

Coordenação e Notas

Pedro Verdelho, Rogério Bravo e Manuel Lopes Rocha

Com a colaboração de Paula Veiga

LEIS DO **CIBERCRIME**

VOLUME 1

Colecção Direito das Novas Tecnologias

A nova economia, dependente das novas tecnologias da informação, traz consigo novos desafios e ameaças.

Quais as respostas dos nossos Juristas, tribunais, compêndios e legislação?



[Encomendar](#)

101 Perguntas e Respostas do Direito da Internet e da Informática

Autores: Ana Margarida Marques, Mafalda Anjos e Sónia Queiróz Vaz

Nº Páginas: 352

ISBN: 972-8426-50-X

Depósito legal: 179.034/02

Preço (papel): 22,20 Euros

Preço (digital): 11,10 Euros

Data da 1ª Edição: Abril/2002



[Encomendar](#)

Guia Jurídico da Internet em Portugal

Autores: Paula Rainha e Sónia Queiróz Vaz

Nº Páginas: 424

ISBN: 972-8426-35-6

Depósito legal: 162.701/01

Preço (papel): 4.450\$00/22,20 Euros

Preço (digital): 2.225\$00/11,10 Euros

Data da 1ª Edição: Março/2001



[Encomendar](#)

As Leis do Comércio Electrónico

Autor: [Manuel Lopes Rocha](#), [Miguel Pupo Correia](#), [Marta Felino Rodrigues](#), [Miguel Almeida Andrade](#), [Henrique José Carreiro](#)

Nº Páginas: 336

ISBN: 972-8426-25-9

Dep. Legal: 147.881/00

Preço (papel): 2.950\$00/14,71Euros

Preço (digital): 1.475\$00/7,36 Euros

Data da 1ª Edição: Março/2000

Dimensões: 15*23cm



[Encomendar](#)

Direito da Informática nos Tribunais Portugueses

Autor: Manuel Lopes Rocha

Nº Páginas: 212

ISBN: 972842609-7

Dep. Legal: 131.444/99

Preço (papel): 2.450\$00/12,22 Euros

Preço (digital): 1.225\$00/6,11 Euros

Data da 1ª Edição: Março/99

PEDRO VERDELHO,
ROGÉRIO BRAVO e
MANUEL LOPES ROCHA
COM A COLABORAÇÃO DE PAULA VEIGA

LEIS DO CIBERCRIME

Vol. I



CENTRO ATLÂNTICO .PT

Portugal/2003

Reservados todos os direitos por Centro Atlântico, Lda.
Qualquer reprodução, incluindo fotocópia, só pode ser feita com autorização expressa dos editores da obra.

Leis do Cibercrime - vol. I

Colecção: Direito das Novas Tecnologias
Autores: Pedro Verdelho, Rogério Bravo e Manuel Lopes Rocha
com a colaboração de Paula Veiga

Direcção gráfica: Centro Atlântico
Revisão final: Centro Atlântico
Capa: Paulo Buchinho

© Centro Atlântico, Lda., 2003
Av. Dr. Carlos Bacelar, 968 - Escr. 1 - A
4764-901 V. N. Famalicão
Rua da Misericórdia, 76 - 1200-273 Lisboa
Portugal
Tel. 808 20 22 21

geral@centroatlantico.pt
www.centroatlantico.pt

Design e Paginação: Centro Atlântico

Impressão e acabamento: Rolo & Filhos
1ª edição: Julho de 2003
ISBN: 972-8426-69-0
Depósito legal: 197.992/03

Marcas registadas: todos os termos mencionados neste livro conhecidos como sendo marcas registadas de produtos e serviços, foram apropriadamente capitalizados. A utilização de um termo neste livro não deve ser encarada como afectando a validade de alguma marca registada de produto ou serviço.

O Editor e os Autores não se responsabilizam por possíveis danos morais ou físicos causados pelas instruções contidas no livro nem por endereços Internet que não correspondam às Home-Pages pretendidas.

Apesar de terem sido tomadas todas as precauções, podem ter existido falhas humanas ou técnicas na transcrição da legislação ou nas suas referências. Por essas, ou por quaisquer outras falhas eventualmente existentes neste livro, quer o Editor quer os Autores, não assumem qualquer responsabilidade.

APRESENTAÇÃO

Publica-se a tradução para português da Convenção sobre Cibercrime do Conselho da Europa. Este instrumento de direito internacional foi aceite por Portugal, que participou na sua elaboração e o assinou. Não foi ainda ratificado pelo direito interno nem foram ainda acolhidas na legislação nacional as suas imposições.

Faz-se a sua publicação integral. Ao texto, são feitos dois comentários: um deles, prévio, é sistémico e aborda a Convenção na sua globalidade; o outro é fragmentário e dirige-se a concretos aspectos do texto. Além disso, publica-se o Relatório Explicativo da Convenção. É um texto extenso e exaustivo, apresentado como relatório final do grupo de trabalho que procedeu à elaboração material do articulado da Convenção. Nele são feitas considerações e dadas explicações sobre as opções do texto e sobre a interpretação que os seus autores fazem das respectivas fórmulas. Trata-se pois de um importante instrumento de interpretação, quer da Convenção, quer da eventual lei nacional a que aquela vier a dar origem.

Publica-se também o vigente texto da Lei da Criminalidade Informática, de 1991. É ainda hoje a estrutural ferramenta legal de combate ao cibercrime. Também a ela é feito um comentário.

