PARLAMENTO EUROPEU

1999 *2004*

Documento de sessão

FINAL
A5-0264/2001
PAR 1

11 de Julho de 2001

RELATÓRIO

sobre a existência de um sistema global de intercepção de comunicações privadas e económicas (sistema de intercepção "ECHELON") (2001/2098 (INI))

Parte 1: Proposta de resolução
Exposição de motivos

Comissão Temporária sobre o Sistema de Intercepção ECHELON

Relator: Gerhard Schmid

“Sed quis custodiet ipsos custodes.”

Juvenal (cerca de 60 a 130 d. C.), Sat. 6, 347

ÍNDICE

Página

PÁGINA REGULAMENTAR 12
PROPOSTA DE RESOLUÇÃO 13
EXPOSIÇÃO DE MOTIVOS 24
1. Introdução: 24
1.1. Motivo da constituição da comissão 24
1.2. As afirmações constantes dos estudos STOA sobre a existência de um sistema global de intercepção com o nome de código ECHELON 24
1.2.1. O primeiro relatório STOA de 1997 24
1.2.2. Os relatórios STOA de 1999 24
1.3. O mandato da comissão 25
1.4. Por que não uma comissão de inquérito? 25
1.5. Metodologia e plano de trabalho 26
1.6. Características atribuídas ao sistema ECHELON 26
2. Actividade dos serviços de informações externas 28
2.1. Introdução 28
2.2. Que é a espionagem? 28
2.3. Objectivos da espionagem 28
2.4. Métodos da espionagem 28
2.4.1. Recurso ao ser humano na espionagem 29
2.4.2. Exploração dos sinais electromagnéticos 29
2.5. Actividade de certos serviços de informações 30
3. Condições técnicas para a intercepção das telecomunicações 32
3.1. Possibilidade de intercepção dos diferentes meios de comunicação 32
3.2. Possibilidades de intercepção no local 32
3.3. Possibilidades de um sistema de intercepção que funciona à escala mundial 33
3.3.1. Acesso aos meios de comunicação 33
3.3.2. Possibilidades da análise automática das comunicações interceptadas: utilização de filtros 37
3.3.3. O exemplo do serviço de informações alemão 38
4. Técnica das comunicações por satélite 40
4.1. Importância dos satélites de comunicações 40
4.2. Funcionamento de uma ligação por satélite 41

4.2.1. Satélites geoestacionários 41
4.2.2. O percurso dos sinais de uma comunicação por satélite 41
4.2.3. Principais sistemas de comunicação por satélite existentes 42
4.2.4. Atribuição de frequências 46
4.2.5. Raios de acção dos satélites (footprints) 47
4.2.6. Dimensões das antenas necessárias para uma estação terrestre 48
4.3. Comunicação via satélite para fins militares 48
4.3.1. Generalidades 48
4.3.2. Frequências utilizadas para fins militares 49
4.3.3. Dimensão das estações de captação 49
4.3.4. Exemplos de satélites de comunicações militares 49
5. Prova indiciária da existência de, pelo menos, um sistema de intercepção global 48
5.1. Porquê uma prova indiciária? 48
5.1.1. Prova da actividade de intercepção por parte dos serviços de informações externas 50
5.1.2. Prova da existência de estações nas zonas geograficamente necessárias 51
5.1.3. Prova da existência de uma associação estreita entre os serviços de informações 51
5.2. Como se reconhece uma estação de intercepção de comunicações por satélite? 51
5.2.1. Critério 1: acessibilidade da instalação 51
5.2.2. Critério 2: tipo de antena 52
5.2.3. Critério 3: dimensões da antena 52
5.2.4. Critério 4: provas procedentes de fontes oficiais 53
5.3. Dados publicamente acessíveis sobre estações de intercepção conhecidas 53
5.3.1. Método 53
5.3.2. Análise exacta 53
5.3.3. Síntese dos resultados 61
5.4. O acordo UKUSA 62
5.4.1. A evolução histórica do acordo UKUSA 62
5.4.2. Provas da existência do Acordo 64
5.5. Avaliação de documentos americanos que deixaram de ser considerados confidenciais 66
5.5.1. Natureza dos documentos 66
5.5.2. Conteúdo dos documentos 66
5.5.3. Resumo 69
5.6. Informações divulgadas por autores especializados e jornalistas 70
5.6.1. Nicky Hager 70

5.6.2. Duncan Campbell 71
5.6.3. Jeff Richelson 72
5.6.4. James Bamford 73
5.6.5. Bo Elkjaer e Kenan Seeberg, ... 74
5.7. Declarações de antigos colaboradores dos serviços de informações 74
5.7.1. Margaret Newsham (ex-colaboradora da NSA) 74
5.7.2. Wayne Madsen (ex-colaborador da NSA) 74
5.7.3. Mike Frost (ex-colaborador dos serviços secretos canadianos) 75
5.7.4. Fred Stock (ex-colaborador do serviço secreto canadiano) 75
5.8. Informações de fontes governamentais 75
5.8.1. Estados Unidos da América 75
5.8.2. Reino Unido 76
5.8.3. Austrália 77
5.8.4. Nova Zelândia 77
5.8.5. Países Baixos 77
5.8.6. Itália 77
5.9. Perguntas ao Conselho e à Comissão 78
5.10. Relatórios parlamentares 79
5.10.1. Relatórios do Comité Permanente R, Comité de Controlo da Bélgica 79
5.10.2. Relatório da Comissão de Defesa Nacional da Assembleia Nacional Francesa 79
5.10.3. Relatório da Comissão parlamentar italiana dos serviços de informação e Segurança e de Defesa do Estado 80
6. Poderão existir outros sistemas de intercepção operantes a nível mundial? 81
6.1. Condições para a existência de um tal sistema 81
6.1.1. Condições técnicas e geográficas 81
6.1.2. Condições políticas e económicas 81
6.2. França 81
6.3. Rússia 82
6.4. Os outros Estados do G-8 e a China 83
7. Compatibilidade de um sistema de intercepção de comunicações do tipo "ECHELON" com o direito comunitário 84
7.1. Observações preliminares 84
7.2. Compatibilidade de um sistema de informações de segurança com o direito da União 84
7.2.1. Compatibilidade com o direito comunitário 84
7.2.2. Compatibilidade com outra legislação comunitária 85

7.3. Questão da compatibilidade em caso de utilização abusiva de um sistema de intercepção para fins de espionagem da concorrência 86
7.4. Conclusões 87
8. Compatibilidade da intercepção de comunicações por parte dos serviços de informações de segurança com o direito fundamental ao respeito pela vida privada 88
8.1. Intercepção das comunicações enquanto ingerência no direito fundamental ao respeito pela vida privada 88
8.2. A protecção da vida privada ao abrigo dos acordos internacionais 88
8.3. As disposições consagradas na Convenção Europeia dos Direitos do Homem (CEDH) 89
8.3.1. A importância da Convenção na UE 89
8.3.2. Âmbito territorial e pessoal da protecção consagrada na CEDH 90
8.3.3. Admissibilidade da vigilância das telecomunicações ao abrigo do artigo 8º da CEDH 90
8.3.4. A importância do artigo 8º da CEDH para as actividades dos serviços de informações 91
8.4. Obrigação de controlo das actividades desenvolvidas pelos serviços de informações estrangeiros 93
8.4.1. Inadmissibilidade da não-observância do disposto no artigo 8º da CEDH através do recurso de serviços de informações de segurança de outros países 93
8.4.2. Exercício tolerado de actividades por parte de serviços de informações não europeus no território de partes contratantes da CEDH: consequências 93
9. Beneficiam os cidadãos da UE de uma protecção adequada no tocante às actividades dos serviços de informações? 97
9.1. Protecção no tocante às actividades dos serviços de informações: uma função dos parlamentos nacionais 97
9.2. Poderes das autoridades nacionais em matéria de execução de medidas de vigilância 97
9.3. Controlo dos serviços de informações 98
9.4. Análise da situação para os cidadãos europeus 101
10. A protecção contra a espionagem económica 103
10.1. A economia como alvo da espionagem 103
10.1.1. Os objectivos da espionagem 103
10.1.2. Espionagem da concorrência 104
10.2. Prejuízos causados pela espionagem económica 104
10.3. Quem pratica a espionagem? 105
10.3.1. Trabalhadores da própria empresa (delitos de iniciados) 105

10.3.2. Empresas de espionagem privadas 106
10.3.3. Piratas informáticos 106
10.3.4. Serviços de informações 106
10.4. Como se processa a espionagem? 106
10.5. Espionagem económica praticada por Estados 107
10.5.1. Espionagem económica estratégica praticada por serviços de informações 107
10.5.2. Serviços de informações como agentes de espionagem da concorrência 107
10.6. Será o ECHELON adequado à espionagem industrial? 108
10.7. Casos divulgados 108
10.8. Protecção em relação à espionagem económica 114
10.8.1. Protecção jurídica 114
10.8.2. Outros obstáculos à espionagem económica 114
10.9. Os EUA e a economia após o termo da guerra fria 115
10.9.1. Repto para o Governo norte-americano: espionagem económica contra empresas norte-americanas 116
10.9.2. A atitude oficial do Governo dos EUA sobre a espionagem económica activa 117
10.9.3. Situação jurídica em caso de corrupção de agentes públicos 118
10.9.4. O papel do "Advocacy Center" na promoção das exportações dos EUA 120
10.10. A segurança das redes informáticas 122
10.10.1. A importância do presente capítulo 122
10.10.2. O risco da utilização das modernas tecnologias da informação na economia 122
10.10.3. Frequência dos ataques contra as redes 124
10.10.4. Agentes e métodos 124
10.10.5. Prática da pirataria informática a partir do exterior 125
10.11. A subavaliação dos riscos 125
10.11.1. A consciência dos riscos no sector económico 125
10.11.2. A consciência dos riscos no sector da investigação 125
10.11.3. A consciência do risco nas Instituições Europeias 126
11. Auto protecção através da criptografia 128
11.1. Objectivo e funcionamento da encriptação 128
11.1.1. Objectivo da encriptação 128
11.1.2. Funcionamento da encriptação 128
11.2. A segurança dos sistemas de encriptação 129
11.2.1. Aspectos gerais do conceito de segurança da encriptação 129
11.2.2. Segurança absoluta: o *one-time pad* 130

11.2.3. Segurança relativa segundo o estado actual da técnica 130
11.2.4. Normalização e limitação premeditada da segurança.....131
11.3. O problema da distribuição/transmissão segura das chaves.....132
11.3.1. A encriptação assimétrica: o processo da chave-pública.....132
11.3.2. A encriptação por chave-pública para os particulares.....133
11.3.3. Processos futuros.....133
11.4. Segurança dos produtos de encriptação.....134
11.5. A encriptação em conflito com os interesses do Estado.....134
11.5.1. Tentativas de limitação da encriptação.....134
11.5.2. Importância da encriptação segura para o comércio electrónico.....134
11.5.3. Problemas para as pessoas que viajam em negócios.....135
11.6. Questões práticas da encriptação.....135
12. Relações externas da UE e recolha de dados por parte dos serviços de informações 137
12.1. Introdução.....137
12.2. Possibilidades de cooperação no interior da UE 137
12.2.1 A actual cooperação.....137
12.2.2. Vantagens de uma política comum europeia no domínio da informação.....138
12.2.3. Conclusões.....138
12.3. Cooperação além União Europeia 139
12.4. Observações finais.....140
13. Conclusões e recomendações 141
13.1. Conclusões.....141
13.2. Recomendações 144

OPINIÃO MINORITÁRIA E ANEXOS PUBLICADOS EM DOCUMENTO SEPARADO, NA PARTE 2

PÁGINA REGULAMENTAR

Na sessão de 5 de Julho de 2000, o Parlamento Europeu decidiu, nos termos do nº 2 do artigo 150º do seu Regimento, constituir uma comissão temporária sobre o sistema de intercepção ECHELON e estabeleceu o respectivo mandato, como consta do Capítulo 1.1.3 da exposição de motivos. Na sua reunião constitutiva de 6 de Julho de 2000, a comissão temporária, no exercício do referido mandato, designou relator o Deputado Gerhard Schmid.

Nas suas reuniões de 29 de Maio, 20 de Junho e 3 de Julho de 2001, a comissão procedeu à apreciação do projecto de relatório.

Na última reunião, a comissão aprovou a proposta de resolução por 27 votos a favor, 5 votos contra e 2 abstenções.

Encontravam-se presentes no momento da votação: Carlos Coelho, presidente; Elly Plooij-van Gorsel, Neil MacCormick e Giuseppe Di Lello Finuoli, vice-presidentes; Gerhard Schmid, relator; Mary Elizabeth Banotti, Bastiaan Belder, Maria Berger, Charlotte Cederschiöld, Gérard Deprez, Giorgios Dimitrakopoulos, Robert Evans, Colette Flesch, Pernille Frahm, Anna Karamanou, Eva Klamt, Alain Krivine, Torben Lund, Erika Mann, Jean-Charles Marchiani, Hughes Martin, Patricia McKenna, William Francis Newton Dunn (em substituição de Jorge Salvador Hernández Mollar, nos termos do nº 2 do artigo 153º do Regimento), Reino Paasilinna, Bernd Posselt (em substituição de Hubert Pirker), Jacques Santkin (em substituição de Catherine Lalumière), Ilka Schröder, Gary Titley (em substituição de Ozan Ceyhun), Maurizio Turco, Gianni Vattimo, W.G. van Velzen, Christian von Bötticher, Jan Marinus Wiersma e Christos Zacharakis (em substituição de Enrico Ferri).

A opinião minoritária e os anexos são alvo de publicação separada (A5-0264/2001 – Parte 2).

O relatório foi entregue em 11 de Julho de 2001.

O prazo para a entrega de alterações ao presente relatório constará do projecto de ordem do dia do período de sessões em que for apreciado.

