

O CASO “ECHELON”: ASPECTOS JURÍDICOS

1. Soberania e segurança no Ciberespaço

1.1. A evolução recente da Sociedade de Informação processa-se a partir do momento em que a Internet - inicialmente um ambiente de comunicação acessível a um grupo restrito de iniciados, pertencentes a centros de investigação universitária ou de empresas de telecomunicações - se democratizou e globalizou, convertendo-se numa fonte inesgotável de informações, num meio libérrimo de comunicação *multimédia*, num mercado de bens e serviços generalizadamente acessível a multidões de empresas e de potenciais clientes empresariais ou individuais. Longe vão os tempos das telecomunicações meramente bi-direccionais, em ambiente “fechado”, hoje ultrapassadas pelo ambiente “aberto” da comunicação no Ciberespaço.

Desde que esta abertura da Internet à globalidade das pessoas e dos países tornou o Ciberespaço um território franco, viabilizando e globalizando a Sociedade de Informação, começaram a posicionar-se perspectivas e atitudes contraditórias acerca de questões estruturais para a sua compreensão e para a definição de um quadro de princípios orientadores das condutas dos entes públicos e privados que nele interferem e participam.

Um primeiro plano de contraposição estabeleceu-se entre, duma parte, a corrente que tendeu a conceber o Ciberespaço como um “Admirável Mundo Novo”, isento de todos os constrangimentos da tradicional sociedade humana – entre eles os do Direito... -, em que todos poderiam intervir com irrestrita liberdade e que, deste modo, seria o terreno ideal para o desenvolvimento de potencialidades globais de inovação, de democratização, de crescimento económico; e, doutra parte, a linha de orientação que considera que o Ciberespaço não é mais do que um conjunto alargado e muito eficiente de meios de comunicação de informação entre pessoas e instituições, o que torna inevitável e imprescindível a sua sujeição a regras éticas e jurídicas, portanto a todo um conjunto de condicionamentos que apenas representarão o natural desenvolvimento e adaptação à nova realidade da envolvente deontológica de qualquer sociedade humana.

Pouco a pouco, como seria lógico prever – mas ainda suscita frequentes reacções de inconformismo ⁽¹⁾ - a formação de uma estrutura de princípios e normas tem vindo a ser preconizada e a verificar-se efectivamente, dando lugar a um Direito do Ciberespaço ainda um tanto informe, mas já visível: seja pela transposição de princípios e normas dos ramos homólogos do Direito, formados para as manifestações e ambientes da vida das sociedades humanas a que poderemos, por antítese, chamar “tradicional”, seja pela criação de novos e específicos instrumentos e formulações normativas, quer baseados na mesma tipologia dos “tradicional”, quer eles mesmos gerados em ambiente e modelagem própria ⁽²⁾.

Deste modo, tem vindo a prevalecer a tendência a que podemos chamar *ordenadora* e, cada vez mais, *reguladora* da Internet e, com ela e para além dela própria, da Sociedade da Informação.

1.2. Todavia, um segundo nível de problemática se nos depara, podendo resumir-se a uma pergunta bem simples e directa: Quem manda na Internet ? Um só – que seria os Estados Unidos da América, como durante muito tempo se admitiu, *de facto*, que não certamente *de jure* - ; ou muitos, em plúrimas esferas de soberania e autonomia, públicos e privados, segundo um padrão de repartição do poder assimilável ao das estruturas sociais tradicionais?

Aparentemente, seria diversa a resposta, posto que mais parece que ninguém manda: o carácter fragmentário da Internet - “manta de retalhos de redes”, como lhe chamou LARS DAVIES⁽³⁾ -, a pluralidade de meios de comunicação (satélites, cabos, feixes hertzianos, etc.) de que ela se vale e forma, a variedade de utilidades ou meios de comunicação que proporciona (WWW, “e-mail”, “Usenet”, etc.), a proliferação - à escala de centenas de milhões - de “sites” e “homepages”, do lado dos fornecedores de informação, e de utilizadores, da banda oposta, - tudo isto parece colocar a capacidade de deter e comunicar nas mãos de toda a gente.

¹ Cfr. LAWRENCE LESSIG, *The Internet Under Siege*, in *Foreign Policy*, <http://www.foreignpolicy.com/issue_novdec_2001/lessig.htm>.

² Sobre o tema: DAVID G. POST, *Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace*, 1995 J.ONLINE L. art. 3, <<http://warthog.cc.wm.edu/law/publications/jol/post.zip>>; e YVES POULLET, *Quelques considérations sur le droit du cyberspace*, 1998

³ LARS J. DAVIES, *Contrat Formation on the Internet (Shattering a few myths)*, in *Law & the Internet*, Hart Publishing, Oxford, 1997.

Mas decerto não é bem assim. É pouco provável a concentração absoluta do poder, que daria origem a um possível fenómeno orwelliano⁽⁴⁾, em que uma só autoridade possuiria um monopólio virtual da informação. Certamente impossível, esta realidade será, porém, tendencialmente aproximável se um único poder ou federação de poderes detiver a possibilidade de submeter a observação e controlo todos os demais intervenientes. Cada "navegante" no Ciberespaço tende a guardar e/ou a disponibilizar e/ou a comunicar cada vez maiores quantidades e variedade de informação. Por isso mesmo, parece que cada vez mais a informação se torna disponível, em localizações e ambientes adequados para ser sujeita a controlo e observação.

Ao mesmo tempo – e porque o Poder vem, antes de mais, do Conhecimento dos factos -, a evolução tecnológica das comunicações criou meios adequados para desenvolver uma cada vez mais apurada e acrescida capacidade de *vigilância informática*. Sob este aspecto, como assinala IAN LLOYD ⁽⁵⁾, a Internet e em especial a WWW, embora muitas vezes exalçadas como um derradeiro refúgio do individualismo, podem realmente ser qualificadas como um *sistema excelente de vigilância*, já que todo o “navegante” da Net deixa traços electrónicos da sua passagem e todos os métodos de preservação da privacidade são cada vez mais postos em causa pelos legisladores, gestores dos meios de rede e prestadores de serviços.

1.3. Ao fim e ao cabo, fica sempre a pairar a questão angustiante: Há no Ciberespaço um “Big Brother” a olhar para cada um de nós, navegantes erráticos na NET, pesquisadores de informação na WWW, comunicadores ou receptores de correio electrónico, em que se exprimem e circulam tantas manifestações do nosso sentir, pensar e relacionar com os outros, livre e confiantemente expressas ?

Os factos que vou referir parecer justificar este temor.