Por último, é publicado o texto e o relatório explicativo da Proposta de Decisão Quadro apresentada pela Comissão da União Europeia ao Conselho, relativa a ataques contra os sistemas de informação, a 19 de Abril de 2002 (publicada no JOCE nº C 203E/109, de 27 de Agosto de 2002). Não se trata de um texto com força legal, porque é uma proposta legislativa. Na data em que se encerra esta publicação decorrem as discussões sobre o articulado do projecto de decisão, no seio do Conselho. Não existe ainda uma versão final do projecto de decisão a adoptar. Sabe-se já que desta discussão irá resultar um texto normativo profundamente alterado, com referência à proposta. Não obstante, pelo marco histórico que esta proposta constitui e por ser a génese de algo que irá surgir, optou-se pela publicação.

Para um segundo volume se deixa a publicação dos diplomas legais que hão-de surgir, de transposição para a lei portuguesa dos instrumentos internacionais aos quais Portugal está vinculado.

ÍNDICE

APRESENTAÇÃO	5
I. CONVENÇÃO SOBRE CIBERCRIME	9
I. 1 CONVENÇÃO SOBRE CIBERCRIME DO CONSELHO DA EUROPA – COMENTÁRIO	10
I.2 CONVENÇÃO SOBRE O CIBERCRIME	24
I.3 RELATÓRIO EXPLICATIVO	102
II. LEI DA CRIMINALIDADE INFORMÁTICA	235
II.1. LEI DA CRIMINALIDADE INFORMÁTICA - LEI N.º 109/91 DE 17 DE AGOSTO	236
II.2 COMENTÁRIO À LEI DA CRIMINALIDADE INFORMÁTICA	246
III. DECISÃO-QUADRO DO CONSELHO RELATIVA A ATAQUES CONTRA OS SISTEMAS DE INFORMAÇÃO (PROPOSTA APRESENTADA PELA COMISSÃO)	289
III.1. EXPOSIÇÃO DE MOTIVOS	290
III.2. PROPOSTA 2002/0086 (Cns) PROPOSTA DE DECISÃO-QUADRO DO CONSELHO RELATIVA A ATAQUES CONTRA OS SISTEMAS DE INFORMAÇÃO	315

I.

CONVENÇÃO

SOBRE

CIBERCRIME

I.1. A Convenção sobre Cibercrime do Conselho da Europa - COMENTÁRIO

1. A Convenção

A Convenção sobre Cibercrime do Conselho da Europa é o primeiro trabalho internacional de fundo sobre crime no ciberespaço. Foi elaborado por um comité de peritos nacionais, congregados no Conselho da Europa e consiste num documento de direito internacional público. Embora tenha na sua origem, sobretudo, países membros do Conselho da Europa, tem vocação universal. Na sua elaboração participaram vários outros países (Estados Unidos da América, Canadá, Japão e África do Sul) e pretende-se que venha a ser aceite pela generalidade dos países do globo.

Sendo o primeiro tratado internacional sobre criminalidade contra sistemas de computadores, redes ou dados, pretende harmonizar as várias legislações nacionais sobre a matéria, propiciar e facilitar a cooperação internacional e facilitar as investigações de natureza criminal.

Para o efeito, esta convenção incide sobre direito penal material (definindo crimes contra a confidencialidade, integridade e disponibilidade dos sistemas de computadores, crimes referentes aos conteúdos e crimes cometidos por via da informática) mas inclui também medidas processuais e de cooperação judiciária internacional.

A sua versão definitiva foi aberta à assinatura a 23 de Novembro de 2001, tendo Portugal assinado.

2. Repercussão na legislação portuguesa

2.1. Direito Penal Material

A Convenção do Cibercrime assume concepções e soluções que já antes haviam sido expressas na resolução nº 9(89) do Conselho da Europa, que foi traduzida para português pela Lei nº 109/91, de 17 de Agosto. Vai, porém, mais além.

A lei portuguesa da criminalidade informática (Lei nº 109/91, de 17 de Agosto) prevê definições – cfr. Artigo 2º. Porém, algumas das definições

consagradas na Convenção do Cibercrime não estão ali previstas. Assim acontece com as expressões “dados informáticos”, “fornecedor de serviço” e “dados de tráfego”. Quanto ao conceito de “dados de tráfego” (*traffic data*) e ao conceito de “fornecedor de serviço” (*service provider*) são novos, específicos do ambiente Internet, até agora não previstos na legislação criminal portuguesa. O conceito de “dados informáticos” (*computer data*) é uma versão mais alargada e adaptada ao ambiente Internet do já existente conceito de “programa informático” (conceito que, aliás, está expressamente incluído no novo conceito de *computer data*).