PROPOSTA DE RESOLUÇÃO

Resolução do Parlamento Europeu sobre a existência de um sistema global de intercepção de comunicações privadas e económicas (sistema de intercepção ECHELON) (2001/2098(INI))

O Parlamento Europeu,

– Tendo em conta a sua Decisão de 5 de Julho de 2000 relativa à constituição de uma comissão temporária sobre o sistema de intercepção "ECHELON"[1], bem como o mandato cometido à referida comissão,

– Tendo em conta o Tratado CE, que visa, *inter alia*, a realização de um mercado comum caracterizado por um elevado grau de competitividade,

– Tendo em conta os artigos 11º e 12º do Tratado da União Europeia, que sujeitam os Estados-Membros à obrigação de reforçarem e de desenvolverem a solidariedade política mútua,

– Tendo em conta o Tratado da União Europeia, em particular o nº 2 do seu artigo 6º, que estabelece o compromisso da UE de respeitar os direitos fundamentais, e o seu Título V, que estabelece disposições relativas à política externa e de segurança comum,

– Tendo em conta o artigo 12º da Declaração Universal dos Direitos do Homem,

– Tendo em conta a Carta dos Direitos Fundamentais da UE, cujo artigo 7º prevê o respeito da vida privada e familiar e consagra expressamente o direito ao respeito das comunicações e cujo artigo 8º prevê a protecção dos dados de carácter pessoal,

– Tendo em conta a Convenção Europeia dos Direitos do Homem, em particular o seu artigo 8º, que protege a vida privada e a confidencialidade da correspondência, e as numerosas convenções internacionais que estabelecem a protecção da vida privada,

– Tendo em conta os trabalhos realizados pela Comissão Temporária sobre o Sistema de Intercepção ECHELON, a qual levou a cabo inúmeras audições e reuniões com peritos de todo o género e, em particular, com responsáveis dos sectores público e privado em matéria de telecomunicações e, de protecção de dados, com pessoal dos serviços de informações, jornalistas e advogados peritos na matéria, deputados dos parlamentos nacionais dos Estados-Membros, etc.,

– Tendo em conta o nº 2 do artigo 150º do seu Regimento,

– Tendo em conta o relatório da Comissão Temporária sobre o Sistema de Intercepção ECHELON (A5-0264/2001),

[1] JO C 121 de 24.4.2001, p. 36

Relativamente à existência de um sistema global de intercepção de comunicações privadas e económicas (sistema de intercepção ECHELON))

A. Considerando não existirem já quaisquer dúvidas quanto à existência de um sistema global de intercepção de comunicações que opera graças à cooperação entre os EUA, o Reino Unido, o Canadá, a Austrália e a Nova Zelândia no âmbito do acordo UKUSA; que, com base nos indícios existentes e em inúmeras declarações coincidentes provenientes de vários círculos – inclusive de fontes americanas –, se pode admitir que o sistema ou partes do mesmo tiveram, pelo menos durante algum tempo, o nome de código "ECHELON",

B. Considerando que não podem agora existir quaisquer dúvidas de que o sistema visa, no mínimo, interceptar comunicações privadas e comerciais, mas não comunicações militares, embora a análise levada a efeito no relatório tenha revelado que as capacidades técnicas do sistema não são provavelmente tão poderosas como, em parte, o haviam suposto os meios de comunicação,

C. Considerando ser, por conseguinte, espantoso, e mesmo preocupante, que inúmeros responsáveis comunitários ouvidos pela Comissão Temporária, nomeadamente Comissários europeus, tenham declarado não ter conhecimento deste fenómeno,

Relativamente aos limites do sistema de intercepção

D. Considerando que o sistema de intercepção se baseia, em particular, na intercepção global de comunicações via satélite, embora, em zonas de elevada densidade de comunicações, só uma parte extremamente reduzida das mesmas seja efectuada por satélite; que, por isso, a maior parte das comunicações não pode ser interceptada por estações terrestres, mas sim unicamente através de ligações por cabo e de escuta via rádio, o que - tal como o demonstram as investigações efectuadas no âmbito do presente relatório - só é possível dentro de limites estritos; que o volume de efectivos necessário para a análise e a avaliação das comunicações interceptadas impõe outras limitações; que, por conseguinte, os Estados UKUSA só têm acesso a uma proporção muito reduzida das comunicações por cabo e por rádio e que só podem analisar e avaliar uma proporção ainda mais reduzida das mesmas; que, além disso, por muito vastos que sejam os meios disponíveis e as capacidades de intercepção das comunicações, o elevadíssimo número das mesmas torna impossível, na prática, o controlo exaustivo e pormenorizado de todas as comunicações,

Relativamente à eventual existência de outros sistemas de intercepção

E. Considerando que a intercepção de comunicações constitui um método de espionagem tradicional dos serviços de informações e que um sistema desta natureza também poderia ser explorado por outros países, desde que dispusessem dos necessários recursos financeiros, bem como das condições geográficas requeridas; que a França, graças aos seus territórios ultramarinos, é o único Estado-Membro da UE que reúne as condições geográficas e técnicas para operar de forma autónoma um sistema global de intercepção e que dispõe também da infra-estrutura técnica e organizativa para o fazer; que existem igualmente fortes indícios de que também a Rússia explora provavelmente um tal sistema,

Relativamente à compatibilidade com o direito da UE

F. Considerando que, no tocante à questão da compatibilidade de um sistema do tipo ECHELON com o direito da UE, há que proceder às seguintes distinção: se o sistema só for utilizado para fins de informação, não há qualquer violação do direito da UE, uma vez que as actividades dos serviços de segurança do Estado não são abrangidas pelo Tratado CE, mas sê-lo-iam pelo Título V do TUE (PESC), que, porém, actualmente não prevê disposições sobre a matéria, pelo que não se dispõe de critérios aplicáveis; se, em contrapartida, o sistema for abusivamente utilizado para fins de espionagem da concorrência, tal acção será contrária à obrigação de lealdade dos Estados-Membros e à concepção de um mercado comum assente na livre concorrência, razão pela qual um Estado-Membro que nele participe viola o direito da CE,

G. Considerando as declarações feitas pelo Conselho na sessão plenária de 30 de Março de 2000, segundo as quais o Conselho não pode aceitar a criação ou a existência de um sistema de intercepção das telecomunicações que não respeite as regras de Direito dos Estados-Membros e que viole os princípios fundamentais destinados a salvaguardar a dignidade humana,

Relativamente à compatibilidade com o direito fundamental ao respeito pela vida privada (Art. 8º CEDH)

H. Considerando que toda e qualquer intercepção de comunicações representa um atentado grave ao exercício do direito à vida privada; que o art. 8º da CEDH, que estatui o direito à protecção da vida privada, permite a ingerência no exercício desse direito apenas para garantir a segurança nacional, desde que aquela esteja prevista em disposições do direito nacional que sejam acessíveis a todos e estabeleçam as circunstâncias em que a autoridade pública a pode exercer; que, além disso, a ingerência deve ser proporcionada, pelo que deve ser feita uma ponderação dos interesses concorrentes, e que, em conformidade com a jurisprudência do TEDH, não é suficiente que a ingerência seja meramente útil ou desejável,

I. Considerando que um sistema de informações que interceptasse, de forma aleatória e permanente, todas as comunicações violaria o princípio da proporcionalidade e não seria compatível com a CEDH; que, do mesmo modo, se as disposições nos termos das quais é efectuado o controlo das comunicações não tivessem base jurídica, se não fossem acessíveis ao público ou se a sua formulação fosse de molde a não permitir prever as suas implicações para o indivíduo, ou ainda se essa intercepção não fosse proporcionada, tal constituiria uma violação da CEDH; que as disposições nos termos das quais os serviços de informações norte-americanos operam no estrangeiro são, na sua maioria, secretas, pelo que o respeito do princípio da proporcionalidade é, pelo menos, questionável e se observa provavelmente uma violação dos princípios da acessibilidade do direito e da previsibilidade dos seus efeitos, princípios esses estabelecidos pelo TEDH,

J. Considerando que os Estados-Membros não podem eximir-se aos compromissos que lhes são impostos pela CEDH, deixando operar no seu território os serviços de informações de outros Estados sujeitos a disposições legais menos rigorosas, uma vez que, de outro modo, o princípio da legalidade e as suas duas componentes - acessibilidade e previsibilidade - perderiam o seu efeito, e a jurisprudência do TEDH seria privada de substância,

K. Considerando que a conformidade das operações legais dos serviços de informações com os direitos fundamentais obriga ainda à existência de sistemas de controlo suficientes, a fim de contrabalançar os riscos inerentes a actividades secretas por parte da Administração; que o Tribunal Europeu dos Direitos do Homem salientou expressamente a importância de um sistema de controlo eficaz da actividade dos serviços de informações e que, por conseguinte, se afigura preocupante que alguns Estados-Membros não disponham de quaisquer órgãos de controlo parlamentar dos respectivos serviços secretos,

Relativamente à questão de saber se os cidadãos da UE estarão suficientemente protegidos contra os serviços de informações

L. Considerando que a protecção dos cidadãos da UE depende da situação jurídica observada em cada um dos Estados-Membros, mas que são consideráveis as diferenças registadas e que, em alguns casos, se verifica mesmo a ausência de órgãos de controlo parlamentares, pelo que dificilmente pode ser considerada suficiente a protecção verificada; que os cidadãos europeus têm um interesse particular em que os respectivos parlamentos nacionais sejam dotados de uma comissão de controlo específica, formalmente estruturada, que vigie e controle a actividade dos serviços de informações; que, todavia, mesmo onde existem tais órgãos de controlo, grande é a tentação de votar maior atenção às actividades internas dos serviços de informações do que às actividades externas, uma vez que, regra geral, os cidadãos nacionais apenas são visados no primeiro caso; que, se os serviços de informações fossem obrigados a notificar *a posteriori* um cidadão cujas comunicações tivessem sido interceptadas, por exemplo, decorridos cinco anos após essa intercepção, tal constituíria um incentivo à prática de intercepção proporcionada,

M. Considerando que, face à sua dimensão, não podem ser construídas no território de um país estações de recepção de comunicações por satélite sem o seu consentimento,

N. Considerando que, em caso de cooperação entre serviços de informações no âmbito da PESC ou da JAI, cumpre às instituições promover a criação de medidas adequadas, a fim de proteger os cidadãos europeus,

Relativamente à espionagem industrial

O. Considerando que constitui parte integrante das atribuições dos serviços de informações no estrangeiro a recolha de dados económicos, como sejam o desenvolvimento de sectores específicos, a evolução dos mercados das matérias-primas, a observância de embargos, o respeito das disposições relativas ao aprovisionamento de bens de utilização dual, etc., e que, por essa razão, as empresas que desenvolvem actividades nesses domínios são, frequentemente, vigiadas,

P. Considerando que os serviços de informações dos EUA não investigam apenas assuntos de interesse económico geral, mas interceptam também pormenorizadamente as comunicações entre empresas, sobretudo no quadro da adjudicação de contratos, justificando essa intercepção com o propósito de combater tentativas de corrupção; que, no caso de uma intercepção pormenorizada, existe o risco de as informações não serem utilizadas para a luta contra a corrupção, mas sim para a espionagem dos concorrentes, ainda que os EUA e o Reino Unido declarem que não o fazem; que, no entanto, o papel do 'Advocacy Center' do

Ministério do Comércio dos EUA continua a não estar cabalmente esclarecido e que foi cancelada uma reunião que havia sido agendada para esclarecer precisamente esta questão,

Q. Considerando que a OCDE adoptou, em 1997, uma Convenção sobre a luta contra a corrupção de agentes públicos, a qual prevê a punição, a nível internacional, da corrupção, pelo que, também por esse motivo, a prática de actos de corrupção não pode justificar a intercepção de comunicações;

R. Considerando que a situação se torna intolerável quando os serviços de informações se deixam instrumentalizar para efeitos de espionagem da concorrência, espionando empresas estrangeiras para lograr vantagens concorrenciais para empresas nacionais; que, embora se afirme com frequência que o sistema global de intercepção é utilizado para esse efeito, não existem, no entanto, provas factuais que o atestem,

S. Considerando que, durante a visita efectuada aos EUA pela Comissão Temporária sobre o Sistema de Intercepção ECHELON, fontes autorizadas confirmaram o relatório Brown do Congresso dos EUA, referindo que 5% das informações recolhidas a partir de fontes não declaradas são utilizadas para fins de espionagem económica; que as mesmas fontes calculam que essa actividade de controlo de informações poderia permitir à indústria norte-americana obter contratos num valor que pode atingir os 7 mil milhões de dólares;

T. Considerando que os dados comerciais sensíveis se encontram, fundamentalmente, no interior das empresas, pelo que a espionagem consiste, nomeadamente, na tentativa de obter informações através dos próprios funcionários ou de pessoas infiltradas e, cada vez mais, penetrando nas respectivas redes informáticas; que, apenas nos casos em que dados sensíveis são transmitidos para o exterior via cabo ou via rádio (satélite), é possível utilizar um sistema de vigilância das comunicações para fins de espionagem da concorrência e que tal se aplica sistematicamente aos três casos seguintes:
– a empresas que operam em três fusos horários, de tal modo que os resultados intercalares podem ser enviados da Europa para a América e, seguidamente, para a Ásia;
– a videoconferências de empresas multinacionais realizadas via satélite ou por cabo;
– a negociações de contratos importantes *in loco* (construção de infra-estruturas, infra-estruturas de telecomunicações, criação de novos sistemas de transporte, etc.) que requeiram contactos com a sede da empresa em causa,

U. Considerando que a sensibilização das pequenas e médias empresas para os riscos e as questões de segurança é muitas vezes insuficiente, e que aquelas não reconhecem os perigos da espionagem económica nem da intercepção de comunicações,

V. Considerando que nem sempre existe um sentido de segurança muito desenvolvido nas Instituições europeias (à excepção do Banco Central Europeu, da Direcção-Geral do Conselho para as Relações Externas, assim como da Direcção-Geral da Comissão para as Relações Externas), pelo que se torna necessário empreender acções neste domínio,

Relativamente às possibilidades de autoprotecção

W. Considerando que as empresas devem proteger todo o seu ambiente de trabalho, bem como todos os meios de comunicação que sirvam para transmitir informações sensíveis; que são em número suficiente os sistemas de encriptação seguros existentes a preços módicos no

mercado europeu; que também as pessoas singulares devem ser incentivadas à encriptação do respectivo correio electrónico, uma vez que um correio não criptado equivale a uma carta sem envelope; que, na Internet, se encontram sistemas relativamente conviviais, postos à disposição de todas as pessoas, por vezes mesmo gratuitamente,

Relativamente a uma cooperação entre os serviços de informações no interior da UE

X. Considerando que a UE chegou a acordo quanto à coordenação da recolha de informações pelos serviços de informações no âmbito do desenvolvimento de uma política de defesa e de segurança comum, embora prossiga a cooperação com outros parceiros nestes domínios,

Y. Considerando que o Conselho Europeu decidiu em Helsínquia, em Dezembro de 1999, desenvolver uma capacidade militar europeia mais eficaz, a fim de poder dar cumprimento a todas as missões estabelecidas em Petersberg no contexto da PESC; que o Conselho Europeu decidiu, além disso, que a União, a fim de concretizar este objectivo até 2003, deveria estar habilitada a destacar rapidamente forças militares compostas por 50.000 a 60.000 pessoas, tropas essas auto-suficientes e que disponham das necessárias capacidades de comando, controlo e informações secretas; que os primeiros passos rumo à criação de uma tal capacidade autónoma em matéria de informações já foram dados no quadro da UEO e do Comité permanente político e de segurança,

