fim de assegurar de imediato a prestação de auxílio nas investigações e nos procedimentos relativos	**Artigo 21º - Ponto de contacto permanente para a cooperação internacional** 1 - Para fins de cooperação internacional, tendo em vista a prestação de assistência imediata para os efeitos referidos no artigo anterior, a Polícia Judiciária assegura a manutenção de uma estrutura que garante um ponto de contacto

a infracções penais relacionadas com sistemas informáticos, ou na recolha de provas sob a forma electrónica, da prática de infracções penais. Esse auxílio deverá compreender a facilitação ou, se o direito e a prática internos o permitirem, a execução directa das seguintes medidas: a) O aconselhamento técnico; b) A conservação de dados em conformidade com os artigos 29.º e 30.º; c) A recolha de provas, prestação de informações de natureza jurídica e localização de suspeitos. 2. a) O ponto de contacto de uma Parte deverá dispor de meios para contactar com rapidez o ponto de contacto de uma outra Parte. b) O ponto de contacto designado por uma Parte deverá assegurar que se pode coordenar de forma célere com a ou as autoridades dessa Parte responsáveis pelo auxílio mútuo internacional ou pela extradição, caso não seja parte integrante dessa ou dessas autoridades. 3. Cada Parte deverá assegurar que dispõe de pessoal com formação e equipamento de modo a facilitar o funcionamento da rede.	disponível em permanência, vinte e quatro horas por dia, sete dias por semana. 2 - Este ponto de contacto pode ser contactado por outros pontos de contacto, nos termos de acordos, tratados ou convenções a que Portugal se encontre vinculado, ou em cumprimento de protocolos de cooperação internacional com organismos judiciários ou policiais. 3 - A assistência imediata prestada por este ponto de contacto permanente inclui: *a*) A prestação de aconselhamento técnico a outros pontos de contacto; *b*) A preservação expedita de dados nos casos de urgência ou perigo na demora, em conformidade com o disposto no artigo seguinte; *c*) A recolha de prova para a qual seja competente nos casos de urgência ou perigo na demora; *d*) A localização de suspeitos e a prestação de informações de carácter jurídico, nos casos de urgência ou perigo na demora; *e*) A transmissão imediata ao Ministério Público de pedidos relativos às medidas referidas nas alíneas *b*) a *d*)*,* fora dos casos aí previstos, tendo em vista a sua rápida execução. 4 - Sempre que actue ao abrigo das alíneas *b*) a *d*) *d*o número anterior, a Polícia Judiciária dá notícia imediata do facto ao Ministério Público e remete -lhe o relatório previsto no artigo 253º do Código de Processo Penal. **Artigo 29º - Competência da Polícia Judiciária para a cooperação internacional** A competência atribuída pela presente lei à Polícia Judiciária para efeitos de cooperação internacional é desempenhada pela unidade orgânica a quem se encontra cometida a investigação dos crimes previstos na presente lei.
Artigo 42.º - Reservas Qualquer Estado pode, no momento da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, mediante notificação escrita dirigida ao Secretário-Geral do Conselho da Europa, declarar que se reserva a faculdade de utilizar a ou as reservas previstas no n.º 2 do artigo 4.º, n.º 3 do artigo 6.º , n.º 4 do artigo 9.º, n.º 3 do artigo 10.º, n.º 3 do artigo 11.º, n.º 3 do artigo 14.º, n.º 2 do artigo 22.º, n.º 4 do artigo 29.º, e n.º 1 do artigo 41.º. Nenhuma outra reserva pode ser formulada.	**Declaration transmitted by a letter from the Permanent Representative of Portugal, dated 30 April 2010, registered at the Secretariat General on 4 May 2010 - Or. Engl.** In accordance with Article 24, paragraph 7a, of the Convention, Portugal declares that in those cases in which the Convention on Extradition or other bilateral or multilateral instruments on extradition are not applicable, the authority responsible for making or receiving requests for extradition or provisional arrest is the *Procuradoria-Geral da República* (Rua da Escola Politécnica, 140 - 1269-269 Lisboa, Portugal). **Period covered: 1/7/2010 -**

The preceding statement concerns
Article(s) : 24

Declaration transmitted by a letter from the Permanent Representative of Portugal, dated 30 April 2010, registered at the Secretariat General on 4 May 2010 - Or. Engl.

In accordance with Article 27, paragraph 2c, of the Convention, Portugal declares that, in the absence of applicable international agreements, the authority responsible for sending and answering requests for mutual legal assistance is the *Procuradoria-Geral da República* (Rua da Escola Politécnica, 140 - 1269-269 Lisboa, Portugal).
Period covered: 1/7/2010 -

The preceding statement concerns
Article(s) : 27

Declaration contained in the instrument of ratification deposited on 24 March 2010 - Or. Engl.

In accordance with Article 24, paragraph 5, of the Convention, the Portuguese Republic declares that it shall not grant extradition of persons who:

a) are to be trialled by an exceptional court or who are to serve a sentence passed by such a court;
b) it has been proved will be subject to a trial which affords no legal guarantees of criminal proceedings complying with the conditions internationally recognised as essential to the protection of human rights, or will serve their sentences in inhuman conditions;
c) are being demanded in connection with an offence punishable with a lifetime sentence or a lifetime detention order.

The Portuguese Republic shall grant extradition only for crimes punishable with penalty of deprivation of liberty superior to one year.

The Portuguese Republic shall not grant extradition of Portuguese nationals.

	Portugal shall not grant extradition for offences punishable with the death penalty under the law of the requesting State. Portugal shall authorise transit through its national territory only in respect of persons whose circumstances are such that their extradition may be granted. **Period covered: 1/7/2010 -** The preceding statement concerns Article(s) : 24 **Declaration transmitted by a letter from the Permanent Representative of Portugal, dated 30 April 2010, registered at the Secretariat General on 4 May 2010 - Or. Engl.** In accordance with Article 35, paragraph 1, of the Convention, Portugal designates as point of contact for the network 24/7 the *Policia Judiciária* (Rua Gomes Freire, 174 - 1169-007 Lisboa, Portugal; telephone (+351) 218 641 000, fax (+351) 213 304 260). **Period covered: 1/7/2010 -** The preceding statement concerns Article(s) : 35