⁴ Obviamente me refiro à visão da sociedade de pesadelo configurada por GEORGE ORWELL no seu célebre “1984”, ultrapassado na cronologia, mas não totalmente na lógica. Para uma interessante análise desta possibilidade, cfr. SIMON DAVIES, *Big Brother – Britain Web of Surveillance and the New Technological Concept*, Pan, 1996, bem como a recensão crítica de IAN LLOYD in *The Journal of Information, Law and Technology (JILT)*, (1996) 3, <<http://elj.warwick.ac.uk/elj/jilt/bookrev/3lloyd/>> . Vd. tb. o mesmo IAN J. LLOYD, “*Information Technology Law*”, Butterworths, London, Edinburgh, Dublin, 2ª ed. 1997, p. 30 e ss.

⁵ *Ibidem*.

2. O ECHELON⁽⁶⁾

2.1. No desenvolvimento da cooperação estabelecida entre os serviços secretos dos Estados Unidos e do Reino Unido durante a 2ª Guerra Mundial e tendo por objectivo prosseguirem as suas actividades conjuntas de "inteligência" (eufemismo que, como se sabe, significa: espionagem), estes países celebraram em 1947 uma convenção internacional de carácter secreto – conhecida como Acordo UKUSA –, à qual posteriormente aderiram o Canadá, a Nova Zelândia e a Austrália.

Findo o período da chamada “Guerra Fria” – durante a qual cada membro do Acordo UKUSA interceptava e analisava autonomamente as comunicações, com os seus próprios meios, comunicando-as depois aos demais -, foi sendo construído um poderoso e eficiente sistema integrado de interceptação de telecomunicações, projectado pela NSA - National Security Agency dos Estados Unidos, permitindo a cada um dos membros daquele Acordo ter acesso directo aos dados de informação recolhidos e tratados pelo Sistema.

Este Sistema, que recebeu o nome de código ECHELON⁽⁷⁾, comporta cerca de 120 satélites espíões e pelo menos 11 estações terrestres de satélites, bem como um número desconhecido de estações terrestres de interceptação de comunicações por cabos submarinos e por outros meios de telecomunicações terrestres.

Constitui uma rede electrónica de vigilância (ou, em linguagem mais crua: de espionagem) apta a interceptar as comunicações telefónicas, por fax e por correio electrónico, à escala mundial, e a torná-las disponíveis aos serviços de segurança dos países UKUSA⁽⁸⁾.

⁽⁶⁾ É já vasta a bibliografia sobre o tema. Fundamental é o “Relatório sobre a existência de um sistema global de interceptação de comunicações privadas e económicas (sistema de interceptação Echelon)”, Parlamento Europeu, Comissão Temporária sobre o Sistema de Interceptação ECHELON, Relator: Gerhard Schmid, Final, A5-0264/2001 (que adiante referiremos apenas como "Relatório do P.E."). Vd tb: NICKY HAGER, “*Exposing the Global Surveillance System*”, in <www.ncoic.com>; PATRICK S. POOLE, “*ECHELON: America's Secret Global Surveillance Network*”, e “*ECHELON: America's Spy in the Sky*”, ambos in <www.ncoic.com>; A. FAZIO e L. GUIDI, *Il Caso ECHELON*, in <<http://www.cli.di.unipi.it/~guidi/echelon/tesi.html>>; Vd. ainda a citada em <http://users.skynet.be/terrorism/html/nsa_echelon_htm>

⁽⁷⁾ “Echelon” significa *degrau, escalo*. Segundo A. FAZIO e L. GUIDI (ob. cit.), o uso deste nome de código refere-se provavelmente à estrutura escalar do Acordo UKUSA, em que a NSA é um primeiro degrau face às agências dos demais países membros.

⁽⁸⁾ PAUL WOLF, “*Echelon*”, in <<http://www.derechos.net/paulwolf/index.htm>>.

A sua concepção é basicamente simples: as estações dispostas através do Mundo interceptam o máximo possível de comunicações por satélite, micro-ondas, redes celulares e fibra óptica, sendo as informações assim captadas em seguida processadas pelos poderosíssimos computadores da NSA – os “dicionários” – que comportam os mais avançados meios de inteligência artificial, nomeadamente programas de reconhecimento de voz (*voice recognition*), reconhecimento óptico de caracteres (*optical character recognition* - OCR), busca de palavras ou frases de código e decifração de textos cifrados, Estes programas habilitam os "dicionários" a assinalar as mensagens ou documentos para gravação e transcrição para futura análise por especialistas, sendo posteriormente encaminhados aos serviços de investigação que pediram a respectiva interceptação. Deste modo, o Sistema permite recolher e analisar informações sobre qualquer assunto, seleccionadas por sujeitos, períodos de tempo, etc.

A partir desta nova fase, os objectivos inicialmente militares do Acordo foram superados por objectivos de carácter civil, em especial de investigação criminal, designadamente o combate ao terrorismo e à criminalidade organizada. Há, todavia, indicações bastante seguras de que o Sistema tem vindo a ser usado para outros fins, designadamente: de espionagem económica, recolhendo informações que são utilizados para favorecer os interesses de empresas dos países UKUSA na competição internacional face aos de outros Estados; e de espionagem política, interna ou internacional, relativamente a grupos políticos “impopulares” e a autoridades de países adversas.

2.2. Como destaca o citado Relatório do Parlamento Europeu (⁹), o ECHELON apresenta duas características muito específicas como sistema de informação: Primeira, a capacidade praticamente global de vigilância: os meios de captação de que dispõe e a sua localização permitem-lhe interceptar e aceder ao conteúdo de praticamente quaisquer comunicações electrónicas por meios públicos, à escala mundial. Segunda, a de resultar da cooperação dos diversos países UKUSA, o que lhe confere claras vantagens face aos sistemas puramente nacionais. Mas, como ali se assinala, a ameaça representada pelo ECHELON resulta sobretudo da ausência

(⁹) N° 1.6, pp. 24-25

de efectiva protecção legal para as pessoas e organizações que sejam alvo da espionagem através dele conduzida, por na maior parte dos casos se tratar de estrangeiros em relação aos Estados UKUSA e, sobretudo, dado o seu carácter secreto (apesar de a sua existência ser já hoje inquestionável e até ter sido reconhecida por entidades oficiais dos Estados UKUSA).

2.3. Não é possível referir num breve relato as múltiplas reacções individuais e de variadas organizações que a difusão pública da existência e características do ECHELON tem vindo a suscitar ao longo dos anos mais recentes. Uma simples busca na Internet evidencia a existência de milhares de referências, em páginas Web generalistas ou específicas sobre o tema, artigos de imprensa, estudos, manifestos, etc, etc.. Alguns (apenas) dos que se mostraram mais interessantes e informativos vão referidos em notas deste trabalho ⁽¹⁰⁾. Vários deles apresentam extensas bibliografias. A informação disponível é, pois, extensíssima. A primeira dificuldade para quem aborda o problema é, portanto, a de seleccionar a melhor dessa informação.