Z. Considerando que a cooperação entre os serviços de informações existentes na UE se afigura indispensável, uma vez que, por um lado, uma política de segurança comum que excluísse os serviços secretos seria absurda e que, por outro, tal comportaria inúmeras vantagens de ordem profissional, financeira e política; que tal seria, além disso, conforme à ideia de uma parceria assente na igualdade de direitos com os Estados Unidos e seria susceptível de reunir todos os Estados-Membros no seio de um sistema instituído na plena observância da Convenção dos Direitos do Homem; que o controlo correspondente por parte do Parlamento Europeu deverá, obviamente, nesse caso encontrar-se assegurado,

AA. Considerando que o Parlamento Europeu se propõe aplicar a regulamentação sobre o acesso do público aos documentos do Parlamento Europeu, do Conselho e da Comissão mediante a adaptação das disposições do seu Regimento respeitantes ao acesso a documentos sensíveis,

Relativamente à conclusão e à alteração de acordos internacionais sobre a protecção dos cidadãos e empresas

1. Afirma, com base nas informações obtidas pela Comissão Temporária, que não subsistem dúvidas quanto à existência de um sistema de intercepção mundial de comunicações que opera com a participação dos Estados Unidos, do Canadá, da Austrália e da Nova Zelândia, ao abrigo do acordo UKUSA;

2. Insta o Secretário-Geral do Conselho da Europa a apresentar ao Comité de Ministros uma proposta tendente a proteger a vida privada, consagrada no artigo 8º da CEDH, em sintonia com métodos de comunicação e de intercepção modernos, por meio de um protocolo adicional ou juntamente com as disposições relativas à protecção dos dados aquando de uma revisão da Convenção relativa à protecção dos dados, na condição de que tal não se traduza, nem numa redução do nível de protecção estabelecido pelo Tribunal Europeu dos Direitos do Homem, nem numa redução da flexibilidade necessária para ter em conta desenvolvimentos futuros;

3. Solicita aos Estados-Membros – cujas leis que regulamentam o poder de intercepção dos serviços secretos criam discriminações em matéria de protecção da privacidade –que assegurem a todos os cidadãos europeus as mesmas garantias legais relativas à protecção da vida privada e ao carácter confidencial da correspondência;

4. Exorta os Estados-Membros da União Europeia a instituírem uma plataforma europeia, composta por representantes dos órgãos nacionais responsáveis pelo controlo do desempenho dos Estados-Membros em matéria de direitos fundamentais e cívicos, a fim de examinar a conformidade das legislações nacionais relativas aos serviços de informações com a CEDH e com a Carta dos Direitos Fundamentais da UE, a reverem as disposições legislativas relativas à garantia da confidencialidade da correspondência e das comunicações, bem como a chegarem a acordo quanto a uma recomendação destinada aos Estados-Membros sobre a elaboração de um código de conduta que garanta, a todos os cidadãos europeus, no território dos Estados-Membros, a protecção da vida privada, tal como definida no artigo 7º da Carta dos Direitos Fundamentais da UE, e que, além disso, assegure que as actividades dos serviços de informações se processem no respeito dos direitos fundamentais e em conformidade com as condições enunciadas no capítulo 8 do presente relatório, em particular no seu ponto 8.3.4, com base no artigo 8º da CEDH;

5. Convida os Estados-Membros a adoptarem, na próxima Conferência Intergovernamental, a Carta dos Direitos Fundamentais da UE enquanto instrumento jurídico vinculativo e susceptível de ser invocado em juízo, por forma a promover o nível de protecção dos direitos fundamentais, em particular no que respeita à protecção da vida privada;

6. Insta os Estados-Membros do Conselho da Europa a adoptarem um protocolo adicional que possibilite a adesão das Comunidades Europeias à CEDH ou a reflectirem sobre outras medidas tendentes a prevenir conflitos jurisprudenciais entre o Tribunal Europeu dos Direitos do Homem e o Tribunal de Justiça Europeu;

7. Insta, entretanto, as Instituições da UE a aplicarem, no âmbito dos respectivos poderes e competências, os direitos fundamentais consagrados na Carta;

8. Exorta o Secretário-Geral da ONU a incumbir a comissão responsável de apresentar propostas que visem a adaptação do artigo 17º do Pacto Internacional sobre os Direitos Civis e Políticos, que garante a protecção da vida privada, ao progresso técnico;

9. Considera necessária a negociação e a assinatura de uma convenção entre a União Europeia e os EUA que estabeleça que cada uma das partes respeitará, relativamente à outra, as disposições em matéria de protecção da vida privada dos cidadãos e de confidencialidade das comunicações das empresas que são aplicáveis aos seus próprios cidadãos e empresas;

10. Insta os EUA a assinarem o Protocolo ao Pacto Internacional sobre os Direitos Civis e Políticos, a fim de tornar admissíveis as queixas apresentadas por particulares por violação do mesmo por parte dos EUA junto da comissão dos direitos do Homem, prevista na Convenção; exorta as ONG americanas pertinentes, em particular a ACLU (American Civil Liberties Union) e a EPIC (Electronic Privacy Information Center) a exercerem pressões nesse sentido junto do governo norte-americano;

Relativamente às disposições legislativas nacionais de protecção dos cidadãos e empresas

11. Exorta os Estados-Membros a examinarem e, se necessário, a adoptarem, a sua própria legislação sobre a actividade dos serviços de informações, a fim de assegurarem a respectiva conformidade com os direitos fundamentais, tal como consagrados na CEDH e na jurisprudência do Tribunal Europeu dos Direitos do Homem;

12. Convida os Estados-Membros a dotarem-se de instrumentos vinculativos que garantam uma protecção efectiva das pessoas singulares e colectivas contra toda e qualquer forma de intercepção ilegal das suas comunicações;

13. Insta os Estados-Membros a diligenciarem no sentido de um nível de protecção comum face à actividade dos serviços de informações e a elaborarem para esse efeito um código de conduta (tal como referido no nº 4) que se norteie pelo nível de protecção nacional mais elevado, uma vez que os cidadãos afectados pela actividade de um serviço de informações externas são, em geral, cidadãos de outros Estados e, por conseguinte, também de outros Estados-Membros;

14. Convida os Estados-Membros a negociarem com os EUA um código de conduta semelhante ao da UE;

15. Convida os Estados-Membros que ainda o não tenham feito a assegurarem um controlo parlamentar e jurisdicional adequado dos respectivos serviços secretos;

16. Exorta o Conselho e os Estados-Membros a conferirem prioridade ao estabelecimento de um sistema de supervisão e de controlo democráticos da capacidade europeia autónoma de recolha de informações, bem como de outras actividades comuns e coordenadas de recolha de informações a nível europeu; sustenta que o Parlamento Europeu deve protagonizar um importante papel nesse sistema de supervisão e de controlo;

17. Convida os Estados-Membros a conjugarem os respectivos meios de intercepção das comunicações, no intuito de reforçar a eficácia da PESD nos domínios dos serviços de informações, da luta contra o terrorismo, da proliferação nuclear ou do tráfico internacional de estupefacientes, no respeito das disposições em matéria de protecção da vida privada dos cidadãos e de confidencialidade das comunicações das empresas, sob o controlo do Parlamento Europeu, do Conselho e da Comissão;

18. Exorta os Estados-Membros a concluirem um acordo com países terceiros na perspectiva do reforço da protecção da vida privada dos cidadãos da UE, nos termos do qual todas as partes contratantes se comprometam a que, em caso de intercepção praticada por uma das partes no território de uma outra, a primeira informará a segunda sobre as medidas previstas;

Relativamente a medidas legais específicas de combate à espionagem económica

19. Exorta os Estados-Membros a examinarem em que medida a espionagem económica e o suborno para fins de obtenção de contratos poderiam ser combatidos mediante disposições do direito europeu e internacional e, em particular, se seria possível adoptar regulamentação no âmbito da OMC que tivesse em conta o impacto de uma tal actividade em termos de distorção da concorrência, determinando, por exemplo, a nulidade de tais

contratos; exorta os Estados Unidos, a Austrália, a Nova Zelândia e o Canadá a participarem nesta iniciativa;

20. Exorta os Estados-Membros a incluírem no Tratado CE uma cláusula que proíba a espionagem económica, a comprometerem-se a não a praticar, directamente ou a coberto de uma potência estrangeira susceptível de operar no seu território, nem a permitir a esta última a realização de operações de espionagem a partir do território de um Estado-Membro da UE, por forma a observarem o espírito e a letra do Tratado CE;

21. Exorta os Estados-Membros a comprometerem-se, mercê de um instrumento inequívoco e vinculativo, a não praticar a espionagem económica e a patentearem desse modo a sua conformidade com o espírito e a letra do Tratado CE; exorta os Estados-Membros a transporem este princípio vinculativo para as respectivas legislações nacionais aplicáveis aos serviços de informações;

22. Exorta os Estados-Membros e o Governo dos EUA a encetarem um diálogo aberto EUA-UE sobre a recolha de informações económicas;

Relativamente às medidas em matéria de aplicação da lei e respectivo controlo

23. Insta os Parlamentos nacionais que não disponham de um órgão parlamentar de controlo dos serviços de informações a procederem à respectiva criação;

24. Insta os órgãos nacionais de controlo das actividades dos serviços secretos a atribuírem grande importância à protecção da vida privada, no exercício das suas funções de controlo, independentemente de os cidadãos visados serem cidadãos nacionais, cidadãos de outros Estados-Membros da UE ou de países terceiros;

25. Exorta os Estados-Membros a diligenciarem no sentido de garantir que os seus sistemas de informações não sejam abusivamente utilizados para fins de recolha de informações em matéria de concorrência, contrariando o dever de lealdade dos Estados-Membros e a perspectiva de um mercado comum assente na livre concorrência;

26. Apela à Alemanha e ao Reino Unido para que, no futuro, subordinem a autorização da intercepção de comunicações, no seu território, pelos serviços de informações dos EUA, à observância do disposto na CEDH, ou seja, para que estabeleçam que tais actividades deverão ser conformes ao princípio da proporcionalidade, que a sua base jurídica deverá ser acessível a todos, devendo os seus efeitos para o indivíduo ser previsíveis, e instituam as devidas medidas de controlo, uma vez que lhes cabe assegurar que as operações desenvolvidas pelos serviços de informações no seu território sejam consentâneas com o respeito dos direitos do Homem, independentemente de as operações em causa serem autorizadas ou meramente toleradas.

Relativamente a medidas de incremento da autoprotecção de cidadãos e empresas

27. Insta a Comissão e os Estados-Membros a informarem os seus cidadãos e as suas empresas sobre a possibilidade de as respectivas comunicações internacionais poderem, em determinadas circunstâncias, ser interceptadas; reitera que esta informação será acompanhada por assistência prática na concepção e implementação de medidas globais de protecção, incluindo a segurança das tecnologias da informação;

28. Insta a Comissão, o Conselho e os Estados-Membros a desenvolverem e a implementarem uma política eficaz e activa em prol da segurança na Sociedade da Informação; reitera que, no quadro desta política, se votará particular atenção ao reforço da sensibilização de todos os utilizadores de modernos sistemas de comunicações para a protecção de informações confidenciais; reitera, além disso, a necessidade de criar, à escala europeia e de forma coordenada, uma rede de organismos capazes de prestar assistência prática na concepção e aplicação de estratégias globais de protecção;

29. Insta a Comissão e os Estados-Membros a elaborarem medidas adequadas à promoção, ao desenvolvimento e à produção de tecnologias e de "software" de encriptação europeus e a apoiarem, sobretudo, os projectos que visem o desenvolvimento de "software" de encriptação de código-fonte aberto e de fácil utilização;

30. Insta a Comissão e os Estados-Membros a promoverem projectos de "software" de código-fonte aberto ("open-source software"), pois só assim se poderá garantir que não tenha lugar a integração de "backdoors" nos programas;

31. Convida a Comissão a definir uma qualificação do nível de segurança dos pacotes de "software" de correio electrónico, colocando na categoria menos fiável todo o "software" cujo código-fonte não seja aberto;

32. Apela às Instituições europeias e às administrações públicas dos Estados-Membros para que pratiquem sistematicamente a encriptação de correio electrónico, por forma a que, a longo prazo, a encriptação se torne regra habitual;

33. Solicita às Instituições comunitárias e às administrações públicas dos Estados-Membros que prevejam a formação do seu pessoal e a familiarização do mesmo com as novas tecnologias e técnicas de encriptação mediante a realização dos estágios e cursos de formação necessários;

34. Requer que seja dispensada uma atenção particular à situação dos países candidatos; solicita que lhes seja prestada assistência, caso os mesmos não possam implementar as medidas de protecção necessárias devido a um défice de independência tecnológica;

Relativamente a outras medidas

35. Exorta as empresas a cooperarem de forma mais estreita com os serviços de contra-espionagem, notificando, em particular, os ataques provenientes do exterior para fins de espionagem económica, de modo a aumentar a eficácia desses serviços;

36. Encarrega a Comissão de providenciar no sentido da realização de uma análise em matéria de segurança que revele aquilo que tem de ser protegido e de desenvolver uma estratégia em matéria de protecção;

37. Exorta a Comissão a actualizar o seu sistema de encriptação de acordo com o nível mais recente, já que é premente uma modernização, e insta a autoridade orçamental (Conselho, juntamente com o Parlamento) a disponibilizar os recursos necessários para o efeito;

38. Solicita à comissão competente quanto à matéria de fundo que elabore um relatório de iniciativa que incida na segurança e na protecção das informações secretas nas Instituições

europeias;

39. Insta a Comissão a garantir a protecção dos dados nos seus próprios sistemas de processamento e a intensificar a protecção das informações confidenciais em relação a documentos que não sejam acessíveis ao público;

40. Exorta a Comissão e os Estados-Membros a investirem, no âmbito do 6º Programa-Quadro de Investigação, em novas tecnologias de descodificação e de codificação;

41. Insta a que, em caso de distorção da concorrência causada por auxílios estatais ou pela espionagem económica, os países prejudicados informem as autoridades e os órgãos de controlo do país a partir de cujo território essas acções tenham sido levadas a cabo, a fim de pôr de termo às actividades de distorção da concorrência;

42. Exorta a Comissão a apresentar uma proposta que, em estreita cooperação com a indústria e com os Estados-Membros, estabeleça uma rede europeia e coordenada de consultoria – em particular naqueles Estados-Membros em que tais centros ainda não existam - sobre questões relacionadas com a segurança das informações nas empresas, a qual, a par do aumento da sensibilização para o problema, tenha também como missão proporcionar ajuda prática;

43. Considera conveniente a organização de um congresso supra-europeu de protecção da vida privada face à vigilância das telecomunicações, a fim de criar uma plataforma que permita às ONG da Europa, dos EUA e de outros Estados debater os aspectos transfronteiriços e internacionais do problema e coordenar domínios de actividades e procedimentos;

44. Encarrega a sua Presidente de transmitir a presente resolução ao Conselho, à Comissão, ao Secretário-Geral e à Assembleia Parlamentar do Conselho da Europa, aos Governos e aos Parlamentos dos Estados-Membros e dos países candidatos à adesão, bem como dos Estados Unidos da América, da Austrália, da Nova Zelândia e do Canadá.