Quanto à parte da Convenção concernente à lei penal material (Capítulo II, Secção 1), na globalidade, os tipos de crime estão já previstos na legislação portuguesa. Mas existem novos tipos de crime. Por outro lado, os crimes já existentes poderão carecer de alguns ajustamentos. Quanto ao crime de acesso ilegal (previsto no Artigo 2º da Convenção), está já previsto na lei portuguesa (Artigo 7º da Lei nº 109/91). O mesmo acontece com o crime de interceptação ilegal (previsto no Artigo 3º da Convenção), consagrado no Artigo 8º da Lei nº 109/91. Poderão, porém, suscitar-se dúvidas quanto à compatibilidade entre os dois textos porque a Convenção refere a interceptação de *non-public transmissions of computer data* e a lei portuguesa “comunicações de dados de interior de um sistema ou rede informáticos”. No que respeita ao crime de dano informático (*data interference*, previsto no Artigo 4º da Convenção), está previsto no Artigo 5º da Lei nº 109/91. Esta disposição da lei portuguesa inclui, porém, elementos adicionais, que restringem o tipo de crime, dando dele um enfoque mais limitado que o da Convenção. Designadamente assim acontece quando se prevê no Artigo 5º da Lei nº 109/91 que o crime será cometido “com a intenção de causar prejuízo ou obter benefício”, enquanto na Convenção apenas se prevê que os actos sejam *committed intentionally*. Por outro lado, na Convenção está prevista, como actuação ilícita, a *alteration of computer data*, expressão que não está consagrada na lei portuguesa. O mesmo acontece no que respeita ao crime de sabotagem informática, previsto no Artigo 5º da Convenção e no Artigo 6º da Lei nº 109/91. Isto é, há também expressões previstas no projecto que não se prevêem na lei portuguesa. É o caso de *transmitting, damaging* e *deteriorating*. Quanto ao demais, o tipo de crime previsto no Artigo 6º da Lei nº 109/91 é mais alargado que o previsto no projecto de Convenção, uma vez que abrange qualquer tentativa de perturbação e não só, como na Convenção, *the serious hindering*.

Já o crime de *misuse of devices* (previsto no Artigo 6º da Convenção) é inovador. Não está previsto na legislação portuguesa. Existe, porém, a possibilidade de formular parcial reserva à sua aplicação (cfr. o nº 3 do Artigo 6º), o que foi consagrado por influência do Japão. Se não for formulada reserva, o legislador nacional deverá introduzir este novo crime na legislação nacional.

O crime de falsidade informática, previsto no Artigo 7º da Convenção, está formulado de forma algo diferente do seu correspondente na lei portuguesa (Artigo 4º da Lei nº 109/91), sem que, todavia, se afigure haver divergências de fundo entre ambos. As realidades factuais cobertas por ambas as normas tendencialmente coincidem. O mesmo se passa no que respeita à burla informática, prevista no Artigo 8º da Convenção e no Artigo 221º do Código Penal.

Uma das grandes divergências com a lei nacional respeita à incriminação de factos respeitantes a pornografia infantil (Artigo 9º da Convenção). Por um lado, este instrumento de direito internacional consagra os 18 anos como a idade de referência quando se fala de um menor, embora possa fazer-se descer este limite aos 16 anos (nº 4 do Artigo 9º da Convenção). O que está em causa não é a definição da idade de livre determinação sexual de menores, questão que escapa ao âmbito da Convenção. Trata-se da idade a partir do qual é admissível – ou não censurável pela lei –, explorar, numa perspectiva pornográfica, imagens de pessoas numa conduta sexual explícita. A lei portuguesa prevê – Artigo 172º do Código Penal –, a punição criminal de exploração de imagens sexuais quanto a menores de 14 anos. A fasquia dos 18 anos, idade bastante abrangente, é já considerada nas discussões sobre a matéria em outros *fora* internacionais – *maxime* a ONU. Não obstante, esta previsão virá a criar, a Portugal, a obrigação de alterar a sua legislação penal. Com efeito, esta Convenção que o Estado Português já assinou passará a obrigar Portugal a considerar e punir como crime os actos que traduzem pornografia em relação a menores de 18 anos. Porém, apesar desta necessidade de alteração legislativa, não se afigure haver contradição essencial desta posição com o conjunto do sistema legal português. De facto, na lei portuguesa de protecção de menores são consideradas pessoas que tenham até 18 anos. Ou seja, para efeitos de protecção de menores a idade considerada pela lei é justamente aquela que se consagra nesta Convenção. Daí que, destinando-se o conjunto destas normas referentes à pornografia infantil a satisfazer os interesses de protecção das crianças, não se

afigura que este marco seja inaceitável, parecendo até que, mau grado exigir uma alteração à legislação penal, vai de encontro ao espírito da legislação portuguesa.

Mais complexa é a questão da criminalização da mera posse de pornografia infantil. De facto, na Convenção prevê-se como crime a mera posse de material pornográfico infantil num sistema de computadores (alínea e) do nº 1 do Artigo 9º). Este pormenor não está abrangido pelo Código Penal Português - Artigo 172º, após a alteração da Lei nº 65/98, de 2 de Setembro.

A tendência mais recente das instâncias internacionais vai no sentido da criminalização da mera posse de material pedófilo. A Convenção vai mais longe, atingindo não só as situações em que as imagens em causa representem efectivamente crianças como também as representações fictícias de crianças (por exemplo, as imagens de crianças completamente criadas em computador ou as imagens de adultos a representar crianças). A criminalização da mera posse de material pedófilo visa, por um lado, satisfazer interesses práticos, de prova de factos em investigação. Ou seja, visa permitir punir quem tenha material pedófilo, suspeitando-se, sem prova suficiente, que o destina à difusão. Permite pois às autoridades policiais e judiciárias prosseguir e accionar criminalmente pessoas de quem se suspeita ser difusor de material pornográfico pedófilo, pela via da mera posse. Por outro lado, a punição da mera posse pretende ser uma forma de dissuadir o eventual interesse pela difusão deste tipo de material. Ora, se no caso da punição da mera posse de imagens de crianças pode ainda ver-se uma forma, embora não directa, de protecção dos interesses dessas crianças, no caso da mera posse de imagens virtuais ou de falsas crianças essa razão não existe.

Todavia, a previsão do nº 4 do Artigo 9º permite a formulação de reserva à aplicação, entre outras, da punição de todas as situações de mera posse e da punição do *procuring* de material pornográfico.