Bastará, pois, referir aquela que parece ser a mais profunda e conseguida dessas reacções: a do Parlamento Europeu (P.E.) ⁽¹¹⁾. Alertado por um estudo que encomendou em 1997 à Fundação Ómega, o STOA (Avaliação das Opções Científicas e Técnicas, serviço da Direcção-Geral de Estudos do P.E.), encomendou em 1999 um desenvolvido estudo sobre as tecnologias de vigilância e os riscos de abuso de informações económicas, cujo 2º volume, da autoria de Duncan Campbell, é dedicado o Sistema ECHELON.

Sobretudo as indicações desse estudo sobre o uso do ECHELON para fins de espionagem económica tiveram profundo eco, desencadeando debates em vários Parlamentos de Estados-Membros da UE e levando o P.E. a deliberar, em 5.6.2000, a constituição de uma comissão temporária sobre o Sistema ECHELON.

⁽¹⁰⁾ Uma menção especial ao documento intitulado "Memorandum" sobre "International Electronic Surveillance", datado de 7.6. 1999 e tendo por objectivo «encorajar os Comités de Reforma do Judiciário e do Governo a empreender uma investigação, incluindo audições públicas, sobre a ameaça à privacidade e às liberdades civis dos Americanos causada pelo envolvimento do Governo dos EUA em actividades de vigilância electrónica e internacional», subscrito pelas seguintes entidades: American Civil Liberties Union; Center for Democracy and Technology; Eagle Forum Electronic Frontier Foundation; Electronic Privacy Information Center; e Free Congress Foundation; in <www.cdt.org/>.

⁽¹¹⁾ A descrição aqui feita baseia-se nos dados referidos no Relatório do P.E.

Esta Comissão apresentou em 11.6.2001 o seu Relatório, tendo sido aprovada em sessão do P.E. de 5.9.2001 uma Resolução que basicamente adopta o projecto que for a apresentado pela mesma Comissão ⁽¹²⁾.

2.3. Convém notar que o ECHELON não constitui realidade única, nem no tocante a iniciativas da Administração dos EUA, nem mesmo quanto a outras de carácter público ou mesmo privado.

O FBI (Federal Bureau of Investigation) norte-americano dispõe de um sistema de vigilância da Internet, denominado *Carnivore*, instalado directamente nas redes dos "Internet Service Providers", que permite gravar todo o tráfego de *sites* visitados e dos *e-mails* recebidos e enviados por pessoas ou entidades suspeitas de envolvimento em práticas criminosas, podendo também reconstruir e adulterar *Webpages* e captar comunicações de voz via Internet. Em princípio, o sistema só capta comunicações com base em autorização judicial, sendo os seus objectivos a investigação criminal e a segurança nacional dos EUA ⁽¹³⁾

Existe também a possibilidade de que outros países - designadamente a França e a Rússia - desenvolvam actividades de vigilância e interceptação das comunicações à escala mundial, como adverte o Relatório do P.E., embora admitindo a insuficiência da informação disponível a tal respeito ⁽¹⁴⁾

Têm sido, por outro lado, denunciados numerosos casos de interceptação abusiva de comunicações por entidades privadas. A mais recente de que tive notícia foi a que vinha sendo levada a cabo pela Comcast Corp., empresa norte-americana que reconheceu que vinha colhendo elementos acerca dos acessos à Internet dos seus cerca de um milhão de clientes, designadamente dos endereços das páginas por eles contactadas. Embora a Comcast tenha alegado não pretender violar a privacidade dos clientes, o uso dessas informações não era claro e, por isso, quando foi confrontada com um pedido de explicações por parte de um deputado federal, a empresa informou que cessaria essa prática ⁽¹⁵⁾.

⁽¹²⁾ 2001/2098 (INI), in <<http://www3.europarl.eu.int/omk/omisapir.so/>>.

⁽¹³⁾ *Apud* "Telecomunicando - Newsletter de Comunicações", Vieira de Almeida & Associados, Outubro 2001.

⁽¹⁴⁾ Cap. 6, p. 79 e ss.

⁽¹⁵⁾ Vd. "EPIC Alert" vol. 9.03, 13.2.2002, in <http://www.epic.org/alert/EPIC_Alert_9.03.html>.

3. Problemas jurídicos do Echelon: Os valores e interesses em confronto

A importância emblemática do caso ECHELON resulta de ele nos colocar directamente no centro do confronto entre as exigências de segurança das comunidades - *maxime*, dos Estados - e os direitos e interesses fundamentais, sejam das Pessoas e de outros Estados.

Na realidade, embora alguma crítica mais apressada possa entrever no ECHELON apenas um exercício do Poder que a detenção e organização de meios tecnológicos avançados pode conferir a alguns Estados - liderados por um deles, não por acaso correspondente à mais poderosa Nação do Mundo... -, é de todo o ponto evidente que este Sistema de recolha de informação tem motivos e objectivos que correspondem a interesses e necessidades de governação em boa parte relevantes e por vezes mesmo justificáveis à luz de critérios de equilíbrio axiológico.

Primeiro, o ECHELON é apresentado como um Sistema avançado de colheita de informações sobre práticas criminosas, tornado indispensável pela multiplicação de organizações criminosas de escala internacional, o desenvolvimento dos meios poderosos e sofisticados com que operam e a gravidade das consequências da sua actuação. Redes de tráfico de armas e de droga, terrorismo internacional, contrabando, evasão fiscal de grande escala - são realidades indesmentíveis, cujos efeitos se fazem sentir em termos cada vez mais notoriamente demolidores nas sociedades humanas do nosso tempo. Combater essa criminalidade de "alto nível" de forma eficaz implica cada vez mais apostar na actuação preventiva, tendo em conta que ela resulta da colaboração de múltiplas organizações criminosas, ou de organizações pluri-localizadas, cujas actuações se baseiam em recurso intensivo a avançados meios de comunicações. O ECHELON permite vigiar e fazer a detecção e triagem das comunicações dessas organizações, fornecendo aos serviços de investigação criminal as informações de que carecem, a tempo de permitir intervenções eficazes que impeçam a produção dos efeitos mais gravosos dessas actividades ilícitas e a captura dos agentes criminosos e respectivos meios.

Segundo: O ECHELON surgiu e continua a funcionar como um Sistema de recolha de informações militares e políticas, tendo em vista a defesa da segurança

interna e externa dos Estados UKUSA. Trata-se de uma realidade e prática dos Estados em geral: todos o fazem, mais ou menos, melhor ou pior. E tal prática correspondente a interesses sérios de segurança colectiva face a ameaças de desagregação ou de destruição, não sendo de estranhar que os Estados UKUSA usem dos meios tecnológicos avançados e estabeleçam cooperação entre eles para colherem, tratarem e usarem essas informações.