EXPOSIÇÃO DE MOTIVOS

1. Introdução:

1.1. Motivo da constituição da comissão

Em 5 de Junho de 2000, o Parlamento decidiu constituir uma comissão temporária sobre o sistema ECHELON. Na base deste decisão esteve o debate sobre o estudo que o STOA[2] encomendara sobre o sistema designado ECHELON[3] que o seu autor Duncan Campbell apresentara por ocasião de uma audição da Comissão das Liberdades e dos Direitos dos Cidadãos, da Justiça e dos Assuntos Internos dedicada ao tema "A União Europeia e a protecção de dados".

1.2. As afirmações constantes dos estudos STOA sobre a existência de um sistema global de intercepção com o nome de código ECHELON

1.2.1. O primeiro relatório STOA de 1997

Num relatório dedicado ao tema "Avaliação das técnicas de controlo político" que o STOA encomendara em nome do Parlamento Europeu em 1997 à Fundação Omega também é feita uma descrição do sistema ECHELON no capítulo intitulado " Redes nacionais e internacionais de intercepção das comunicações". O autor do estudo afirma que todas as comunicações electrónicas, telefónicas e por fax, na Europa são quotidianamente interceptadas pela NSA (Agência de Segurança Nacional Norte-Americana)[4]. Este relatório chamou a atenção de toda a Europa para a existência do sistema ECHELON, considerado um sistema de intercepção polivalente à escala mundial.

1.2.2. Os relatórios STOA de 1999

Para uma maior informação sobre este assunto, o STOA encomendou em 1999 a realização de um estudo em cinco partes dedicado ao desenvolvimento da tecnologia de vigilância e aos riscos de abuso de informações económicas. O volume 2/5, da autoria de Duncan Campbell é consagrado ao estudo das capacidades de informação actuais, em particular, ao estudo do funcionamento do ECHELON[5].

---

[2] STOA (Avaliação das Opções Científicas e Técnicas) é um serviço da Direcção-Geral de Estudos do Parlamento Europeu que, a pedido das comissões, encomenda trabalhos de investigação a entidades externas. Todavia, não tem lugar qualquer verificação científica dos trabalhos em causa.

[3] *Duncan* Campbell, A tecnologia de ponta em matéria de espionagem de comunicações (COMINT) de processamento automatizado para fins de espionagem de sistemas, de operadores de rede pública ou alugada de banda larga multilíngues interceptados e a respectiva aplicabilidade na procura e selecção de COMINT, incluindo o reconhecimento de voz, vol. 2/5, em: STOA (Ed), O desenvolvimento de tecnologias de vigilância e o risco de utilização abusiva de informações económicas (Outubro de 1999), PE 168.184.

[4] *Steve Wright*, uma avaliação das tecnologias de controlo político, Estudo intercalar do STOA, PE 166.499/INT.ST. (1998), p. 20.

[5] *Duncan Campbell,* A tecnologia de ponta em matéria de espionagem de comunicações (COMINT) de processamento automatizado para fins de espionagem de sistemas, de operadores de rede pública ou alugada de banda larga multilíngues interceptados e a respectiva aplicabilidade na procura e selecção de COMINT, incluindo o reconhecimento de voz,vol. 2/5, em: STOA (Ed), O desenvolvimento de tecnologias de vigilância e o risco de utilização abusiva de informações económicas (Outubro de 1999), PE 168.184.

Uma afirmação contida neste relatório acabaria por suscitar grande polémica: o ECHELON já não prosseguiria o seu objectivo inicial de defesa face ao Leste, tendo passado a constituir um instrumento de espionagem económica. Este tese é fundamentada no relatório por exemplos de alegada espionagem económica, que teriam prejudicado em particular a Airbus e a Thomson CFS. Campbell reporta-se para o efeito a relatos da imprensa americana[6],

Na sequência do estudo do STOA, o ECHELON foi alvo de debates em quase todos os Parlamentos dos Estados-Membros; na França e na Bélgica foram inclusivamente elaborados relatórios sobre este assunto.

1.3. O mandato da comissão

Através da sua decisão sobre a constituição de uma comissão temporária, o Parlamento Europeu fixou igualmente o seu mandato[7]. Nos termos do mesmo, a comissão temporária está encarregada de:

"- confirmar a existência do sistema de intercepção de comunicações conhecido por ECHELON, cujo funcionamento é descrito no relatório STOA sobre o desenvolvimento da tecnologia de vigilância e riscos de abuso de informações económicas;

- verificar a compatibilidade de tal sistema com o direito comunitário, designadamente com o artigo 286º do Tratado CE, com as Directivas 95/46/CE e 97/66/CE, e ainda com o nº 2 do artigo 6º do Tratado UE à luz das seguintes questões:
  - os direitos dos cidadãos europeus encontram-se protegidos das actividades dos serviços secretos?
  - a criptagem constitui uma protecção adequada e suficiente para garantir a defesa da vida privada dos cidadãos, ou deverão ser adoptadas medidas complementares e, em caso afirmativo, que tipo de medidas?
  - de que modo poderão as Instituições da UE ser alertadas para os riscos decorrentes de tais actividades, e que medidas poderão ser adoptadas?

- verificar se a intercepção de informações a nível mundial constitui um risco para a indústria europeia;

- formular, eventualmente, propostas de iniciativas políticas e legislativas."

1.4. Por que não uma comissão de inquérito?

Se o Parlamento Europeu optou pois pela constituição de uma comissão temporária, é porque a constituição de uma comissão de inquérito só é possível para fins de exame de violações do direito comunitário no quadro do Tratado CE (artigo 193º TCE) e que portanto, uma comissão de inquérito só pode ocupar-se das matérias ali visadas.

Os domínios que decorrem do Título V (PESC) e do título VI TUE (Cooperação policial e judicial em matéria penal) são excluídos. Além disso, de acordo com a decisão

[6] Rayethon Corp Press release, http://www.raytheon.com/sivam/contract.html; *Scott Shane, Tom Bowman*, America's Fortress of Spies, Baltimore Sun, 3.12.1995

[7] Decisão do Parlamento Europeu de 5 de Julho de 2000, B5-0593/2000, JO C 121/131 de 24.4.2001

interinstitucional[8], uma comissão de inquérito só pode exercer os seus direitos específicos em matéria de audição e de consulta dos processos se motivos de segredo ou de segurança pública ou nacional não se lhes opuserem, o que impede que se solicite a comparência de membros dos serviços secretos. Do mesmo modo, uma comissão de inquérito não pode estender os seus trabalhos a países terceiros, dado que, por definição, estes não podem violar o direito da União Europeia. Como a constituição de uma comissão de inquérito teria implicado restrições quanto ao trabalho de fundo, sem dar direitos suplementares, a maioria dos deputados ao Parlamento Europeu rejeitou esta solução.

1.5. Metodologia e plano de trabalho

Para poder exercer plena e inteiramente o seu mandato, a comissão optou pelo seguinte procedimento. Um programa de trabalho, proposto pelo relator e aprovado pela comissão, elaborava uma lista dos grandes temas em causa: 1. Conhecimentos seguros relativos ao ECHELON, 2. Discussão nos Parlamentos e governos nacionais, 3. Serviços de espionagem e suas actividades, 4. Sistemas de comunicação e possibilidade de os interceptar, 5. criptagem, 6. Espionagem económica, 7. Objectivos da espionagem e medidas de protecção, 8. Quadro jurídico e protecção da vida privada, 9. Consequências para as relações externas da UE.

Estes temas foram seguidamente estudados em diversas reuniões, sendo a ordem por que foram apreciados ditada por pontos de vista práticos e não pela maior ou menor importância atribuída a cada um deles. Para preparar cada uma das reuniões, o relator consultou e explorou de maneira sistemática a documentação existente. Tendo em conta as necessidades associadas à apreciação do ponto em causa, foram convidados a participar nas diferentes reuniões representantes das administrações nacionais (e nomeadamente dos serviços secretos), bem como dos Parlamentos nacionais, que são os órgãos de controlo dos serviços secretos, peritos jurídicos e peritos nos domínios das técnicas de comunicação e de intercepção, da segurança das empresas e das técnicas de criptagem, e ainda peritos tanto do meio científico como empresarial. Foram igualmente convidados jornalistas que tinham efectuado trabalhos de investigação sobre este tema. Regra geral, as reuniões foram públicas, se bem que foi igualmente decidido realizar reuniões à porta fechada quando tal podia ser útil para obter informações. Além disso, o presidente da comissão e o relator deslocaram-se conjuntamente a Londres e Paris, a fim de ali encontrar pessoas, que, por diferentes razões, não podiam participar nas reuniões da comissão, mas cuja associação aos trabalhos da comissão se afigurava útil. Pelas mesmas razões, a Mesa da comissão, os coordenadores e o relator deslocaram-se aos Estados Unidos. Além disso, o relator realizou numerosas entrevistas individuais, às vezes com carácter confidencial.

1.6. Características atribuídas ao sistema ECHELON

O sistema designado por "ECHELON" distingue-se dos outros sistemas de informação pelo facto de apresentar duas características destinadas a conferir-lhe um nível de qualidade muito específico.

A primeira característica que lhe é atribuída é a capacidade praticamente global de vigilância. Recorrendo principalmente a estações receptoras via satélite e a satélites de espionagem, será possível interceptar qualquer comunicação via telefone, telefax, Internet ou *e-mail*, emitida seja por quem for, de molde a aceder ao respectivo conteúdo.

[8] Decisão do Parlamento Europeu, do Conselho e da Comissão, de 19 de Abril de 1995, relativa às formas de exercício do direito de inquérito do Parlamento Europeu (95/167/CE, Euratom, CECA), art. 3º, nºs 3, 4 e 5.

A segunda característica apontada ao ECHELON é o facto de o sistema funcionar a nível mundial graças a uma cooperação entre vários países (o Reino Unido, os EUA, o Canadá, a Austrália e a Nova Zelândia), o que representa uma mais-valia relativamente a sistemas nacionais: os diferentes países que participam no sistema ECHELON (Estados UKUSA)[9] podem disponibilizar reciprocamente os respectivos dispositivos de escutas, partilhar entre si os encargos e utilizar em comum os resultados obtidos. Esta forma de cooperação internacional é essencial, precisamente, para a vigilância das comunicações de rádio via satélite, pois só assim se pode assegurar que, no caso das comunicações internacionais, seja possível interceptar as informações transmitidas por ambos os interlocutores. Dadas as suas dimensões, é absolutamente evidente que não é possível instalar estações receptoras de comunicações via satélite no território de um país sem o respectivo consentimento. Para tal, é indispensável o acordo mútuo e uma cooperação partilhada entre vários países distribuídos pelo Globo.

No entanto, a ameaça que o ECHELON encerra para a vida privada e a economia não deve ser vista apenas em função do poderoso sistema de vigilância que representa, mas também pelo facto de operar num espaço praticamente à margem da lei. Um sistema de escutas das comunicações internacionais não incide, na maioria dos casos, nos habitantes do próprio país. O visado não dispõe assim, enquanto estrangeiro, de qualquer forma de protecção jurídica nacional, ficando desse modo inteiramente à mercê deste sistema. O controlo parlamentar neste domínio é igualmente insuficiente, pois os eleitores, que partem do princípio de que não são eles os visados, mas "apenas" indivíduos no estrangeiro, não têm qualquer interesse especial nessa questão, e os eleitos seguem essencialmente os interesses dos respectivos eleitores. Assim sendo, não é de surpreender que as audições realizadas no Congresso norte-americano sobre a actividade da NSA se centrem apenas em torno da questão de saber se também haverá incidências nos cidadãos norte-americanos. A existência de um sistema dessa natureza não provoca, em si mesma, qualquer indignação. Tanto mais importante se afigura pois um debate sobre este assunto a nível europeu.

[9] Cf. capítulo 5, 5.4.

2. Actividade dos serviços de informações externas

2.1. Introdução

Para garantir a segurança do Estado, a maior parte dos governos recorrem não só à polícia mas também aos serviços de informações. Estes, dado que a sua actividade é predominantemente secreta, são também chamados de serviços secretos. Estes serviços têm por missão:

- a recolha de informações que permitam fazer face a qualquer perigo para a segurança do Estado,
- dedicar-se, geralmente, à contra-espionagem,
- fazer face aos riscos susceptíveis de constituir uma ameaça para as forças armadas e
- a recolha de informações sobre os desenvolvimentos registados no estrangeiro.

2.2. Que é a espionagem?

Para os governos, é essencial recolher e explorar de maneira sistemática as informações sobre certos desenvolvimentos noutros países. O que procuram neste caso são as bases para as decisões a tomar no domínio das forças armadas, da política externa, etc.. Também se dotaram de serviços de espionagem externa, os quais se dedicam, em primeiro lugar, à exploração sistemática de fontes de informação livremente acessíveis. Com base nas afirmações que lhe foram prestadas, o relator considera que tal representa em média pelo menos 80% da actividade dos serviços de informações[10]. Não obstante, informações particularmente importantes nestes domínios são mantidas secretas pelos governos ou pelas empresas, não sendo por conseguinte acessíveis ao público. Mas quem a elas pretenda aceder, terá de as roubar. A espionagem mais não é do que o roubo organizado de informações.

2.3. Objectivos da espionagem

Os objectivos clássicos da espionagem são os segredos militares, os segredos de outros governos ou informações relativas tanto à estabilidade dos governos como aos riscos a que os estes estão expostos. Em causa estão, por exemplo, os novos sistemas de armamento, as estratégias militares, ou informações relativas ao estacionamento de tropas. Não menos importantes são as informações relativas a decisões iminentes em matéria de política externa, as decisões monetárias ou as informações de iniciados sobre as tensões num governo. Paralelamente, também existe interesse por informações importantes do ponto de vista económico, que podem ser não só informações sectoriais mas também informações precisas sobre novas tecnologias ou transacções comerciais com o estrangeiro.

2.4. Métodos da espionagem

A espionagem significa obter o acesso a informações cujo proprietário deseja precisamente ver salvaguardadas contra a curiosidade de terceiros. É portanto necessário vencer e quebrar essa protecção. Assim acontece tanto na espionagem política como na espionagem económica, razão por que a espionagem nestes dois sectores coloca os mesmos problemas. Por esse motivo são neles aplicadas as mesmas técnicas de espionagem. Do ponto de vista lógico, não há diferença, excepto o nível de protecção, que no mundo económico é geralmente menor, tornando a espionagem económica frequentemente mais simples. Em particular, a consciência do risco

[10] No seu relatório "Preparing for the 21st Century: An Appraisal of U.S. Intelligence" (1996), a "Commission on the Roles and Capabilities of the US Intelligence Community" verifica que 95 % de todas as informações de natureza económica provêm de fontes publiques (capítulo 2 "The Role of intelligence"). http://www.gpo.gov/int/report.html

envolvido na utilização de comunicações susceptíveis de serem interceptadas é menos nítida no meio económico do que a utilizada pelo Estado nos domínios relativos à segurança.