A este propósito há que referir que a Nona Alteração ao Código Penal (Lei nº 99/2001, de 25 de Agosto) criminalizou a posse de material pedófilo, mas apenas se essa posse tem como determinação “o propósito de os exhibir ou ceder” (alínea e) do nº 3 do Artigo 172º). Isto é, a alteração do Código Penal, realizada já depois de estar concluído o texto da Convenção do Cibercrime, consagrou uma solução mais restrita (menos incriminadora)

que a prevista na Convenção. Ou seja, nesta matéria resta a Portugal alterar mais uma vez o Código Penal (que neste aspecto já foi alterado em 1995, 1998 e 2001), passando a punir a mera posse de material pornográfico infantil ou, em alternativa, formular reserva à aplicação de parte deste Artigo 9º do projecto de Convenção. A este propósito refira-se ainda que a União Europeia tem adoptado posições no sentido de criminalizar a mera posse de material pornográfico infantil (veja-se, por exemplo, a decisão do Conselho da União Europeia sobre pornografia na Internet, adoptada em 29 de Maio de 2000).

No que respeita ao direito de autor e direitos conexos, nos termos do Artigo 10º da Convenção, não se afigura haver alterações a efectuar à legislação nacional. De facto, a Convenção apenas obriga os Estados contratantes a incriminar violações de direito de autor e conexos, quando cometidos por via de um sistema de computadores, de forma idêntica à já prevista na lei nacional, em respeito por tratados internacionais. Estão, designadamente, em causa o Acordo de Paris de 24 de Julho de 1971, a Convenção de Berna sobre Protecção de Trabalhos Literários e Artísticos, o Acordo sobre Aspectos Comerciais dos Direitos da Propriedade Intelectual, o Tratado WIPO sobre *Copyright*, a Convenção Internacional para a Protecção dos Intérpretes, Produtores de Fonogramas e Organismos de Radiodifusão (Convenção de Roma) e o Tratado WIPO sobre Interpretações e Fonogramas. Todavia, consagrou-se na Convenção uma restrição à aplicabilidade destes tratados no ambiente digital. De facto, optou-se por limitar a aplicabilidade de sanções criminais a situações em que a violação do direito de autor fosse grave, o que foi traduzido pela expressão *on a commercial scale*. Optou-se também por excluir a punição da violação de direitos morais e a punição de violações não intencionais de direito de autor.

O Artigo 11º da Convenção prevê a obrigação de os Estados incriminarem actos de cumplicidade na prática de todos os crimes previstos e a obrigação de incriminarem a tentativa no que respeita a alguns dos crimes (excluem-se os crimes de acesso ilegal, *misuse of devices* e os crimes relacionados com o direito de autor e conexos). No que respeita ao direito português, a punição da cumplicidade resultaria já da aplicação do Artigo 27º do Código Penal. Por sua vez, quanto à tentativa, ela é já expressamente punida para os crimes de interceptação ilegítima (Artigo 8º, nº2) e dano informático (Artigo 5º, nº 2), ambos previstos na Lei nº 109/91. Quanto à sabotagem informática e à falsidade informática, previstos na mesma lei, a tentativa é

punível por a respectiva pena máxima ser superior a 3 anos de prisão – Artigo 23º do Código Penal. Também em função do limite máximo da pena, o mesmo acontece com os ilícitos respeitantes à pornografia infantil previstos na lei portuguesa e a burla informática (no caso do crime de burla informática não qualificada, previsto no nº 1 do Artigo 221º do Código Penal, cuja pena máxima é de 3 anos, a tentativa é punível por existir disposição expressa – cfr o nº 3 do mesmo artigo).

No que respeita à responsabilização criminal de pessoas colectivas, a mesma está prevista no Artigo 12º da Convenção. Esta responsabilidade ocorre se forem praticados actos por representantes legítimos de pessoas colectivas, em sua representação e benefício. Mas ocorre também se, por omissão de supervisão ou controlo da parte de um legal representante da pessoa colectiva, alguém sob a sua autoridade pratica um acto ilícito em seu benefício. Na falta de um quadro geral que defina genericamente a incriminação de pessoas colectivas (cfr. *a contrario*, o Artigo 11º do Código Penal), não se afigura que a forma como aqui se prevê esta responsabilização choque com o espírito das situações em que ela existe, no direito português. Aliás, a responsabilização de pessoas colectivas está já prevista quanto à chamada criminalidade informática, no Artigo 10º da Lei nº 109/91.

2.2. Direito Processual

Uma das previsões mais importantes da Convenção é a que consta do Artigo 14º, que consagra o âmbito de aplicação das medidas processuais. Prevê-se a aplicação da Convenção aos crimes que ela define, mas estão previstas duas extensões extremamente significativas: por um lado, prevê-se que sejam aplicadas a qualquer outro tipo de crime cometido por via de um sistema de computadores; por outro, prevê-se que sejam aplicáveis à obtenção de prova em forma electrónica, se respeitante a ilícitos criminais. Porém, quanto a estas duas extensões, o projecto prevê que os Estados possam formular reservas.

Não se afigura haver incompatibilidade desta previsão com a legislação nacional, não se afigurando necessária a formulação de qualquer reserva. Tanto mais que é o próprio texto da Convenção que prevê que a aplicação das disposições processuais deverá observar as condições e salvaguardas dos direitos nacionais e dos instrumentos internacionais na área dos direitos

humanos, bem como a regra da proporcionalidade da medida à natureza e circunstâncias da infracção.