Terceiro: O ECHELON terá sido usado como fonte de informações de carácter económico, de interesse para empresas estabelecidas nos Estados UKUSA, de modo a favorecê-las em confronto com suas congéneres de outros países. Evidentemente, este uso não é confessado pelas organizações de segurança dos Estados UKUSA. Mas o que mais importa é a evidente possibilidade dessa ocorrência e a detecção das suas repercussões jurídicas.

Face a estas necessidades e interesses, que justificam ou explicam a existência e utilização do Sistema ECHELON, posicionam-se, porém, valores e interesses muito significativos e relevantes, quer por fazerem parte do núcleo essencial dos *direitos humanos individuais* que alicerçam estruturalmente as comunidades humanas democráticas, quer por dizerem respeito a valores básicos de convivência entre Estados, consagrados no Direito Internacional.

Irei, assim, equacionar neste caso emblemático, os seguintes grupos de problemas jurídicos:

- Os referentes ao confronto dos direitos das Pessoas com os interesses do Estado ou Estados;
- Os inerentes ao apoio do Estado a empresas nacionais em detrimento das empresas de outros Estados.

Outros temas de carácter jurídico poderiam decerto apresentar-se - nomeadamente os de direito internacional resultantes de confronto de interesses dos Estados face às actividades de espionagem militar, política ou económica conduzidas por outros Estados. Não irei aqui abordá-los por falta de requisitos básicos: tempo e conhecimento.

3.3.O direito fundamental à intimidade pessoal

3.1.1. No primeiro conjunto de problemas irei tecer algumas linhas de enquadramento dos aspectos jurídicos resultantes do choque dos interesses acima apontados como subjacentes ao ECHELON, com a defesa dos direitos pessoais, designadamente o da intimidade (ou privacidade) pessoal.

O tema tem implicações muito variadas, que acabam todas, mais ou menos directamente, por nos conduzir à indagação do suporte axiológico das relações na Sociedade de Informação, ou seja, de como salvaguardar os valores que devem nortear nesse contexto a convivialidade das pessoas e das instituições, tendo como essencial preocupação a salvaguarda da dignidade humana.

Usando como ponto de partida as indagações de RICHARD O. MASON no quadro das questões éticas atinentes à Sociedade de Informação ⁽¹⁶⁾, a questão da *privacidade* pode sintetizar-se assim:

«Que informação acerca de si próprio ou das suas relações deve uma pessoa relevar a outros, sob que condições e com que salvaguardas? Que coisas podem as pessoas conservar para si mesmas e não ser forçadas a revelar a outras?»

Sob esse prisma, em tema de informação e comunicação, ocorre de imediato a necessidade de preservar o *direito à reserva da intimidade da vida privada* ⁽¹⁷⁾, que ÁLVARO D'ORS radica no próprio Direito Natural ⁽¹⁸⁾.

Na verdade, é *vox communis* a consagração superlativa deste direito dentro do núcleo mais inquestionável dos direitos fundamentais, tanto a nível internacional, como ao das leis fundamentais da maioria dos Estados civilizados: é o que sucede com o art. 12º da Declaração Universal dos Direitos do Homem ⁽¹⁹⁾, com o art. 17º do Pacto Internacional sobre os Direitos Civis e políticos ⁽²⁰⁾, com o art. 8º da

⁽¹⁶⁾ "Four Ethical Issues of the Information Age", in "Management Information Systems Quarterly", (10:1) March, 1986.

⁽¹⁷⁾ Terminologia que prefiro por corresponder à consagrada, com manifesta conotação personalista, na nossa Constituição e no nosso Código Civil). Isto sem deixar de ter em conta o cada vez mais frequente emprego, por influxo anglo-saxónico, do termo *privacidade* ("privacy").

⁽¹⁸⁾ "Derecho y sentido común", Civitas Ediciones, Madrid, 1999, p. 136.

⁽¹⁹⁾ «Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito à protecção da lei.»

⁽²⁰⁾ Praticamente idêntico ao art. 12º da Declaração Universal dos Direitos do Homem.

Convenção Europeia dos Direitos do Homem ⁽²¹⁾, com o art. 7º da Carta dos Direitos Fundamentais da União Europeia ⁽²²⁾.

O nosso País enfileira nessa corrente, consagrando-o como direito fundamental de carácter pessoal (art. 26º, nº 1 da CRP), corroborado pela sua inclusão na categoria civilística dos direitos da personalidade (art. 80º do Cód. Civil), para além de consagrar diversos outros direitos que podem considerar-se a justo título como corolários ou garantes daquele.

Como bem ressaltam GOMES CANOTILHO – VITAL MOREIRA ⁽²³⁾, trata-se de um dos direitos que estão «directamente ao serviço da protecção da esfera nuclear das pessoas e da sua vida», integrante da mesma categoria específica do direito à vida e à integridade pessoal.

É evidente a dificuldade de determinar de modo geral o alcance da intimidade ou privacidade da informação referente a uma pessoa, atendendo a que cada qual tem necessidades pessoais e conseqüentemente percepções próprias acerca do âmbito que pretende preservar do alcance dos outros. Mas é comum a opinião de que há certos factos e, conseqüentemente, certos dados que, em homenagem à protecção da intimidade pessoal, devem formar uma «esfera privada de cada pessoa» a ser preservada da intromissão, seja das outras pessoas, seja dos poderes política ou juridicamente constituídos, que os mesmos Autores propõem sejam subordinados ao critério da *privacidade* e da *dignidade humana* ⁽²⁴⁾.

⁽²¹⁾ «1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.

2. Não pode haver ingerência de autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros.»

⁽²²⁾ “Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações”.

⁽²³⁾ “Constituição da República Portuguesa Anotada”, 3ª ed. 1993, p. 179.

⁽²⁴⁾ *Ibidem*, p. 182. Vd. tb. sobre este tema PAULO MOTA PINTO, “O Direito à reserva sobre a intimidade da vida privada”, Bol. Fac. Dir. Univ. Coimbra, nº 69, p. 526 e ss, *apud* GARCIA MARQUES - LOURENÇO MARTINS, “Direito da Informática”, IJC e Almedina, Coimbra, 2000, p. 104 ss.; MARIA EDUARDA GONÇALVES, “Direito da Informação”, Almedina, Coimbra, 1994, p. 74 ss.; FRANCISCO EUGENIO DIAZ, “La Protección de la Intimidad y el uso de Internet”, in “Informática y Derecho - Revista Iberoamericana de Derecho Informático”, nºs 30-31-32, Mérida, 1999, p. 149 e ss.

3.1.2. A protecção do direito à intimidade pessoal no tocante às realidades características da Sociedade de Informação apresenta múltiplas cambiantes, que dão origem a variados problemas e a profusa produção normativa.