2.4.1. Recurso ao ser humano na espionagem

A protecção das informações secretas organiza-se sempre da mesma maneira:

- só um número reduzido de pessoas consideradas seguras tem acesso às informações secretas;
- existem normas estritas que regem o uso destas informações;
- normalmente, as informações não saem do sector protegido e se o fazem, é unicamente de forma segura ou codificada. Por esse motivo, a espionagem organizada visa em primeiro lugar obter, através de **pessoas** (a chamada *human intelligence*), um acesso directo e sem desvios às informações desejadas. Pode tratar-se neste caso:
  - de membros infiltrados (agentes) do(a) próprio(a) serviço/empresa, ou
  - de pessoas recrutadas junto do alvo.

Geralmente, estas últimas trabalham para serviços/empresas estrangeiros pelas seguintes razões:

- Sedução sexual,
- corrupção pelo dinheiro ou prestações lucrativas,
- chantagem,
- convicções ideológicas,
- conquista de um estatuto ou de uma honra específica (apelo ao descontentamento ou a complexos de inferioridade).

Um caso limite é o da cooperação involuntária (o chamado "fazer render"). Neste caso, os colaboradores de serviços ou empresas são, através da adulação e no âmbito de circunstâncias aparentemente inocentes (conversas à margem de conferências, por ocasião de congressos especializados, em bares de hotel), incitados a "dar à língua".

A utilização de pessoas apresenta a vantagem de oferecer um acesso directo às informações desejadas. Esta solução, porém, também tem inconvenientes:

- a atenção da contra-espionagem concentra-se sempre em pessoas ou agentes principais;
- no caso de pessoas recrutadas, os pontos fracos que incitaram ao seu recrutamento podem ter um efeito de boomerang;
- errar é humano e as pessoas acabam pois, mais tarde ou mais cedo, por se verem envolvidas na rede da contra-espionagem.

Portanto, sempre que possível, procura-se substituir a utilização de agentes ou de pessoas recrutadas por uma espionagem anónima e não pessoal. A solução mais simples consiste em explorar os sinais hertzianos de instalações ou veículos que possuem uma importância militar.

2.4.2. Exploração dos sinais electromagnéticos

Para a opinião pública, a forma a mais conhecida da espionagem por meios técnicos é a utilização da fotografia por satélite. Paralelamente, porém, são interceptados, analisados e avaliados sinais electromagnéticos de todo o tipo (a chamada *signal intelligence*, SIGINT).

2.4.2.1. Sinais electromagnéticos que não servem às comunicações

Certos sinais electromagnéticos, por exemplo, as radiações provenientes das estações radar, podem, no domínio militar, fornecer informações preciosas sobre a organização da defesa aérea do adversário (ELINT, ou *electronic intelligence*). Além disso, as radiações electromagnéticas que fornecem indicações sobre a posição de tropas, aviões, navios ou submarinos, constituem uma fonte de informação muito preciosa para um serviço de informações. Reveste também importância a observação dos satélites de espionagem de outros países que tiram fotografias e o registo e descodificação dos sinais destes satélites.

Os sinais são captados por centrais fixas, satélites de órbita baixa ou satélites SIGINT quase geostacionários. Este domínio da actividade dos serviços secretos relacionada com os sinais electromagnéticos absorve, em termos quantitativos, uma parte importante das capacidades de intercepção dos serviços, mas as possibilidades técnicas não ficam contudo esgotadas.

2.4.2.2. Exploração das comunicações interceptadas

Os serviços de informações externa de muitos países interceptam as comunicações militares e diplomáticas de outros países. Muitos destes serviços vigiam igualmente, desde que a elas tenham acesso, as comunicações civis de outros países. Em certos países, os serviços têm igualmente o direito de controlar as comunicações que entram ou saem do território nacional. Nas democracias, a vigilância das comunicações dos próprios cidadãos pelos serviços de informações está sujeito a certas condições de intervenção e a certos controlos. As ordens jurídicas nacionais porém só protegem, regra geral, os cidadãos e demais pessoas que se encontram no seu próprio território (cf. capítulo 8).

2.5. Actividade de certos serviços de informações

Foi sobretudo a actividade de intercepção dos serviços de informações norte-americanos e britânicos que desencadeou o debate público. As críticas visam a montagem, a análise e avaliação das comunicações (voz, fax, correio electrónico). Para poder emitir um julgamento político, é necessário um quadro de referência que permita avaliar esta actividade. Um critério de comparação pode ser a actividade de intercepção dos serviços de informações externas na União Europeia. O quadro 1 dá uma panorâmica da situação. Dele se deduz que a intercepção das comunicações privadas pelos serviços de informações externas não é uma particularidade dos serviços de informações norte-americanos ou britânicos.

País	Comunicações Exteriores	Comunicações públicas	Comunicações privadas
Bélgica	+	+	-
Dinamarca	+	+	+
Finlândia	+	+	+
França	+	+	+
Alemanha	+	+	+
Grécia	+	+	-
Irlanda	-	-	-
Itália	+	+	+
Luxemburgo	-	-	-

Países Baixos	+	+	+
Áustria	+	+	-
Portugal	+	+	-
Suécia	+	+	+
Espanha	+	+	+
Reino Unido	+	+	+
EUA	+	+	+
Canadá	+	+	+
Austrália	+	+	+
Nova Zelândia	+	+	+

Quadro 1: Actividades de intercepção dos serviços de informações na União Europeia e nos Estados UKUSA

Significado das diferentes colunas:

1ª coluna: país em causa
2ª coluna: comunicações exteriores: abrangem as comunicações que se destinam ao estrangeiro, bem como as comunicações vindas do estrangeiro, podendo tratar-se de comunicações civis, militares ou diplomáticas[11]
3ª coluna: comunicações públicas (militares, diplomáticas, etc.)
4ª coluna: comunicações civis

O sinal de „+“ significa que a comunicação é interceptada
O sinal de „-“ significa que a comunicação não é interceptada

[11] Se o serviço de informações tiver acesso a comunicações transmitidas por cabo, pode interceptar, tanto as comunicações procedentes do estrangeiro como as a este destinadas. Se o serviço de informações interceptar comunicações por satélite, embora tenha apenas acesso ao «downlink », pode, no entanto, interceptar toda a comunicação transportada, ou seja, também a que se não destina ao território do Estado respectivo. Uma vez que os raios de acção dos satélites se estendem, regra geral, por toda a Europa ou por superfícies ainda maiores (cf. Capítulo 4, 4.2.5.), é possível, por meio de terminais de recepção de telecomunicações por satélite num país europeu captar a comunicação via satélite em toda a Europa.

3. Condições técnicas para a intercepção das telecomunicações

3.1. Possibilidade de intercepção dos diferentes meios de comunicação

Quando duas pessoas que se encontram a uma certa distância uma da outra pretendem comunicar, necessitam de um meio de comunicação, que pode ser:

- o ar (som),
- a luz (sinalizador morse, cabo de fibra óptica),
- a corrente eléctrica (telégrafo, telefone),
- uma onda electromagnética (rádio nas mais variadas formas).

Uma terceira pessoa que consiga ter acesso ao meio de comunicação pode interceptar a mesma. O acesso pode ser fácil ou difícil, possível em qualquer sítio ou apenas a partir de certos locais. Em seguida, são abordados dois casos extremos: por um lado, as possibilidades técnicas de um espião no local e, por outro, as possibilidades de um sistema de intercepção que funciona à escala mundial.

3.2. Possibilidades de intercepção no local[12]

Qualquer comunicação pode ser interceptada no local se o interceptador estiver decidido a infringir a lei e o interceptado não se proteger.

- As **conversas** no interior de edifícios podem ser interceptadas por meio de microfones escondidos (escutas) ou de equipamento laser que capta as vibrações das janelas.
- Os **ecrãs** emitem radiação que pode ser captada até uma distância de 30 metros; deste modo, as imagens que aparecem no ecrã tornam-se visíveis.
- O **telefone,** o **telefax** e o **correio electrónico** podem ser interceptados se o interceptador fizer uma ligação aos cabos que saem do edifício.
- Um **telemóvel** pode ser interceptado, ainda que tal seja tecnicamente difícil, se a estação de intercepção se situar na mesma célula (diâmetro em meio urbano - 300 metros; em meio rural - 30 quilómetros).
- As **radiocomunicações móveis privadas** podem ser interceptadas dentro do alcance das ondas rádio ultracurtas.

As condições para a utilização de meios técnicos de espionagem são ideais no local, uma vez que as medidas de intercepção podem ser restringidas a uma única pessoa ou alvo e quase todas as comunicações podem ser captadas. O único inconveniente dos microfones escondidos e das ligações a cabos é o risco de detecção.

[12] *Manfred Fink*, Lauschziel Wirtschaft – Abhörgefahren und –techniken, Vorbeugung und Abwehr, Richard Boorberg Verlag, 1996

3.3. Possibilidades de um sistema de intercepção que funciona à escala mundial

Actualmente, as comunicações intercontinentais dispõem de vários suportes para todos os tipos de comunicação (voz, fax e dados). As possibilidades de um sistema de intercepção que funciona à escala mundial estão limitadas por dois factores:

- o acesso limitado ao meio de comunicação,
- a necessidade de filtrar a comunicação relevante a partir da massa gigantesca de comunicações efectuadas.

3.3.1. Acesso aos meios de comunicação

3.3.1.1. Comunicações por cabo

Todos os tipos de comunicações são transmitidas por cabo (voz, fax, correio electrónico, dados). As comunicações por cabo só podem ser interceptadas quando é possível o acesso ao cabo. O acesso é sempre possível no terminal de uma ligação por cabo se este se encontrar no território do Estado que procede à intercepção. Dentro das fronteiras nacionais, **do ponto de vista técnico**, é possível interceptar todos os cabos, desde que a intercepção seja permitida por lei. Contudo, na maior parte dos casos, os serviços de informações estrangeiros não têm acesso legal aos cabos no território de outros Estados. Na melhor das hipóteses, podem obter, ilegalmente, um acesso pontual, correndo um risco considerável de detecção.

Desde a época do telégrafo, as ligações intercontinentais por cabo são efectuadas através de cabos submarinos. O acesso a estes cabos é sempre possível nos pontos em que voltam a emergir da água. Se vários Estados colaborarem numa rede de intercepção, é possível o acesso a todos os terminais das ligações por cabo situadas nesses Estados. Isto teve alguma importância histórica, dado que tanto os cabos telegráficos submarinos como os primeiros cabos telefónicos coaxiais submarinos entre a Europa e a América emergiam da água na Terra Nova (território canadiano) e as ligações com a Ásia passavam pela Austrália, sendo necessário equipamento de amplificação intermédia. Actualmente, os cabos de fibra óptica seguem uma rota directa, sem qualquer desvio pela Austrália ou Nova Zelândia, independentemente do relevo submarino e da necessidade de equipamento de amplificação intermédia.

Os cabos eléctricos podem igualmente ser conectados por indução (ou seja, por um processo electromagnético, aplicando uma bobina ao cabo) aos terminais de uma ligação, sem efectuar uma ligação condutora directa. Isto é ainda possível a partir de submarinos, embora com custos elevados, no que diz respeito aos cabos eléctricos submarinos. Esta técnica foi utilizada pelos EUA para efectuar uma conexão a um determinado cabo submarino da URSS, através do qual eram transmitidas ordens não codificadas aos submarinos nucleares russos. Uma utilização generalizada desta técnica não é viável, quanto mais não seja devido aos seus custos elevados.

Os cabos de fibra óptica da antiga geração actualmente utilizados só permitem uma ligação indutiva ao nível do equipamento de amplificação intermédia. Este equipamento de amplificação intermédia transforma o sinal óptico num sinal eléctrico, amplifica-o e transforma-o novamente

num sinal óptico. Resta, porém, saber como a quantidade enorme de dados transportada por um cabo deste tipo pode ser transportada do local da intercepção para o local do processamento, sem a colocação de outro cabo de fibra óptica. Devido aos seus custos elevados, a utilização de um submarino equipado com dispositivos técnicos de processamento só é possível muito raramente, por exemplo em caso de guerra, com vista a interceptar comunicações militares estratégicas do inimigo. Na opinião do relator, não se justifica a utilização de um submarino para o controlo quotidiano das telecomunicações internacionais. O equipamento de amplificação intermédia utilizado pelos cabos de fibra óptica da nova geração é o laser de érbio – equipamento que já não permite a intercepção através de uma conexão electromagnética! Portanto, os cabos de fibra óptica deste tipo só podem ser interceptados nos terminais da ligação.

Na prática, isto significa que a rede de intercepção constituída pelos **Estados UKUSA** só pode interceptar comunicações, mediante custos aceitáveis, nos terminais dos cabos submarinos situados no seu território. Em suma, só podem interceptar as comunicações por cabo que entram ou saem do seu território! Por outras palavras, **na Europa,** o seu acesso às comunicações por cabo, à entrada e à saída, restringe-se ao **território do Reino Unido!** Com efeito, até à data, as comunicações internas têm sido quase sempre efectuadas através da rede de cabo interna; com a privatização das telecomunicações, poderão surgir excepções – mas estas serão parciais e imprevisíveis!

Isto aplica-se, pelo menos, ao telefone e ao telefax. No que diz respeito às comunicações por cabo via Internet, as condições são diferentes. A situação pode ser resumida do seguinte modo:

- As comunicações via Internet são efectuadas através de pacotes de dados, podendo os pacotes dirigidos a um mesmo destinatário seguir diferentes caminhos na rede.
- No início da era da Internet, a capacidade não utilizada da rede científica pública foi aproveitada para a transmissão de correio electrónico. Por conseguinte, o encaminhamento de uma mensagem era totalmente imprevisível, seguindo cada pacote de dados uma rota caótica e imprevisível. Nessa época, a ligação internacional mais importante era a "espinha dorsal científica" entre a Europa e a América.
- A comercialização da Internet e o estabelecimento de fornecedores de serviços da Internet deu igualmente origem a uma comercialização da rede. Os fornecedores de serviços da Internet exploravam ou alugavam as suas próprias redes. Por conseguinte, procuravam cada vez mais confinar as comunicações às suas próprias redes, a fim de evitar o pagamento de taxas de utilização a outros operadores. Deste modo, o caminho seguido na rede por um pacote de dados não é hoje determinado apenas pela capacidade, dependendo também de considerações financeiras.
- Um e-mail enviado pelo cliente de um fornecedor ao cliente de outro fornecedor é geralmente encaminhado através da rede da empresa, mesmo que esse não seja o caminho mais rápido. Os computadores situados nos nós da rede e que decidem o transporte dos pacotes de dados (os "encaminhadores") organizam a transferência para outras redes em determinados pontos (os "comutadores").
- Na época da espinha dorsal científica, os comutadores das comunicações globais via Internet estavam situados nos EUA. Por esse motivo, os serviços de informações podiam interceptar uma parte substancial das comunicações europeias via Internet. Actualmente,

apenas uma pequena percentagem das comunicações intraeuropeias via Internet passa pelos EUA[13].