Nos Artigos 16º e 17º da Convenção estão previstas a preservação expedita de dados armazenados num computador e a preservação expedita e revelação de dados de tráfego. A previsão destas duas medidas processuais é separada. Tal separação é motivada pelo diferente enfoque de ambas. Ambas são medidas expeditas, impostas pela velocidade da circulação da informação no ambiente digital. O seu carácter expedito faz diminuir as garantias dos visados pela investigação em causa. Por isso, se quanto aos meros dados de tráfego está também prevista a sua revelação expedita, o mesmo não acontece quanto aos outros dados (o conteúdo da comunicação ou dados já armazenados). Ambas as medidas são inovadoras. Por outro lado, ambas são essenciais para o sucesso de eventuais investigações criminais no domínio digital. A rapidez na preservação de dados é normalmente imprescindível a qualquer investigação, uma vez que se assim não for, pela sua natureza, os dados perder-se-ão. É razoável, neste contexto, quanto aos dados propriamente ditos, apenas impor, como se faz na Convenção, a sua preservação, até ser obtida pelas vias normais a formalidade legalmente exigida para a sua obtenção material ou revelação (ordem judicial, ou outra). O mesmo já não vale para os dados de tráfego. De facto, os dados de tráfego permitem reconstruir o percurso de determinada comunicação. Nessa comunicação pode ter utilizado mais que um servidor Internet. Por isso, é importante que o servidor preserve e revele, de forma expedita, qual ou quais os outros operadores utilizados no percurso da comunicação em causa, permitindo assim, de forma expedita a preservação e revelação de informação por outros operadores, em tempo útil.

Afigura-se assim útil o acolhimento pela legislação nacional desta distorção às regras gerais em matéria de sigilo de telecomunicações.

É igualmente inovadora a previsão do Artigo 18º da Convenção, segundo a qual cada Estado signatário deverá adoptar as medidas legislativas necessárias à criação de um mecanismo de injunção (*production order* na versão inglesa e *injonction de production* na versão francesa) destinada a cidadãos e a servidores de Internet, pela qual as competentes autoridades ordenam que aquelas pessoas singulares e colectivas forneçam dados armazenados num computador sob a sua responsabilidade ou forneçam dados de subscritores do serviço Internet. Esta figura da injunção existe já, embora com contornos e finalidades diferentes, no processo civil português, sendo des-

conhecida no processo penal. A sua eventual introdução, com este perfil, não parece levantar problemas essenciais.

É importante sublinhar que o texto da Convenção prevê que a injunção de submeter dados seja referente a dados específicos. Ou seja, de forma expressa prevê-se que os dados em relação aos quais pode ser emitida uma injunção deverão ser previamente determinados. Esta limitação tem em vista impedir situações de abuso policial. De facto, no mundo real, numa busca e apreensão de objectos ou documentos as entidades policiais ou judiciais apenas tomam conhecimento de objectos e documentos que possam estar relacionados com o caso em investigação. Ora, ao permitir-se, sem reservas, dar ordens de submissão de dados informáticos (que, por certo, não podem aperceber-se antes de serem processados), estaria a permitir-se o acesso indiscriminado a toda e qualquer informação. É aquilo a que na gíria policial se apelida de *fishing expedition* ou de *data mining*.

A matéria da busca e apreensão de dados armazenados num computador está prevista no Artigo 19º da Convenção. A essência da medida processual em causa coincide, no ambiente do ciberespaço, com as formas de busca e apreensão, desenhadas no processo penal português. Porém, a forma como a busca e a apreensão estão descritas no Código de Processo Penal não se enquadra nas realidades do ciberespaço. Tem pois o legislador que adaptar o processo penal à realidade virtual.

Além disso, no nº 2 do Artigo 19º da Convenção prevê-se algo não previsto no direito português, embora não proibido nem contrariado. Prevê-se aí que quando no decurso de busca a um sistema de computadores se note que os dados que se procuram estarão guardados noutro sistema de computadores, as entidades competentes, de forma expedita, estenderão a busca (ou o acesso similar a que se proceda) ao outro sistema. É uma inovação que importa consagrar na lei nacional, uma vez que as buscas, tal como elas estão desenhadas no sistema processual penal, em regra, não podem ser determinadas pelas entidades que na prática as executam (é exigida, como regra, a autorização da autoridade judiciária – Ministério Público ou Juiz -, sendo como regra, as buscas executadas por entidades policiais).

Especificamente quanto a apreensões, prevê-se que os Estados devam legislar no sentido de prever a mera apreensão de dados, a elaboração ou retenção de uma cópia desses dados, a manutenção da integridade de dados informáticos relevantes guardados num sistema de computadores e a impo-

sição de impedimento de acesso ou remoção de dados de um determinado computador. Com exceção da mera apreensão de dados no seu suporte, que em nada se distingue de uma mera apreensão, todas estas medidas (incluindo a apreensão de dados separadamente do seu suporte) são medidas específicas do espaço virtual. Não são por isso enquadráveis nos conceitos actuais da lei processual. A lei portuguesa terá pois que ser ajustada a estas novas realidades.

Uma última nota, quanto à competência territorial. Apenas está prevista pela Convenção uma inovação face ao que já resulta dos Artigos 4º e 5º do Código Penal. Com efeito, prevê-se a obrigação de os Estados signatários se declararem competentes para prosseguirem criminalmente, independentemente do local da prática dos factos, os seus cidadãos nacionais se a infracção for punível no local onde foi cometida ou não for da competência de nenhum Estado (na Antártida, por exemplo). Esta solução não está consagrada na lei portuguesa. Porém, não parece que esta norma colida com qualquer princípio do ordenamento jurídico nacional, que já prevê, para certos crimes (cfr. Artigo 5º, nº 1, alínea a) do Código Penal), a competência universal da lei portuguesa.