É particularmente relevante, neste domínio, a clássica detecção neste direito fundamental de duas vertentes ⁽²⁵⁾ que originam normativos legais de cariz diferenciado:

- a) O «direito de impedir o acesso de estranhos a informações sobre a vida privada e familiar»; e
- b) O «direito a que ninguém divulgue as informações que tenha sobre a vida privada e familiar de outrém»

Estas duas vertentes manifestam-se de forma específica no direito (instrumental do direito à intimidade, mas nem por isso secundarizável) ao *sigilo das comunicações*, que o nosso ordenamento jurídico consagra de maneira enfática no art. 34º, nº 1 da CRP, ao declarar *invioláveis* «...o sigilo da correspondência e dos outros meios de comunicação privada...», acrescentando o nº 4 do mesmo artigo: «É proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de procedimento criminal.» ⁽²⁶⁾.

Este direito comporta as duas vertentes atrás assinaladas, ou seja, tanto a proibição do acesso não autorizado de terceiros ao conteúdo das comunicações – a por vezes chamada *vigilância* ou *intercepção* das comunicações - como a da divulgação e

⁽²⁵⁾ A que GOMES CANOTILHO – VITAL MOREIRA (obra cit., p. 181) chamam “direitos menores”, qualificação de que discordo, por me parecer que se trata antes de duas variações ou modalidades do direito à intimidade, que devem compartilhar o mesmo nível e força de dignidade e protecção constitucional que lhe está atribuída.

⁽²⁶⁾ Coerentemente, os operadores de serviços de telecomunicações de uso público são obrigados a «providenciar, no que for necessário e estiver ao seu alcance, no sentido de assegurar e fazer respeitar, nos termos da legislação em vigor, o sigilo das comunicações do serviço prestado...» (art. 4º, nº 2, al. e), do Regulamento de Exploração dos Serviços de Telecomunicações de Uso Público, aprovado pelo Decreto-Lei nº 290-B/99, de 30 de Julho); e os operadores do serviço fixo de telefone são igualmente obrigados «...a tomar as providências necessárias para assegurar o sigilo das comunicações efectuadas através do acesso ao SFT...” (art. 6º, nº 1, do Regulamento de Exploração do Serviço Fixo de Telefone, aprovado pelo Decreto-Lei nº 474/99, de 8 de Novembro). No mesmo sentido vd. tb. o art. 5º da Lei nº 68/98, de 28 de Outubro, que regula o tratamento de dados pessoais e a protecção da privacidade no sector das telecomunicações, transpondo para a ordem interna a Directiva nº 97/66/CE, de 15.12.1997. A efectividade da tutela jurídica deste direito resulta do art. 384º do Cód. Penal (Crime de violação de segredo de correspondência ou de telecomunicações). Sobre este último aspecto, vd. FARIA COSTA, “Direito Penal da Comunicação”, Coimbra Editora, Coimbra, 1998, pp. 63 e ss., e 143 e ss.

utilização por terceiros desse conteúdo e das circunstâncias (tais como a hora, a duração, os endereços, etc.) das comunicações estabelecidas⁽²⁷⁾.

Mais voltado para a segunda vertente – proibição de divulgação de dados pessoais reservados - é o chamado *princípio da liberdade informática*, «ou seja, o direito de controlar (conhecer, corrigir, retirar ou agregar) os dados pessoais inscritos num programa electrónico» - para usar a definição de A.-H. PEREZ-LUÑO ⁽²⁸⁾ -, a que corresponde a construção da doutrina alemã da *autodeterminação informática*, concebida como direito de cada pessoa à informação, ao acesso, e ao controlo dos dados que lhe digam respeito ⁽²⁹⁾, com a sua derivação processual designada por "*habeas data*"⁽³⁰⁾.

Esta linha temática dá lugar ao ordenamento da *protecção de dados pessoais*, entre nós actualmente regulada em dois diplomas fundamentais: a Lei nº 67/98, de 26 de Outubro (Lei da Protecção de Dados Pessoais), que transpôs para a ordem interna a Directiva nº 95/46/CE, de 24.10.1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados; e a Lei nº 68/98, de 28 de Outubro, que regula o tratamento de dados pessoais e a protecção da privacidade no sector das telecomunicações, transpondo para a ordem interna a Directiva 97/66/CE, de 15.12.1997. Vale referir também a Convenção do Conselho da Europa para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal (aprovada pela Resolução da Assembleia da República n.º 23/93) ⁽³¹⁾.

3.1.3. Não obstante a importância dos direitos fundamentais – bem patente na variedade e fontes dos instrumentos de direito internacional que os consagram – é preocupante constatar que a comunidade internacional é pobre de meios adequados para assegurar a efectividade dos direitos fundamentais da Pessoa.

⁽²⁷⁾ Cfr. GOMES CANOTILHO-VITAL MOREIRA, obra cit., p. 213; e PEDRO GONÇALVES "Direito das Telecomunicações", IJC e Almedina, Coimbra, 1999, p. 190.

⁽²⁸⁾ "Manual de Informática y Derecho", Ariel Derecho, Barcelona, 1996, p.43,

⁽²⁹⁾ *Idem, ibidem*, p. 44. Vd. tb. AGOSTINHO EIRAS, "Segredo de Justiça e Controlo de Dados Pessoais Informatizados", Coimbra Editora, Coimbra, Col. Argumentum/4, 1992, pp. 9 e 65 e ss. e doutrina aí citada.

⁽³⁰⁾ PEREZ LUÑO, obra cit. p. 44.

⁽³¹⁾ Sobre o tema, vd. GARCIA MARQUES - LOURENÇO MARTINS, obra cit. pp. 75 e ss.; IAN WALDEN, "Data Protection", in CHRIS REED, "Computer Law", Blackstone Press Ltd., London, 3ª ed. 1996, p. 329 e ss.

É sintomático que os EUA – tantas vezes auto-proclamados campeões da causa dos Direitos Humanos... - não tenham até agora subscrito o Protocolo Adicional ⁽³²⁾ que alargou os poderes da Comissão dos Direitos do Homem, de modo a permitir-lhe acolher queixas individuais por violações do Pacto Internacional sobre os Direitos Civis e Políticos.

Como constatou o Relatório do P.E. ⁽³³⁾, só a Convenção Europeia dos Direitos do Homem (CEDH) - ratificada por todos os Estados-membros da União Europeia, que também acataram a jurisdição do Tribunal Europeu dos Direitos do Homem (TEDH) – permite tornar eficaz a nível internacional a protecção do direito à intimidade da vida privada, devido à competência daquele Tribunal para condenar os Estados signatários da CEDH por violações dos direitos humanos, inclusivamente ao pagamento de indemnizações.