- Uma pequena parte das comunicações intraeuropeias é encaminhada através de um comutador localizado em Londres, ao qual o serviço de informações britânico GCHQ tem acesso, dado tratar-se de comutações com o estrangeiro. O grosso das comunicações não sai do continente. Mais de 95% das comunicações alemãs via Internet, por exemplo, são encaminhadas através de um comutador localizado em Frankfurt.

Na prática, isto significa que os Estados UKUSA só podem ter acesso a uma **percentagem muito limitada** das comunicações por cabo via Internet.

3.3.1.2. Radiocomunicações [14]

A possibilidade de intercepção das radiocomunicações depende do alcance das ondas electromagnéticas utilizadas. Se as ondas radioeléctricas emitidas seguirem a curvatura da superfície terrestre (**ondas de superfície**), o seu alcance é limitado e depende da natureza do terreno, das construções e da vegetação. Se as ondas radioeléctricas forem enviadas para o espaço (**ondas de espaço)**, podem transpor distâncias consideráveis após reflexão nas camadas da ionosfera. Reflexões múltiplas aumentam substancialmente o alcance.

O alcance depende do comprimento de onda:

- As ondas miriamétricas e longas (3 kHz-300 kHz) propagam-se apenas através de ondas de superfície, uma vez que as ondas de espaço não são reflectidas. Têm um alcance reduzido.
- As ondas médias (300 kHz-3 MHz) propagam-se apenas através de ondas de superfície e, à noite, também através de ondas de espaço. Têm um alcance médio.
- As ondas curtas (3 MHz-30 MHz) propagam-se sobretudo através de ondas de espaço e, em virtude de reflexões múltiplas, permitem uma recepção **global**.
- As ondas ultracurtas (30 MHz-300 MHz) propagam-se apenas através de ondas de superfície, uma vez que as ondas de espaço não são reflectidas. Propagam-se praticamente em linha recta, como a luz. Deste modo, o seu alcance é determinado, devido à curvatura da Terra, pela altura das antenas emissoras e receptoras. Dependendo da potência, o seu alcance pode atingir aproximadamente 100 km (no caso dos telemóveis, cerca de 30 km).
- As ondas decimétricas e centimétricas (30 MHz-30 GHz), ainda mais que as ondas ultracurtas, propagam-se de forma quase idêntica à luz. São fáceis de reunir em feixes e permitem transmissões unidireccionais com potência reduzida (feixes hertzianos terrestres). Só podem ser captadas com uma antena muito próxima e paralela ao feixe hertziano, situada no eixo do mesmo ou no seu prolongamento.

[13] Com a ajuda de uma versão de demonstração de Visual Route, um programa que indica o trajecto percorrido por uma ligação na Internet, foi possível ilustrar que, no caso de uma ligação com a Inglaterra, a Finlândia ou a Grécia feita a partir da Alemanha, essa ligação se processa via EUA e Grã-Bretanha. Uma ligação da Alemanha para a França processa-se igualmente via Grã-Bretanha. As ligações para a Bélgica, Grécia, Suécia ou Portugal a partir do Luxemburgo são encaminhadas via EUA. As ligações para a Alemanha, Finlândia, França, Itália, os Países Baixos ou Áustria são encaminhadas através do « switch » em Londres, http://visualroute.cgan.com.hk/

[14] *Ulrich Freyer*, Nachrichtenübertragungstechnik, Hanser Verlag 2000

As ondas longas e médias são utilizadas apenas para emissores rádio, radiofaróis, etc. As radiocomunicações militares e civis efectuam-se através de ondas curtas e, sobretudo, através de ondas ultracurtas, ondas decimétricas e centimétricas.

O acima exposto revela que um sistema de intercepção de comunicações que funciona à escala mundial só pode interceptar transmissões em onda curta. No que diz respeito a todos os outros tipos de radiocomunicações, a estação de intercepção deve estar situada a 100 km de distância ou mais perto (por exemplo, num navio, numa embaixada).

Na prática, isto significa que os **Estados UKUSA** que dispõem de estações de intercepção terrestres só têm acesso a uma percentagem muito reduzida das radiocomunicações.

3.3.1.3. Comunicações transmitidas por satélites de telecomunicações geoestacionários[15]

Conforme já foi referido, as ondas decimétricas e centimétricas podem facilmente ser reunidas em feixes hertzianos. Se um feixe hertziano for dirigido para um satélite de comunicações em órbita geostacionária de altitude elevada, satélite esse que recebe, transforma e reenvia para a Terra os sinais hertzianos, é possível transpor grandes distâncias sem a utilização de cabos. Na realidade, o alcance de tal ligação é apenas limitado pelo facto de o satélite não poder receber e enviar sinais de e para todo o globo terrestre. Por este motivo, são utilizados vários satélites para obter uma cobertura global (para mais pormenores, ver o capítulo 4). Se os Estados UKUSA explorarem estações de intercepção nas regiões relevantes da Terra, poderão, em princípio, interceptar todas as comunicações – de telefone, fax e dados – efectuadas através de tais satélites.

3.3.1.4. Possibilidades de intercepção a partir de aviões e navios

Sabe-se há muito tempo que aviões especiais do tipo AWACS são utilizados para localizar outros aviões a longa distância. O radar destes aparelhos está equipado com um sistema de identificação de objectivos específicos que pode localizar, classificar e correlacionar radiações electrónicas através de contactos por radar. Contudo, não dispõem de uma capacidade SIGINT (actividades de espionagem de sinais electrónicos) distinta[16]. Em contrapartida, o avião de espionagem EP-3 da Marinha americana, que voa a baixa velocidade, possui a capacidade de interceptar microondas, ondas ultracurtas e ondas curtas. Os sinais são analisados directamente a bordo; o avião é utilizado apenas para fins militares[17].

Além disso, são utilizados navios de superfície e, nas zonas costeiras, submarinos para a intercepção das radiocomunicações militares[18].

---

[15] *Hans Dodel*, Satellitenkommunikation, Hüthig Verlag 1999

[16] Carta de Walter Kolbow, Secretário de Estado no Ministério Federal Alemão da Defesa, ao relator, com data de 14 de Fevereiro de 2001

[17] Süddeutsche Zeitung nº 80, de 5 de Abril de 2001, p. 6

[18] *Jeffrey T. Richelson*, The U.S. Intelligence Community, Ballinger, 1989, p. 188 , p. 190

3.3.1.5. Possibilidades de intercepção a partir de satélites espia

Desde que não estejam reunidas em feixes por antenas apropriadas, as ondas radioeléctricas propagam-se em todas as direcções, incluindo o espaço. Os satélites SIGINT de órbita de baixa altitude só podem manter o contacto com o emissor alvo durante alguns minutos. Em zonas densamente povoadas e altamente industrializadas, a intercepção é de tal modo dificultada pela elevada densidade de emissores que utilizam a mesma frequência, que se torna praticamente impossível filtrar sinais isolados.[19] Os satélites não se prestam ao controlo continuado das radiocomunicações civis.

Paralelamente, existem os satélites SIGINT americanos, ditos quase-estacionários, de órbita de altitude elevada (42.000 km)[20]. Ao contrário dos satélites de comunicações geoestacionários, estes satélites têm uma inclinação que varia entre os 3 e os 10 graus, um apogeu de 39.000 a 42.000 km e um perigeu de 30.000 a 33.000 km. Portanto, estes satélites não permanecem imóveis em órbita, descrevendo uma órbita elíptica complexa. Deste modo, no decurso de um dia, cobrem uma região mais vasta e permitem localizar fontes de radiocomunicações. Estas e outras características, do domínio público, apontam para uma utilização puramente militar dos satélites.

Os sinais recebidos são transmitidos para a estação receptora através de uma potente ligação descendente de 24 GHz.

3.3.2. Possibilidades de análise automática das comunicações interceptadas: utilização de filtros

Quando as comunicações do estrangeiro são objecto de intercepção, esta não visa uma determinada ligação telefónica. O objectivo consiste antes em interceptar a totalidade ou uma parte da comunicação efectuada através dos satélites controlados ou do cabo controlado e filtrar a mesma por meio de computadores, utilizando conceitos-chave. Isto porque a análise de todas as comunicações interceptadas é completamente impossível.

A filtragem das comunicações efectuadas por determinadas ligações é fácil. Através da utilização de conceitos-chave, também é possível interceptar de forma específica comunicações transmitidas por telefax e correio electrónico. É mesmo possível distinguir uma determinada voz, desde que o sistema tenha sido concebido para reconhecer a voz[21]. Por outro lado, o reconhecimento automático de palavras pronunciadas por uma voz qualquer, de acordo com as informações de que o relator dispõe, ainda não é possível com a devida precisão. Além disso, as possibilidades de filtragem também são limitadas por outros factores: a capacidade final do computador, o problema linguístico e, principalmente, o número reduzido de peritos capazes de ler e analisar as mensagens filtradas.

---

[19] Carta de Walter Kolbow, Secretário de Estado do Ministério Federal Alemão da Defesa, ao relator, de 14 de Fevereiro de 2001

[20] *A. Major*, Zarubezhnoye voyennoye obozreniye, nº 12,1993, págs. 37-43

[21] Comunicação transmitida ao relator em privado, fonte protegida

Ao avaliar as possibilidades dos sistemas de filtragem, é necessário ter igualmente em conta que o conjunto das possibilidades técnicas de um tal sistema de intercepção, que funciona de acordo com o "princípio do aspirador", se repartem por diversos temas. Uma parte das palavras-chave diz respeito à segurança militar, uma segunda parte ao tráfico de droga e a outras formas de criminalidade internacional, uma terceira parte a conceitos relativos ao comércio de bens de dupla utilização e uma outra parte está relacionada com o cumprimento de embargos. Uma parte dos conceitos-chave relaciona-se igualmente com a economia. Isto significa que as capacidades do sistema se dividem por diversos domínios. Uma concentração das palavras-chave no domínio interessante do ponto de vista económico não contrariaria apenas as exigências impostas aos serviços de informações pelos dirigentes políticos; tal medida não foi adoptada nem mesmo após o final da guerra fria[22].

3.3.3. O exemplo do serviço de informações alemão

A segunda secção do serviço de informações alemão (BND) obtém informações através da intercepção das comunicações do estrangeiro. Esta actividade foi objecto de um exame por parte do Tribunal Constitucional Alemão. Os pormenores que foram tornados públicos no decurso deste processo[23], juntamente com as declarações prestadas pelo coordenador dos serviços secretos na chancelaria federal, Ernst Uhrlau, perante a comissão ECHELON, em 21 de Novembro de 2000, dão uma ideia das possibilidades dos serviços de informações em matéria de intercepção de comunicações via satélite (até Maio de 2001 não era permitida na Alemanha a intercepção, pelo BND, de comunicações transmitidas por cabo com procedência do estrangeiro).

As possibilidades dos outros serviços de informações, em consequência de diferentes condições-quadro de ordem legal, podem ser maiores, em questões de pormenor, em determinadas zonas. A intercepção das comunicações por cabo aumenta especialmente a probabilidade estatística de êxito, mas não necessariamente o número das comunicações analisáveis. De facto, o caso do BND constitui, na opinião do relator, um exemplo bem claro das possibilidades e estratégias dos serviços de informações estrangeiros no que se refere à intercepção de comunicações do estrangeiro, mesmo que os referidos serviços não divulguem estas questões ao público.

O serviço de informações alemão procura, através de um controlo **estratégico** das telecomunicações, obter no estrangeiro informações sobre o estrangeiro. Para este efeito, as comunicações via satélite são interceptadas mediante a utilização de uma série de termos de pesquisa (os quais, na Alemanha, carecem de uma autorização prévia da comissão G10[24]). Em termos quantitativos, o panorama é o seguinte (situação relativa a 2000): dos cerca de 10 milhões de comunicações internacionais efectuadas diariamente da e para a Alemanha, cerca de 800.000 são transmitidas via satélite. Menos de 10% destas comunicações (75.000) são filtradas por um motor de pesquisa. Na opinião do relator, esta limitação não se deve a razões jurídicas (em teoria, teria sido autorizado um número de 100%, pelo menos antes do processo no tribunal constitucional alemão), mas sim técnicas, decorrentes de outras limitações, nomeadamente a capacidade de análise limitada.

---

[22] Comunicação transmitida ao relator em privado, fonte protegida

[23] BverfG, 1 BvR 2226/94 de 14 de Julho de 1999, nº 1

[24] Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (lei relativa ao artigo 10º da Lei Fundamental) de 13 de Agosto de 1968

De igual modo, o número dos termos de pesquisa utilizáveis é limitado por motivos técnicos e pela necessidade de uma autorização prévia. A exposição de motivos do acórdão do tribunal constitucional alemão refere, para além dos termos de pesquisa puramente formais (ligações efectuadas por estrangeiros ou por empresas estrangeiras no estrangeiro), 2.000 termos de pesquisa no domínio da proliferação nuclear, 1.000 termos de pesquisa no domínio do comércio de armas, 500 termos de pesquisa no domínio do terrorismo e 400 termos de pesquisa no domínio do tráfico de droga. No entanto, o processo não foi muito bem sucedido em relação ao terrorismo e ao tráfico de droga.

O motor de pesquisa controla os termos de pesquisa autorizados, transmitidos por telefax ou telex. Actualmente, não é possível o reconhecimento automático de palavras nas comunicações vocais. Se os termos de pesquisa não são encontrados, as comunicações acabam automaticamente, por motivos técnicos, no cesto dos papéis; não podem ser analisadas, dado não haver nenhuma base jurídica que o permita. Diariamente, cerca de 5 comunicações efectuadas por utilizadores das telecomunicações são protegidas ao abrigo da Constituição alemã. A intercepção estratégica do serviço de informações alemão visa encontrar elementos que possam servir de base a uma outra intercepção. O seu objectivo não consiste em proceder a um controlo absoluto das comunicações do estrangeiro. De acordo com as informações de que o relator dispõe, o mesmo se aplica em relação às actividades SIGINT de outros serviços de informações estrangeiros.

4. Técnica das comunicações por satélite

4.1. Importância dos satélites de comunicações

Os satélites de comunicações constituem hoje um elemento indispensável da rede mundial de telecomunicações e da difusão de programas de televisão e de rádio, assim como dos serviços multimédia. Não obstante, a percentagem das comunicações por satélite nas comunicações internacionais diminuiu consideravelmente na Europa Central nos últimos anos, situando-se entre 0,4 e 5%[25]. Esta situação está relacionada com as vantagens oferecidas pelos cabos de fibra óptica, que podem receber um número muito mais elevado de comunicações, assegurando simultaneamente uma qualidade mais elevada das ligações.