2.3. Cooperação Internacional

As regras referentes à cooperação internacional estão previstas no Capítulo III da Convenção.

O Artigo 23º prevê regras gerais, de natureza programática, para a cooperação internacional. Sublinha o âmbito material de aplicação da convenção e a remissão para outros instrumentos internacionais.

A extradição está prevista no Artigo 24º. No geral, não são criadas regras novas ou regras que contrariem o que já resulta de anteriores instrumentos internacionais aos quais Portugal esteja vinculado. É fixado o limite mínimo de um ano de prisão, para que seja admissível a extradição, sendo paralelamente exigida a dupla incriminação. Porém, a par daqueles limites, o texto prevê a possibilidade de haver extradição para crimes de pena inferior em caso de existir um tratado bilateral entre os dois estados envolvidos e nesse tratado se prever um limite inferior. Ainda a este propósito, a Convenção prevê a possibilidade de recusa de extradição em caso de o crime em causa ser considerado um crime político ou relacionado com um crime

político e ainda quando esteja em causa a soberania, a segurança, a ordem pública ou outros interesses essenciais do Estado requerido. Além disso, está expressamente consagrado que a extradição será submetida às condições previstas na lei do país requerido e nos tratados internacionais eventualmente aplicáveis.

A Convenção inclui um pormenorizado articulado – o Artigo 27º -, a propósito das disposições gerais referentes à assistência mútua. Porém, estas disposições apenas respeitam a situações em que os Estados não estejam vinculados por acordos internacionais. São assim aplicáveis a uma pequena fatia dos potenciais signatários.

Ainda na área dos princípios gerais em matéria de assistência mútua, prevê o Artigo 26º a possibilidade de um Estado, no decurso de investigações internas, concluir que deverá reencaminhar certas informações a um outro Estado, parte nesta Convenção. Assim acontecerá se essas informações se lhe afigurarem úteis ou necessárias ao início ou ao desenvolvimento de uma investigação de um crime enquadrado na Convenção. O nº 2 do artigo prevê que essa remessa de informação seja condicionada à observância de certas condições, designadamente de confidencialidade. Não se afigura haver qualquer contradição desta previsão com o ordenamento jurídico português.

O Artigo 29º da Convenção prevê regras respeitantes à preservação expedita de dados armazenados num computador. É um regime paralelo ao que está previsto para o nível interno, mas com especificidades. Prevê-se que um Estado solicite a outro a preservação expedita de dados, desde que manifeste a intenção de vir a fazer-lhe um pedido formal de assistência para realização de uma busca, apreensão ou diligência similar. Nesse caso, o Estado requerido deverá tomar todas as medidas necessárias à preservação daqueles dados, com respeito pela sua própria lei nacional. Como nota importante, refira-se que este artigo prevê, no nº 3, que não será necessário observar o requisito da dupla incriminação, como condição da preservação dos dados. Claro está que esta dispensa do requisito de dupla incriminação apenas se reporta a crimes não previstos na Convenção – isto é, a crimes cometidos por meio de um computador ou a crimes cuja prova esteja registada num computador (aos quais os meios processuais são aplicáveis). Quanto aos crimes previstos na Convenção, existirá em princípio, dupla incriminação.

Trata-se de uma medida de cooperação internacional nova. Como outras, resulta da especificidade do ambiente digital. Por outro lado, a forma emergente que reveste a necessidade de preservar, de forma expedita, os dados, justifica a adaptação das regras. Acresce que a medida em causa é apenas de preservação de dados, por razões cautelares, sem implicar a sua revelação. Quanto à revelação, tem outras regras, mais estreitas, sobretudo se não respeitar a dados de tráfego. Por isso, poderá haver preservação de dados sem que depois haja condições para a sua divulgação ao Estado requerente. Porém, esta situação poderá ser preferível à não preservação expedita de dados por haver dúvidas (porventura ulteriormente ultrapassadas) sobre a verificação ou não de dupla incriminação. De certa forma, este texto significa uma evolução na forma como se considera o princípio da dupla incriminação. Porém, esta dispensa do requisito da dupla incriminação não vale, com a mesma amplitude, para a revelação desses dados. Por esse motivo, prevê-se que, caso os Estados exijam a verificação da dupla incriminação, possam fazer reserva no que respeita à própria preservação de dados.

Afigura-se ser interessante esta inovação, que o legislador nacional terá que operar.

O artigo 30º da Convenção prevê a revelação de dados de tráfego. São dados em relação aos quais, no contexto da Convenção, a cooperação internacional é facilitada. Não são criadas regras especiais para a sua revelação expedita, como aliás acontece ao nível interno. Valem, aliás, quanto a ela, as razões da preservação de dados ao nível doméstico.

Por sua vez, o Artigo 31º define regras gerais de pedido de assistência internacional para obtenção de dados armazenados num computador. Não cria regras especiais, remetendo para os instrumentos internacionais existentes.

Quanto ao Artigo 32º, prevê uma forma de obtenção de prova no estrangeiro sem recurso à cooperação internacional. Trata-se de, no decurso de uma investigação, obter de um computador localizado no estrangeiro, dados de livre acesso ou cujo acesso tenha sido autorizado pela pessoa com legitimidade para autorizar tal acesso. Esta forma de obtenção de prova não está prevista no processo penal português, mas também não é proibida – Artigo 125º do Código de Processo Penal. Estruturalmente, trata-se da recolha de prova em locais de acesso público ou de acesso autorizado pelo legítimo titular.