Importa notar que o nº 2 do art. 8º da CEDH procura estabelecer um equilíbrio entre a salvaguarda do direito fundamental de que aqui cuidamos com os interesses públicos que podem entrar em colisão com ele. Ressaltam nesta norma pressupostos restritivos das ingerências das autoridades públicas, que se devem notoriamente ter em conta a respeito da intercepção das telecomunicações:

- a) *Legalidade*, ou seja, a vigilância só poderá ter lugar quando prevista em lei;
- b) *Democraticidade*, já que os motivos invocados como justificativos têm de conformar-se com os princípios que devem reger uma sociedade democrática;
- c) *Proporcionalidade*, isto é, a necessidade da devassa para a prossecução de determinados fins de interesse público: segurança nacional, segurança pública, bem-estar económico do país, defesa da ordem, prevenção das infracções penais, protecção da saúde ou da moral, protecção dos direitos e das liberdades de terceiros.

A jurisprudência do TEDH citada pelo Relatório do P.E. ⁽³⁴⁾ mostra uma orientação para a busca de equilíbrio que leva a combater a utilização de uma

⁽³²⁾ Adoptado pela Assembleia Geral das Nações Unidas em 19.12.1966.

⁽³³⁾ p. 87/88.

⁽³⁴⁾ Idem, p. 90.

metodologia de interceptação massiva e indiscriminada de telecomunicações, mesmo sob a invocação do objectivo da segurança nacional ou do combate à criminalidade organizada, ou outro dos previstos no n.º 2 do art. 8.º da CEDH. A esse respeito, o TEDH já decidiu que:

- As circunstâncias e condições em que uma autoridade pode interferir na vida privada devem ser consignadas em lei;
- A protecção da segurança nacional apenas se justifica na medida em que for necessária numa sociedade democrática, comportando o risco de a inviabilizar ou destruir sob o pretexto de a defender, pelo que só é compatível com os direitos fundamentais caso o Estado em questão tenha previsto adequados sistemas de controlo e garantias contra abusos ⁽³⁵⁾.

Por outro lado, a jurisprudência do TEDH tem interpretado o conceito de *correspondência* constante do art. 8.º, n.º 1, da CEDH no sentido de abranger todos os tipos de comunicações, incluindo as telecomunicações, pensamento que já se reflecte no art. 7.º da Carta dos Direitos Fundamentais da U.E.

A esta luz, importa ressaltar que a CEDH consagra a protecção dos direitos humanos independentemente da nacionalidade e da localização ou residência das pessoas, bastando que a um Estado signatário da Convenção seja imputada a violação de um desses direitos. A questão assume particular relevância no tocante à interceptação de telecomunicações, na medida em que tal circunstância permite responsabilizar qualquer Estado signatário mesmo que as pessoas visadas sejam estrangeiras ou que os meios de vigilância por ele usados se situem fora do seu território ou mesmo fora da Europa.

Nesta perspectiva, como ressalta o Relatório do P.E. ⁽³⁶⁾, não deve ser admitido o recurso por autoridades de Estados signatários da CEDH à colaboração de autoridades homólogas de Estados não-signatários – seja no território daquele, seja no destes –, designadamente como pretexto para se furtarem ao cumprimento das regras da Convenção, o que constituiria conduta de má fé e violação de tais regras. Deste modo, a colaboração com, p. ex., serviços de informação de outros Estados não-

⁽³⁵⁾ Idem, p. 90.

⁽³⁶⁾ Idem, p. 91.

signatários só deve entender-se admissível se uns e outros satisfizerem os requisitos do art. 8º, nº 2, da CEDH.

O caso ECHELON parece configurar precisamente este tipo de situação, já que a comunidade UKUSA comporta países signatários da CEDH e outros que o não são. Daí a necessidade, para salvaguarda da aplicação da CEDH, de que os Estados signatários não consintam a actuação nos seus territórios, ou com uso de meios neles instalados, de autoridades – *maxime*, serviços de informação – de outros Estados não-signatários, nem com estas colaborem, a não ser na medida em que lhes imponham o respeito pelas regras da Convenção.

É de notar, a este respeito, que a NSA apenas está sujeita a controlos das autoridades dos EUA, país não-signatário da CEDH. E é preocupante constatar que a fundamentação legal da actuação da NSA e outras agências de segurança e inteligência dos EUA apenas as sujeita a limites referentes à protecção dos direitos humanos de cidadãos norte-americanos⁽³⁷⁾, omitindo os dos cidadãos doutros países.

Assim, embora a ordem jurídica dos EUA - a partir da 4ª Emenda à Constituição, secundada pelo *Privacy Act* de 1974, pelo *Privacy Protection Act* de 1980 e pelo *Electronic Communications Privacy Act* de 1986, entre outros diplomas⁽³⁸⁾ – consagre um conjunto de consistentes garantias dos direitos humanos, aquela interpretação restritiva, adicionada a uma sinuosa legislação especial para a actividade dos serviços de informação, conduzem a abrir brechas consideráveis nessas garantias.

É esclarecedor o relatório “*Legal Standards for the Intelligence Community in Conducting Electronic Surveillance*”⁽³⁹⁾, elaborado pela NSA, o qual revela que a garantia consagrada pela 4ª Emenda para os direitos individuais é regulada, nesta matéria, pelo *Foreign Intelligence Surveillance Act* e pela “Executive Order” 12333, que disciplinam o respeito pelos direitos dos cidadãos norte-americanos, sujeitando, designadamente, a vigilância electrónica destes à obtenção de uma ordem judicial. Se o cidadão norte-americano estiver no estrangeiro, porém, a ordem é solicitada ao “Attorney General” (equivalente norte-americano do nosso Ministro da Justiça),

⁽³⁷⁾ Idem, p. 90.

⁽³⁸⁾ Cfr. para uma descrição da substância destes diplomas, JONATHAN ROSENBERG, “*Cyberlaw - the law of Internet*”, Springer-Verlag, New York, 1996, p.130ss; e OLIVIER HANCE, “*Business et Droit d’Internet*”, McGraw-Hill, 1996, p. 111.

⁽³⁹⁾ Dirigido, por imposição legal, ao Congresso dos Estados Unidos em Fevereiro de 2000, que descreve em termos estritamente técnico-jurídicos as bases legais da actuação dos serviços de informação daquele País (Vd. in <www.fas.org/irp/nsa/standards.html>).

passando assim para a esfera puramente administrativa. Mas – sintomaticamente... - nada consta acerca da vigilância dirigida a pessoas ou organizações que não sejam cidadãos norte-americanos.

E a questão ganha contornos ainda mais preocupantes se se tiver em conta que as ordens judiciais de vigilância e busca física requeridas pelas agências de informação e segurança norte-americanas são solicitadas a um tribunal especial e secreto, o “Foreign Intelligence Surveillance Court” (FISC), criado pelo FISA e que, segundo PATRICK S. POOLE, em 20 anos de actividade terá recebido mais de 10.000 pedidos de autorização para vigilância e buscas e não indeferiu nenhum ...⁽⁴⁰⁾

3.1.4. A resposta do Direito do Ciberespaço a estas ameaças apenas começa a esboçar-se. Não certamente na criação de meios efectivos de controlo de um ECHELON ou sistemas análogos, mas sim, para já, na afirmação de novos direitos que permitam reforçar a salvaguarda dos interesses individuais face aos novos “Big Brothers”.