Actualmente, as comunicações processam-se de forma digital, incluindo o sector vocal. A capacidade das ligações digitais via satélite limita-se, por transponders de satélite, a **1890** canais vocais que obedecem à norma ISDN (64 kbists/seg). Em contrapartida, uma única fibra óptica pode hoje transmitir **241920** canais vocais com base na mesma norma. Tal corresponde a uma relação de **1:128**!

Acresce que a qualidade das ligações via satélite é inferior à da oferecida por cabos submarinos de fibra óptica. As perdas de qualidade devidas aos atrasos dos sinais - diversas centenas de milisegundos - quase não são perceptíveis numa transmissão vocal normal, embora se possa ouvir o diferido. No caso de comunicações de dados e de telefax, que se efectuam através de um processo complexo de "handshaking", o cabo apresenta vantagens manifestas em termos de segurança da ligação. Todavia, apenas 15% da população mundial está conectada à rede global de cabos[26].

A longo prazo, os sistemas de satélites continuarão, no entanto, a ser mais vantajosos que o cabo para determinadas aplicações. Podemos citar alguns exemplos no plano civil:

- Comunicações telefónicas e de dados nacionais, regionais e internacionais em regiões com um reduzido volume de comunicações, ou seja, em regiões em que a realização de uma ligação por cabo não seria rentável, tendo em conta a baixa taxa de utilização.

- Comunicações limitadas no tempo no caso de intervenções em situações de catástrofe, manifestações, obras de construção de grandes dimensões, etc.

- Missões da ONU em regiões que não dispõem de infra-estruturas de comunicações suficientemente desenvolvidas.

- Comunicação económica flexível/móvel com microestações terrestres (V-SAT, ver infra)

Este espectro da utilização de satélites nas comunicações resulta das seguintes características: o raio de acção de um único satélite geoestacionário pode cobrir quase 50% da superfície terrestre;

[25] Indicações com base em respostas dos operadores de telecomunicações de alguns Estados-Membros europeus, a pedido da comissão.

[26] "Homepage" da Deutsche Telekom: www.detesat.com/deutsch/

terrenos inacessíveis podem ser igualmente transpostos. Neste domínio, 100% dos utilizadores, que podem ser cobertos, quer a nível terrestre, quer a nível marítimo ou aéreo. Os satélites podem tornar-se operacionais em poucos meses, independentemente a infra-estrutura local, são mais fiáveis que o cabo e podem ser facilmente desactivados.

As seguintes características das comunicações por satélite suscitam um juízo negativo: o tempo de percurso relativamente longo dos sinais, a degradação da propagação, o tempo de vida - 12 a 15 anos - mais curto que o do cabo, a maior vulnerabilidade, assim como a fácil intercepção.

4.2. Funcionamento de uma ligação por satélite[27]

Como já foi anteriormente dito (ver capítulo 3), as microondas podem ser facilmente reunidas em feixes através de antenas adequadas. Por esse motivo, é possível substituir o cabo por feixes hertzianos. Se a antena de emissão e a antena de recepção não se encontrarem ao mesmo nível, o que acontece no caso da Terra em que a superfície é uma esfera, a antena de recepção "desaparece" debaixo do horizonte a partir de uma determinada distância em virtude da curvatura. As antenas deixam então de se "ver". Tal aconteceria igualmente, por exemplo, no caso de um feixe hertziano intercontinental entre a Europa e os EUA. As antenas teriam de estar situadas em postes de 1,8 km de altura para poderem estabelecer uma ligação. Basta este motivo para que um tal feixe hertziano intercontinental não seja viável, para não falar no amortecimento do sinal pela atmosfera e pelo vapor de água ao longo do percurso. Contudo, se se conseguir instalar a grande altitude no espaço e numa "posição fixa" uma espécie de espelho para o feixe hertziano, consegue-se transpor grandes distâncias apesar da curvatura da Terra, tal como um espelho retrovisor que permite ver determinados ângulos. O princípio atrás descrito é aplicado na prática através da utilização dos denominados satélites geoestacionários.

4.2.1. Satélites geoestacionários

Se um satélite for colocado numa órbita circular paralelamente ao Equador e girar, em 24 horas, uma vez à volta da Terra, este segue exactamente a rotação da Terra. Visto da superfície terrestre, encontra-se imóvel a uma altitude de cerca de 36000 km, o que significa que tem uma posição **geoestacionária**. A maior parte dos satélites de telecomunicações e de radiodifusão pertencem a este tipo de satélites.

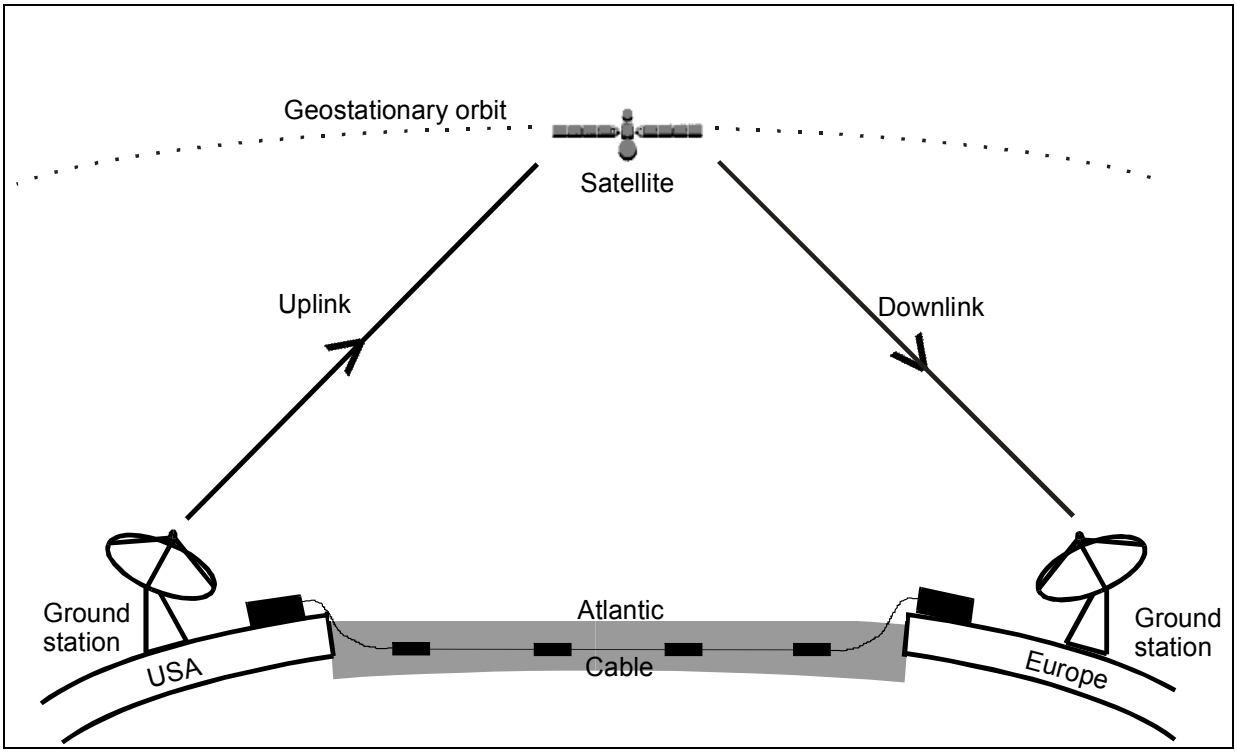
4.2.2. O percurso dos sinais de uma comunicação por satélite

A transmissão de sinais por satélites processa-se do seguinte modo:

O sinal proveniente de uma linha é enviado para o satélite por uma estação terrestre equipada com uma antena parabólica através de um feixe hertziano ascendente, o denominado "**uplink**". O satélite recebe o sinal, reforça-o e envia-o através de um feixe hertziano descendente, o denominado "**downlink**", para outra estação terrestre. Aí, o sinal é reencaminhado para uma rede de cabo.

No caso das comunicações móveis (telemóveis que funcionam via satélite), o sinal é transmitido directamente da unidade móvel de comunicações para o satélite, podendo ser daí novamente introduzido numa linha através de uma estação terrestre ou ser directamente retransmitido para outra unidade móvel.

[27] *Hans Dodel,* Satellitenkommunikation, Hüthig Verlag (1999), *Georg E. Thaller,* Satelliten im Erdorbit, Franzisverlag (1999)



4.2.3. Principais sistemas de comunicação por satélite existentes

As comunicações provenientes de **redes de cabo de acesso público** (não necessariamente estatais) são, se tal for o caso, transmitidas através de sistemas de satélite de diferentes dimensões a partir de e para estações terrestres fixas e seguidamente introduzidas em redes de cabo. Estabelece-se uma distinção entre sistemas de satélite

- globais (por exemplo, INTELSAT)

- regionais (continentais) (por exemplo, EUTELSAT)

- nacionais (por exemplo, ITALSAT)

A maior parte destes satélites encontram-se numa posição geoestacionária; a nível mundial 120 empresas privadas exploram cerca de 1000 satélites colocados nesta posição[28].

Paralelamente, existem para o extremo Norte satélites com uma órbita especial altamente excêntrica (órbitas russas Molnyia), sendo os satélites visíveis para os utilizadores no extremo Norte durante mais de metade do seu percurso orbital. Dois satélites permitem, em princípio, uma cobertura regional[29] que não seria viável através de uma posição geoestacionária sobre o Equador. No caso dos satélites russos Molnyia, operacionais desde 1974 enquanto satélites de comunicações (protótipo já em 1964), são três os satélites que giram em torno da Terra com

[28] *Georg. E. Thaller*, Satelliten im Erdorbit, Franzisverlag (1999)

[29] Cf. *Hans Dodel,* Satellitenkommunikation, Hüthig Verlag (1999)

períodos orbitais de 12 horas e uma distância entre si de 120°, assegurando, assim, uma transmissão contínua de comunicações[30].
Além disso, o sistema INMARSAT, que opera a nível mundial e foi inicialmente concebido para utilização no mar, constitui um **sistema de comunicações móveis** que permite estabelecer ligações por satélite em qualquer parte do mundo. Funciona igualmente com a ajuda de satélites geoestacionários.

O sistema IRIDIUM, um sistema de telemóvel por satélite operando a nível mundial graças a diversos satélites colocados em órbitas baixas diferidas, foi há pouco tempo desactivado por razões de rentabilidade, dada a baixa taxa de utilização.

Existe ainda um mercado em rápida evolução para as denominadas ligações VSAT (VSAT = terminal de abertura muito pequena). Trata-se de microestações terrestres equipadas com antenas de um diâmetro entre 0,9 e 3,7 m, que são exploradas pelas empresas para as suas necessidades próprias (por exemplo, videoconferências) ou por fornecedores de serviços móveis para ligações limitadas no tempo (por exemplo, congressos). Em 1996, existiam a nível mundial 200.000 microestações terrestres. A Volkswagen AG explora 3.000, a Renault 4.000, a General Motors 100.000 e o maior grupo petrolífero europeu 12.000 unidades. VSAT. As comunicações realizam-se de forma aberta se o cliente não assegurar ele próprio a criptagem[31].

4.2.3.1. Sistemas de satélite que operam à escala mundial

Estes sistemas de satélite cobrem a totalidade do globo terrestre através da distribuição de diversos satélites na zona do Atlântico, do Índico e do Pacífico.

INTELSAT[32]

A INTELSAT (International Telecomunications Satellite Organisation) foi fundada em 1964 como uma autoridade dotada de uma estrutura organizativa semelhante à das Nações Unidas e com o objectivo comercial de operar as comunicações internacionais. Os seus membros eram constituídos pelos Correios nacionais públicos. Hoje são membros da INTELSAT 144 governos. A INTELSAT será privatizada em 2001.

A INTELSAT explora entretanto uma frota de 20 satélites geoestacionários, que ligam mais de 200 países e cujos serviços são alugados aos membros da INTELSAT. Os membros dispõem das suas próprias estações terrestres. Desde 1984, terceiros (por exemplo, empresas de telefones, grandes empresas, grupos internacionais) podem utilizar os satélites através do INTELSAT Business Service (IBS). A INTELSAT oferece, a nível mundial, serviços em diferentes domínios, designadamente comunicações, televisão, etc. As telecomunicações processam-se nas bandas C e Ku (vide infra).

Os satélites INTELSAT são os mais importantes satélites de comunicações internacionais. Asseguram a maior parte das comunicações internacionais por satélite e cobrem as zonas do Atlântico, do Índico e do Pacífico (ver tabela, capítulo 5, 5.3).

[30] Homepage da Federação Americana de Cientistas Americanos http://www.geo-orbit.org

[31] *Hans Dodel*, Comunicação particular

[32] "Homepage" da INTELSAT-http://www.intelsat.com

Sobre o Atlântico, existem 10 satélites situados entre 304°E e 359°E, o Índico é coberto por 6 satélites situados entre 62°E e 110,5°E e o Pacífico por 3 satélites situados entre 174°E e 180°E. Diversos satélites individuais sobre o Atlântico permitem cobrir o elevado volume de tráfego.

INTERSPUTNIK[33]

Em 1971, foi criada por 9 países a organização internacional de comunicações por satélite INTERSPUTNIK como uma agência da ex-União Soviética com tarefas idênticas à INTELSAT. INTERSPUTNIK é hoje uma organização interestatal, à qual pode aderir o governo de qualquer Estado. Conta actualmente com 24 países membros (designadamente, a Alemanha) e cerca de 40 utilizadores (designadamente a França e o Reino Unido), representados pelas suas administrações postais ou empresas de telecomunicações. A sua sede é em Moscovo.

As telecomunicações processam-se nas bandas C- e Ku- (ver infra).

Os satélites (Gorizont, Express, Express A da Federação Russa e LMI-1 da "joint venture" Lockhead-Martin), cobrem igualmente todo o globo terrestre: sobre o Atlântico encontra-se um satélite, estando projectado um segundo, sobre o Índico encontram-se 3 satélites e sobre o Pacífico 2 satélites (ver tabela, capítulo 5, 5.3).

INMARSAT[34]

INMARSAT (Interim International Maritime Satellite) assegura, desde 1979, com o seu sistema de satélites, a nível mundial comunicações **móveis** a nível marítimo, aéreo e terrestre, bem como um sistema de chamadas de emergência. INMARSAT nasceu de uma iniciativa da Organização Marítima Internacional como uma organização entre Estados. A INMARSAT foi entretanto privatizada e tem a sua sede em Londres.