Resulta ainda da Convenção uma obrigação específica no âmbito da cooperação internacional, que é a da criação de um ponto de contacto permanentemente disponível (a chamada rede 24/7), que possa prestar a congéneres estrangeiros aconselhamento técnico, proceder à conservação expedita de dados e à recolha de outras provas e informações, bem como localizar suspeitos. Nenhuma instituição portuguesa tem disponível qualquer contacto deste tipo no âmbito da cooperação internacional, mas não se vê qualquer obstáculo legal à sua criação, desde que devidamente articulado com as autoridades judiciárias.

3. O Protocolo adicional relativo à incriminação de actos de natureza racista ou xenófoba cometidos através de sistemas informáticos.

Na convenção do Cibercrime não foi inserida nenhuma norma incriminando a difusão de material de conteúdo racista, embora esta nova incriminação tenha sido debatida no comité redactor. Veio a ser abandonada por não haver consenso na sua inserção, já que para algumas das ordens jurídicas nacionais dos Estados contratantes a sua previsão iria eventualmente colidir com o direito de liberdade de expressão.

Houve porém evoluções, registadas noutros *fora* internacionais, designadamente em conferências no âmbito do Conselho da Europa e das Nações Unidas de luta contra o racismo.

Após a assinatura da Convenção do Cibercrime foi constituído um novo comité, destinado à elaboração de um protocolo adicional à Convenção. Do respectivo trabalho resultou uma proposta de protocolo adicional que tem por finalidade incriminar actos de natureza racista ou xenófoba, cometida através de sistemas informáticos.

Liminarmente, há que considerar que este protocolo denota uma clara intenção de obter consenso. Ou seja, as soluções consagradas são minimalistas, de modo a que possam aderir a este protocolo um grande número de Estados, sem que haja colisão com os princípios das respectivas ordens jurídicas. A fórmula encontrada foi definir um elenco alargado de crimes, mas prevendo-se para a maior parte deles a possibilidade de formular reservas.

Prevê-se assim a incriminação da difusão e outras formas de colocação à disposição do público de material racista e xenófobo em sistemas informá-

ticos. Porém, a este propósito, prevê-se a possibilidade de formular reserva e não incriminar esta difusão se a mesma não implicar violência e estiverem previstas outras sanções não penais. Além disso, prevê-se mesmo a possibilidade de reserva total, se esta incriminação colidir com princípios nacionais consagrados a propósito da liberdade de expressão.

Este crime é completamente inovador na ordem jurídica portuguesa, embora não se afigure contrariar os princípios estruturantes do ordenamento jurídico português. Recorde-se que na Constituição da República se consagra o princípio da igualdade de todos os cidadãos independentemente da sua raça, cor, religião ou credo político.

Outro dos crimes previstos é o da ameaça com motivação racista ou xenófoba. Traduz-se em proferir ameaça de prática de crime grave contra outrem, através de um sistema informático. Esta ameaça pode ser dirigida a um indivíduo concreto, em função da sua raça, da sua cor, da sua ascendência ou origem nacional ou étnica, ou ainda da sua religião na medida em que isso sirva de pretexto a um dos outros elementos. Mas pode também ser dirigida a um grupo de pessoas com estas características. Este é o único dos crimes previstos que não admite a formulação de qualquer reserva.

Este crime não está expressamente consagrado na ordem jurídica nacional. Porém, não parece que seja necessário alterá-la para ir ao seu encontro. O crime de ameaça, tal como ele é previsto pelo Artigo 153º do Código Penal, parece cobrir este tipo de situações. Na lei portuguesa não está prevista a motivação da ameaça. Por outro lado, no projecto de Protocolo são considerados “crimes graves”, sendo no Código Penal Português considerados crimes “contra a vida, a integridade física, a liberdade pessoal, a liberdade e autodeterminação sexual ou bens patrimoniais de valor elevado” e ainda “crimes com pena de prisão superior a três anos”. Por último, há que considerar que o crime de ameaça, no Código Penal, exige um elemento do tipo não previsto expressamente no projecto de Protocolo, o qual é o de a actuação em causa “provocar medo ou inquietação ou prejudicar a liberdade de determinação”.

Prevê-se ainda como crime, no projecto de Protocolo, o insulto com motivação racista ou xenófoba, feito por via de um sistema informático. Está prevista a possibilidade de formular reserva integral a este artigo ou, em alternativa, de exigir como elemento do tipo de crime o de a pessoa visada ser exposta a ódio ou ao ridículo.

Não se afigura ser necessária qualquer adaptação da lei nacional para satisfazer esta incriminação, face à formulação abrangente dos crimes de difamação e de injúria, previstos nos Artigo 180º e 181º do Código Penal, que incriminam palavras ou imputação de actos “ofensivos da honra ou consideração”.

Por outro lado, está já expressamente prevista, no Artigo 240º do Código Penal, a difamação ou injúria contra pessoa em razão da sua raça, em reunião pública ou através da comunicação social com intenção de encorajar ou incitar discriminação racial.

O último dos crimes previstos é mais complexo e traduz-se na negação, minimização grosseira, aprovação ou justificação de genocídio ou de crimes contra a humanidade. No fundo, impõe a incriminação daqueles que fazem a apologia de certas ideologias através da negação de realidades históricas generalizadamente aceites.

Este crime prevê a formulação de reserva, seja integral, seja à condição de a acção em causa incitar ao ódio, à discriminação ou à violência.