Em texto recente ⁽⁴¹⁾, YVES POULLET apresenta quatro novos direitos cuja consagração e tutela parecem impor-se no novo contexto da Internet:

- a) O *direito ao anonimato* no uso dos novos serviços disponibilizados pelas tecnologias de informação, já sustentado em várias manifestações e instâncias, das quais destacamos:
 - (i) A recomendação nº R (99) 5 do comité dos ministros do Conselho da Europa, afirmou que «o acesso e a utilização anónimos dos serviços e dos pagamentos constituem a melhor protecção da vida privada»;
 - (ii) A Directiva nº 1999/93/CE, relativa a um quadro comum para as assinaturas electrónicas, que permite o uso de pseudónimo do titular de um certificado de assinatura electrónica;

⁽⁴⁰⁾ Cfr. PATRICK S. POOLE, “*Inside America’s Secret Court: Ythe Foreign Intelligence Surveillance Court*”, in <<http://www.digits.com>>.

⁽⁴¹⁾ “*Internet et Vie Privée: Entre Risques et Espoirs*”, in *Journal des Tribunaux*”, 2001, p. 155 e ss. Deste artigo colhemos as referências enunciadas neste ponto deste trabalho.

- (iii) Enfim, a proposta de Directiva sobre o tratamento de dados pessoais e protecção da vida privada no sector das comunicações electrónicas permite aos utilizadores recusar, ou até bloquear temporariamente o tratamento de dados de localização (“cookies”), sem prejuízo da possibilidade de os Estados-membros poderem limitar este direito na medida necessária para salvaguardar a segurança do Estado, a defesa, a segurança pública, a prevenção e investigação criminais e a utilização não-autorizada do sistema de comunicações electrónicas.
- b) O *princípio da reciprocidade de vantagens*, segundo o qual, na medida em que a Internet faculta aos prestadores de serviços de comunicações electrónicas a recolha e tratamento de dados, deve ser facultado por aqueles ao utilizador dos serviços valer-se do mesmo meios para exercer mais facilmente os seus direitos, p. ex., no tocante: a exercer “on line”, mediante um simples “click” os seus direitos de consentimento ou de oposição; a conhecer os dados pessoais que lhe respeitem e estejam registados, a sua origem, a lógica do seu processamento, etc., a dispor de meios expeditos de regulação de conflitos sobre os serviços da sociedade de informação (como já prevêm o art. 7º da Directiva nº 2000/31/CE, de 8.6.2000 - conhecida como “Directiva sobre o Comércio Electrónico” e o acordo UE - EUA acerca dos “Safe Harbor principles” no tocante aos fluxos de dados da Europa para os Estados Unidos).
- c) O *direito a uma tecnologia “privacy compliant”*, isto é, a que a indústria informática tanto do “software” como do “hardware” desenvolva produtos que propiciem o cumprimento das regras das directivas sobre protecção de dados pessoais, princípio proclamado pelo “International Working Group on Data Protection in Telecommunications” (conhecido como “Grupo do Artigo 29”) na sua recomendação 1/99, de 23.2.1999. Como assinala Y. POULLET, fica aberta a questão de este princípio ser alargado em direcção ao direito ao desenvolvimento de “privacy enhancing technologies”, isto é, de meios informáticos que permitam melhorar o respeito pelos direitos dos utilizadores.

- d) O direito à privacidade enquanto direito do consumidor, designadamente quanto a práticas empresariais agressivas do tipo das comunicações comerciais não solicitadas (*spamming*). Medidas neste sentido estão em vias de ser consagradas no quadro da futura directiva relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas, que irá expandir as medidas ainda algo tímidas da anterior Directiva 97/66/CE, de 15.12.1997 ⁽⁴²⁾.

3.4. A espionagem económica

3.2.1. Começo por um artigo jornalístico colhido na Internet e datado de 29.6.2000:

«Em Março, James Woolsey, antigo Director da CIA, “deixou fugir o gato” quando admitiu que a América (EUA) furta segredos económicos usando “espionagem com comunicações e satélites de reconhecimento”. Também enfatizou que existia “ênfase acrescida” acerca de informação económica, justificada por as empresas terem uma “cultura nacional” de “suborno”. Foi ainda até ao ponto de acusar as empresas Europeias de serem as “principais autoras de ilícitos do ponto de vista de pagarem “subornos” nos principais contratos internacionais no mundo”.»

«Em Maio foram revelados documentos, principalmente cartas da CIA para o Congresso, comprovando um intenso esforço de colheita de informações com o desígnio de assegurar que as empresas Americanas ganhem contratos internacionais. Os documentos, todos publicados durante a Administração Clinton, parecem confirmar relatos de que o aparelho americano de vigilância electrónica estava envolvido em espionagem comercial.

Os documentos revelam a extensão do esforço de Washington para promover os negócios dos Estados Unidos, detalhando quão frequentemente

⁽⁴²⁾ Trata-se da quinta directiva do novo quadro regulamentar comunitário para as telecomunicações, a respeito da qual já existe Posição Comum aprovada pelo Conselho de Ministros, faltando apenas a

estes agiram perante provas de concorrência "desleal" por contratantes estrangeiros.

Em 1993 e 1994, foi largamente relatado que a "intelligence community" (comunidade de informações...) dos EUA ajudou empresas americanas a ganhar cerca de \$16.5bn (£10bn) em contratos internacionais, alertando os EUA que ministros de governos do Terceiro Mundo estavam "no bolso". Entre as empresas referidas como tendo beneficiado dessa vigilância contam-se a Raytheon, a Boeing e a Hughes Network Systems.»⁽⁴³⁾

A conferência de imprensa de 7.3.2000 em que James Woolsey terá proferido as frases acima citadas deixou rasto devido à franqueza com que o mesmo reconheceu que os EUA interceptam telecomunicações internacionais com o fim de obter informações de carácter económico, designadamente sobre actividades e interesses de empresas estrangeiras, em especial no domínio de concursos e contratos internacionais.

Não foi, note-se, a única vez em que responsáveis norte-americanos se manifestaram nesse sentido. O Relatório do P.E. apresenta múltiplas citações do mesmo jaez⁽⁴⁴⁾, para além de apresentar um vasto elenco de casos em que as agências de informação norte-americanas - nomeadamente a NSA, portanto com mais do que provável uso dos meios do Sistema ECHELON - terão recolhido informações de molde a permitir a empresas norte-americanas intervir com sucesso em negociações internacionais, entre outros casos.