Com este crime pretende evitar-se que se reescreva a história ou se defendam determinadas ideologias através da negação de factos históricos. É certo que, em Portugal, a Constituição da República, prevê a proibição da apologia de certo tipo de ideologias. Porém, nem por isso a esta proibição é dada relevância criminal. Ou seja, face à ordem jurídica nacional este crime será, a ser adoptado, um caso isolado e, quiçá, injustificado de extensão do direito criminal.

Como última nota, refira-se que o projecto de Protocolo prevê a definição de “material racista ou xenófobo”, a qual não existe no direito português. É dito ser “material racista ou xenófobo” todo o material escrito, imagem ou outra representação de ideias ou de teorias que preconizem ou encorajem a raiva, discriminação ou violência contra uma pessoa ou grupo de pessoas em função da sua raça, da sua cor, a sua ascendência ou origem nacional ou étnica, ou ainda da sua religião na medida em que isso sirva de pretexto a um dos outros elementos.

I.2. Convenção sobre o Cibercrime

Budapeste, 23.XI.2001

Preâmbulo

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Recordando as Recomendações do Comité de Ministros N.º R (85) 10 relativa à aplicação prática da Convenção Europeia sobre Auxílio Judiciário Mútuo em Matéria Penal quanto às cartas rogatórias para a intercepção de telecomunicações, N.º R (88) 2 sobre as medidas destinadas a combater a pirataria no domínio do direito de autor e dos direitos conexos, N.º R (87) 15 que regula a utilização de dados de carácter pessoal no sector da polícia, N.º R (95) 4 relativa à protecção dos dados de carácter pessoal no sector das telecomunicações, tendo em conta, designadamente os serviços telefónicos e a N.º R (89) 9 sobre a criminalidade informática que estabelece directrizes para os legisladores nacionais respeitantes à definição de certos crimes informáticos e, ainda, a N.º R (95) 13 relativa a problemas processuais penais relacionados com as tecnologias da informação;

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

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

Acordaram no seguinte:

Capítulo I – Terminologia

Artigo 1º - Definições

Para os fins da presente Convenção:

- a) “Sistema informático” significa qualquer dispositivo isolado ou grupo de dispositivos relacionados ou interligados, em que um ou mais de entre eles, desenvolve, em execução de um programa, o tratamento automatizado dos dados;
- b) “Dados informáticos” significa qualquer representação de factos, de informações ou de conceitos sob uma forma susceptível de processamento num sistema de computadores, incluindo um programa, apto a fazer um sistema informático executar uma função;
- c) “Fornecedor de serviço” significa:
 - (i) Qualquer entidade pública ou privada que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático e
 - (ii) Qualquer outra entidade que processe ou armazene dados informáticos em nome do referido serviço de comunicação ou dos utilizadores desse serviço.
- d) “Dados de tráfego” significa todos os dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.

COMENTÁRIO

Como primeiro destaque, a assunção do termo “cibercrime” para definir de forma genérica uma panóplia de crimes praticados com recurso a novas tecnologias, como as de informação e de comunicação.

Aqui, nada de novo: caem naquele conceito crimes novos a par de crimes antigos praticados de formas novas; é a tradicional distinção entre “criminalidade informática” e “criminalidade praticada com recurso a meios informáticos” e por via desta separação, a dupla ver-

tente das tecnologias de informação elas próprias quer como “meio de execução” quer como “alvo do crime”.

Como segundo ponto a destacar, a eleição da necessidade de proteger a sociedade do cibercrime como prioridade da política criminal europeia, acentuando desta forma o carácter eminentemente repressivo da Convenção. Com maior ou menor intensidade, esta linha orientadora poderá repercutir-se a prazo, na política criminal portuguesa e no ordenamento jurídico interno, para além da própria Convenção.

Depois, há ainda a alusão a várias Recomendações, entre as quais, a Recomendação N.º R(89)9, (já vertida na legislação nacional pela Lei 109/91, de 17 de Agosto), praticamente tida como uma das fontes da Convenção, apresentando-a como o passo seguinte, quase como o “next step”, a evolução natural e necessária de vária legislação de cariz europeu (comunitário). Em relação ao ordenamento jurídico português, não parece ser assim.

Por um lado, a Convenção, enquanto originada na vontade política do espaço europeu, extravasa os parceiros europeus ao englobar na sua feitura outros países, como os Estados Unidos da América do Norte e o Canadá, onde o sistema jurídico é diferente do europeu, claro, com excepção do Reino Unido.

Por outro lado e no tocante ao legislador português, este não adoptou a referida Recomendação R(89)9 na sua totalidade, tendo ficado apenas pela lista mínima daquela Recomendação, não nos parecendo ser agora a Convenção que supera ou que preenche o espaço daquela lista opcional de crimes. Finalmente, a própria Convenção parece assentar num aparente pressuposto de que já foi atingida harmonização legislativa mínima mas efectiva entre os Estados proponentes, nomeadamente em áreas como a da protecção de dados pessoais, da assistência judiciária mútua e da dos meios de obtenção da prova, relevando a menção expressa a um esforço concertado entre a ONU, o G8 e a própria União Europeia nos seus considerandos.

O que não está escrito mas que daqui se depreende implicitamente, é que politicamente se reconhece que no estado legislativo anterior à Convenção, o custo das falhas do aparelho repressivo nos vários ordenamentos jurídicos era insuportável. E porquê? Porque fundamentalmente a “cibercriminalidade” é um fenómeno criminal de