Segundo a mesma fonte, o ECHELON revela-se particularmente útil para estas actividades de espionagem da concorrência, particularmente: quando dela são alvos empresas multinacionais que operam em várias regiões horárias, ocasionando transmissão de informações entre a Europa, a América e a Ásia; quando essas empresas multinacionais recorrem a video-conferências, por satélite ou por cabo

aprovação pelo Parlamento Europeu em 2ª leitura, o que se espera venha a ocorrer até ao final do 1º trimestre de 2002.

⁽⁴³⁾ RICHARD BARRY, "Echelon: The evidence", 29.6.2000, in ZDNet UK, News, <<http://news.zdnet.co.uk/story/0,,s2079850,00.html>>. A tradução é minha.

⁽⁴⁴⁾ Vd. o Cap. 10, "A protecção contra a espionagem económica", p. 103 e ss., em especial os quadros de pp. 107/111.

submarino; e quando os negociadores de contratos têm de estabelecer comunicações internacionais com a sede da empresa ⁽⁴⁵⁾.

Segundo uma interpretação dos factos que encontram eco no Relatório ⁽⁴⁶⁾, a partir de 1990, com o termo da chamada "Guerra Fria", a Administração Clinton desenvolveu uma estratégia que equiparou a "segurança económica" à "segurança nacional" e que passou a determinar as actividades das agências de informação e segurança dos EUA, nomeadamente a CIA e a NSA.

Sintomático é, também, o papel do "Advocacy Center" instituído em 1993 pela Administração Clinton no Ministério do Comércio dos EUA, o qual se vangloria de ter ajudado centenas de empresas norte-americanas a vencer concursos públicos em países estrangeiros ⁽⁴⁷⁾ e terá contado por vezes com o apoio de agentes da CIA.

É certo que a Administração norte-americana sistematicamente vem afirmando que as suas agências não efectuam espionagem económica activa, mas apenas procuram combater condutas de "unfair competition" de empresas de outros países. Mas tal pretexto tem sido desmentido pela realidade dos factos, que a própria estratégia oficial supracitada corrobora.

3.2.2. Estes factos suscitam uma problemática questão que envenena as relações do comércio internacional e afecta as próprias relações políticas entre os Estados.

No intuito de procurar construir uma ordem jurídica internacional que propicie a melhoria deste clima, foi adoptada em 1997 a Convenção da OCDE sobre a luta contra a corrupção de agentes públicos estrangeiros nas transacções comerciais internacionais, que entrou em vigor em 15.2.1999, tendo sido ratificada por todos os Estados-Membros da UE (à excepção da Irlanda) e pelos EUA ⁽⁴⁸⁾.

No âmbito do Conselho da Europa foram adoptadas em 1999: a Convenção de Direito Penal contra a Corrupção - assinadas por todos os Estados-Membros da UE (salvo a Espanha) e pelos EUA, mas apenas ratificada até agora pela Dinamarca -; e a

⁽⁴⁵⁾ Idem, nº 10.6, p. 106.

⁽⁴⁶⁾ Idem, pp. 113 e ss. Vd. tb. A. FAZIO e L. GUIDI, ob. cit..

⁽⁴⁷⁾ Relatório do P.E., nº 10.9.4., p. 118.

⁽⁴⁸⁾ Idem, p. 116-117.

Convenção de Direito Civil contra a Corrupção - assinadas por todos os Estados-Membros da UE (salvo a Espanha, a Holanda e Portugal).

A UE, por sua vez, adoptou uma Convenção contra a corrupção em que estejam implicados funcionários das Comunidades Europeias ou dos Estados-Membros, e também uma Acção Comum contra a corrupção no sector privado, com vista à punição da corrupção activa e passiva das empresas ⁽⁴⁹⁾

3.2.3. Um outro tipo de implicações jurídicas das actividades de intercepção de comunicações para fins de colheita de informações de carácter económico, para fins concorrenciais, reside na sua compatibilidade com o Direito Comunitário. O que tem evidente relevância no tema que me ocupa, em virtude de o Acordo UKUSA ter como parte um Estado-Membro da UE - o Reino Unido - e ter outros como associados - Alemanha e Dinamarca -.

Ora, como assinalou o Relatório do P.E. ⁽⁵⁰⁾, a realização de tais actividades pelos serviços de informação de um Estado-membro, bem como o fornecimento de meios para as empreender aos serviços de informação de um outro Estado, teria várias implicações de violação de regras comunitárias:

Por um lado, constituiria violação dos deveres que impendem sobre os Estados-Membros, à luz do art. 10º do Tratado CE, de se absterem de todas as medidas susceptíveis de pôr em perigo a realização dos objectivos do Tratado, já que afectaria a prossecução do princípio do mercado comum, na medida em que distorceria as condições de efectiva e leal concorrência entre as empresas beneficiadas e as lesadas pela indevida recolha e utilização de informações comerciais.

Por outro lado, caso tais actividades conduzissem a beneficiar empresas nacionais de um Estado-Membro, então estar-se-ia perante uma ajuda estatal falseadora da concorrência, favorecendo certas empresas, e como tal incompatível com o mercado comum e por isso proibida pelo art. 87º do Tratado CE.

Ainda por outro lado, uma tal conduta implicaria uma violação do dever, que incumbe aos Estados-Membros, de garantir a confidencialidade das comunicações, devendo «designadamente, ...proibir a escuta, a colocação de dispositivos de escuta, o

⁽⁴⁹⁾ Idem, p. 117.

armazenamento ou outro meios de interceptação ou vigilância de comunicações por terceiros, sem o consentimento dos utilizadores»; dever este que só comporta as restrições necessárias «para salvaguardar a segurança do Estado, a defesa, a segurança pública, a prevenção, investigação, detecção e repressão de infracções penais ou da utilização não autorizada do sistema de telecomunicações» - conforme estabelecem as disposições conjugadas dos arts. 5º, nº 1, e 14º, nº 1, da Directiva 97/66/CE, de 15.12.1997, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das telecomunicações ⁽⁵¹⁾. Não sendo a interceptação de comunicações para fins económicos consentida pelo citado art. 14º, nº 1, é obviamente proibida por força do art. 5º, nº 1.

4. À guisa de conclusão

Uma vez mais nos deparamos com o inevitável confronto do direito da Força com a força do Direito. Na fase histórica fundamental de construir um ordenamento jurídico para a Sociedade da Informação, imprescindível é afirmar os Valores e, mais ainda, consagrá-los de forma efectiva em normas e instrumentos de sua execução.

Uma vez mais, a tarefa fundamental nos cabe a nós, homens do Direito!

Lisboa, 2002-03-06

⁽⁵⁰⁾ Idem, p. 84.

⁽⁵¹⁾ A transposição destas normas para o direito interno português encontra-se basicamente: no art. 5º, nº 2, da Lei nº 69/98, de 28 de Outubro; e no art. 8º, conjugado com o art. 2º, al. f), da Lei nº 109/91, de 17 de Agosto - Lei da Criminalidade Informática - que pune o crime de *intercepção ilegítima*.