O sistema INMARSAT é constituído por 9 satélites em órbitas geoestacionárias. Quatro destes satélites - a geração INMARSAT-III - cobrem todo o globo terrestre até às regiões polares mais afastadas. Cada satélite cobre cerca de 1/3 da superfície terrestre. Graças ao seu posicionamento sobre as 4 regiões oceânicas (Atlântico Ocidental e Oriental, Pacífico e Índico) permitem uma cobertura global. Simultaneamente, cada satélite INMARSAT dispõe de um certo número de feixes pontuais, o que permite concentrar a energia nas regiões com um elevado volume de tráfego.

As comunicações efectuam-se nas bandas L- e Ku- (ver infra 4.2.4).

[33] "Homepage" do INTERSPUTNIK: http://www.intersputnik.com

[34] « Homepage » da INMARSAT, http://www.inmarsat.com

PANAMSAT[35]

A PanAmSat foi fundada em 1988 como operador comercial de um sistema de satélites global, tendo a sua sede nos EUA. Entretanto, a PanAmSat possui uma frota de 21 satélites, oferecendo, a nível mundial, mas sobretudo nos EUA, vários serviços, nomeadamente de televisão, Internet e telecomunicações.

A transmissão das telecomunicações efectua-se nas bandas C e Ku.

Dos 21 satélites existentes, 7 cobrem o Oceano Atlântico, duas o Pacífico e duas o Índico. Os raios de acção dos restantes satélites estendem-se pela América (do Norte e do Sul). No respeitante às comunicações na Europa, os satélites PanAm desempenham apenas um papel secundário.

4.2.3.2. Sistemas de satélite regionais

O raio de acção de satélites regionais permite cobrir determinadas regiões e continentes. As comunicações transmitidas por estes satélites apenas podem ser recebidas nestas regiões.

EUTELSAT[36]

EUTELSAT foi fundada em 1977 por 17 administrações postais europeias com o objectivo de cobrir as necessidades específicas da Europa no domínio das comunicações por satélite e apoiar a indústria aeroespacial europeia. Tem a sua sede em Paris e cerca de 40 membros. A EUTELSAT deve ser privatizada em 2001.

A EUTELSAT explora 18 satélites geoestacionários, que cobrem a Europa, a África e uma grande parte da Ásia e asseguram uma ligação com a América. Os satélites estão situados entre 12,5°W e 48°E. A EUTELSAT oferece principalmente serviços de televisão (850 canais digitais e analógicos) e rádio (520 canais), assegurando igualmente serviços de comunicações - essencialmente na Europa (incluindo a Rússia): por exemplo, videoconferências, redes privadas de grandes empresas (por exemplo, General Motors e Fiat), agências noticiosas (Reuters, AFP), fornecedores de dados financeiros, assim como serviços móveis de transmissão de dados.

As telecomunicações efectuam-se na banda Ku.

ARABSAT[37]

A ARABSAT, criada em 1976, é o correspondente de EUTELSAT na região árabe. Os seus membros são 21 países árabes. Os satélites ARABSAT são utilizados tanto para a difusão de televisão como para as comunicações.

As telecomunicações são efectuadas principalmente na banda C.

---

[35] « Homepage » da PANAMSAT, http://www.panamsat.com

[36] "Homepage" de EUTELSAT: http://www.com

[37] "Homepage" de ARABSAT: http://www.arabsat.

PALAPA[38]

O sistema indonésio PALAPA funciona desde 1995 e é o correspondente sulasiático de EUTELSAT. O seu raio de acção cobre a Malásia, a China, o Japão, a Índia, o Paquistão e outros países da região.

As telecomunicações processam-se nas bandas C e Ku.

4.2.3.3. Sistemas de satélite nacionais[39]

Muitos Estados utilizam, para satisfazer as necessidades nacionais, sistemas de satélite próprios com raios de acção limitados.

O satélite francês de telecomunicações **TELECOM** assegura, inter alia, a ligação entre os departamentos franceses em África e na América do Sul com a França. As telecomunicações processam-se nas bandas C e Ku.

A **ITALSAT** explora satélites de telecomunicações que cobrem a totalidade do território italiano mediante raios de acção contíguos e limitados, pelo que a recepção apenas é possível em Itália. As telecomunicações processam-se na banda Ku.

AMOS é um satélite israelita, cujo "raio de acção" cobre o Médio Oriente. As telecomunicações processam-se na banda Ku.

Os satélites espanhóis **HISPASAT** cobrem a Espanha e Portugal ("spots" Ku) e transportam programas espanhóis de televisão para a América do Norte e do Sul.

4.2.4. Atribuição de frequências

A atribuição de frequências é da responsabilidade da União Internacional das Telecomunicações (ITU (International Telecommunication Union)). A fim de estabelecer uma certa ordem, o mundo foi dividido em três regiões para efeitos de comunicações:

1. Europa, África, ex-União Soviética, Mongólia

2. América do Norte e América do Sul, assim como a Groenlândia

3. Ásia, exceptuando os países da região 1, Austrália e Sul do Pacífico

Esta repartição tradicional foi mantida para as comunicações por satélite e deu origem a uma concentração de satélites em determinadas zonas geoestacionárias.

As principais bandas de frequência para as comunicações por satélite são as seguintes:

- a banda L (0.4 - 1.6 GHz) para as comunicações móveis por satélite, por exemplo, via INMARSAT.

[38] *Hans Dodel*, Satellitenkommunikation, Hüthig Verlag 1999

[39] *Hans Dodel*, , Satellitenkommunikation e pesquisa Internet

- a banda C (3,6 - 6,6 GHz) para estações terrestres, por exemplo, via INTELSAT, e outros satélites de comunicações civis.

- a banda Ku (10 - 20GHz) para estações terrestres, por exemplo, INTELSAT-Ku-Spot e EUTELSAT

- a banda Ka (20 - 46 GHz) para estações terrestres, por exemplo, satélites de comunicações militares (cf. capítulo 4, 4.3)

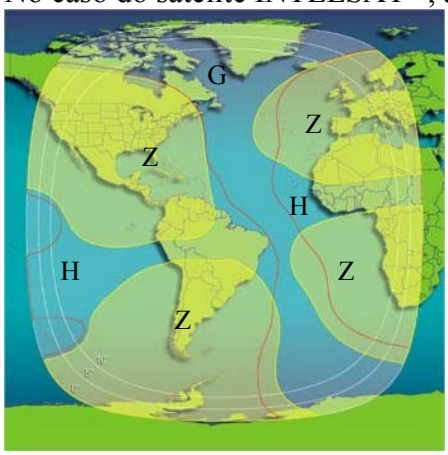
- a banda V (46 – 56 GHz) para microestações terrestres (V-SAT)

4.2.5. Raios de acção dos satélites (footprints)

Por raio de acção ou "footprint", entende-se a região da Terra que é coberta pela antena do satélite. Pode abranger até 50% da superfície terrestre ou, mediante a concentração do sinal, limitar-se a pequenos "spots" regionais.

Quanto mais elevada é a frequência do sinal emitido, mais este pode ser concentrado e mais limitado é, em consequência, o raio de acção. Mediante uma concentração do sinal de satélite emitido em raios de acção mais limitados, a energia do sinal pode ser aumentada. Quanto mais pequeno é o raio de acção, mais forte pode ser o sinal e mais pequenas podem ser, por conseguinte, as antenas de recepção.

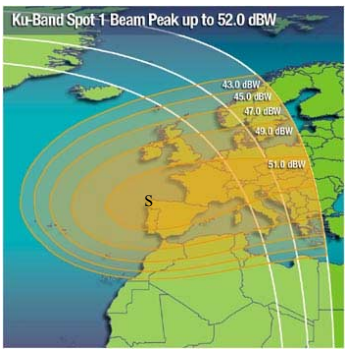
No caso do satélite INTELSAT[40], a situação é resumidamente a seguinte:

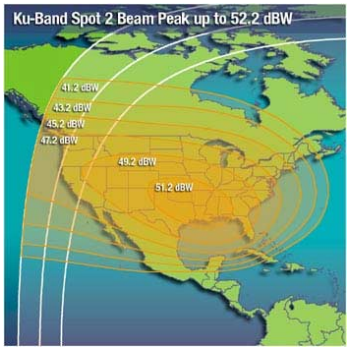


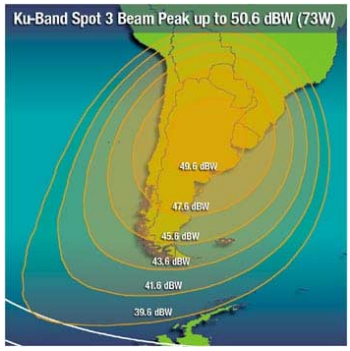
Os raios de acção dos satélites INTELSAT estão subdivididos em diversos "beams":

O "global-beam" (G) de cada satélite cobre cerca de 1/3 da superfície terrestre, os "hemi-beams" (H) cobrem, respectivamente, uma metade que é ligeiramente mais pequena do que a metade do "global beam". “Zone-beams” (Z) são "spots" em determinadas zonas da Terra; são de dimensões inferiores às dos "hemi-beams". Além disso, existem ainda os denominados "spot-beams", que são "footprints" precisos e de pequenas dimensões (ver infra).

[40] Satélite INTELSAT 706, 307°E, raios de acção dos satélites da Homepage INTELSAT : http://www.intelsat.com







As frequências da banda C encontram-se nos "global", "hemi" e "zone-beams". As frequências da banda Ku encontram-se nos "spot-beams".

4.2.6. Dimensões das antenas necessárias para uma estação terrestre

Como antenas de recepção terrestres são utilizadas antenas parabólicas com diâmetro de 0,5 metros a 30 metros. O espelho parabólico reflecte todas as ondas captadas e concentra-as no seu ponto focal. No ponto focal, encontra-se o sistema de recepção propriamente dito. Quanto mais forte é a energia do sinal no local de recepção, mais reduzido pode ser o diâmetro da antena parabólica.

Determinante para o objectivo do inquérito realizado mediante o presente relatório é o facto de uma parte das comunicações intercontinentais se processar através da banda C nos "global-beams dos satélites INTELSAT e de outros satélites (por exemplo, INTERSPUTNIK), para cuja recepção são, por vezes, necessárias antenas de satélite com um diâmetro de cerca de 30 m (ver capítulo 5). Antenas com 30 m de diâmetro foram igualmente necessárias para as primeiras estações de recepção de comunicações por satélite, dado que a primeira geração INTELSAT apenas dispunha de "global-beams" e a transmissão de sinais estava muito menos aperfeiçoada do que está hoje. Estas antenas com um diâmetro, por vezes, superior a 30 m são ainda utilizadas nas estações correspondentes, ainda que não sejam necessárias do ponto de vista técnico (cf. capítulo 5, 5.2.3).

As antenas típicas, hoje utilizadas nas comunicações INTELSAT em banda C, têm um diâmetro de 13 a 20 m.

Para os "spots-Ku" dos satélites INTELSAT e também de outros satélites (EUTELSAT-banda Ku, AMOS banda Ku etc.) são necessárias antenas com um diâmetro entre 2 a 10 m.

Para as microestações terrestres, que operam na banda V e cujo sinal pode ser ainda mais concentrado do que na banda Ku, dada a frequência elevada, são suficientes antenas com um diâmetro entre 0,5 e 3,7 m (por exemplo, VSAT de EUTELSAT ou INMARSAT).

4.3. Comunicação via satélite para fins militares

4.3.1. Generalidades

Também no domínio militar é importante o papel desempenhado pelos satélites de telecomunicações. São muitos os países – entre os quais os EUA, o Reino Unido, a França e a Rússia – que operam satélites próprios geoestacionários de comunicações militares, que permitem uma comunicação global independente de outros meios de transmissão de

comunicações. Dispondo de cerca de 32 posições orbitais em todo o mundo, os EUA procederam à colocação, em média, de um satélite de 10 em 10°. Para fins de comunicação militar, recorre-se, por vezes, também a satélites geoestacionários comerciais.

4.3.2. Frequências utilizadas para fins militares

As bandas de frequência em que se processa a comunicação militar situam-se entre 4 GHz e 81 GHz. Frequências habitualmente utilizadas por satélites de comunicações militares são a banda X (SHF) (3-30 GHz) e a banda Ka (EHF) (20-46 GHz).

4.3.3. Dimensão das estações de recepção

No tocante às estações de recepção utilizadas, procede-se à distinção entre estações móveis cujas dimensões podem ser de poucos decímetros, e estações fixas cujo diâmetro não ultrapassa, regra geral, os 11 metros. Existem, todavia, dois tipos de antenas (para a recepção de satélites DSCS) com um diâmetro de 18 metros.

4.3.4. Exemplos de satélites de comunicações militares

O programa norte-americano **MILSTAR** (Military Strategy, Tactical and Relay Satellite System), que, na globalidade, opera seis satélites geoestacionários, permite às forças armadas dos EUA comunicar entre si e com as centrais de comando a nível mundial, utilizando pequenas estações terrestres, aviões, navios e também "Man-Packs". Graças à interconexão dos satélites, a sua operacionalidade a nível mundial mantém-se assegurada, mesmo que todas as estações terrestres sitas fora do território americano se encontram inoperacionais.

O DSCS (Defense Satellite Communications System) permite igualmente uma comunicação a nível global mercê de cinco satélites geoestacionários. O sistema de comunicação é utilizado pelos serviços militares dos EUA, bem como por alguns organismos governamentais.

O sistema de satélites militares britânico **SKYNET** é igualmente disponível a nível global.

O sistema francês **SYRACUSE**, o sistema italiano **SICRAL**, bem como o sistema espanhol encontram-se instalados nos satélites de comunicações civis nacionais respectivos e disponibilizam comunicação militar na banda X, a qual é, contudo, apenas de alcance regional.

Os Russos asseguram a comunicação das suas forças armadas através de "transponder" (repetidores de satélite) na banda dos satélites Molnyia.

A NATO opera os seus próprios satélites de comunicações (**NATO IIID, NATO IVA** e **IVB**). Os satélites transmitem comunicação vocal, telex e dados entre as diferentes unidades militares.

5. Prova indiciária da existência de, pelo menos, um sistema de intercepção global

5.1. Porquê uma prova indiciária?

Os serviços secretos não divulgam obviamente os detalhes das suas actividades. Do mesmo modo, não existe qualquer declaração oficial dos serviços de informações externas dos Estados UKUSA em que afirmem que cooperam na exploração de um sistema de intercepção global. Assim sendo, a existência apenas pode ser provada mediante a recolha do maior número possível de indícios por forma a obter uma prova indiciária convincente.

A cadeia dos indícios que constituem esta prova é composta por três elementos:

- a prova de que os serviços de informações externas dos Estados UKUSA interceptam comunicações privadas e comerciais.
- a prova de que, dado o modo de funcionamento do sistema civil de comunicações por satélite, é possível encontrar nas partes da Terra necessárias para o efeito estações de intercepção geridas por um dos Estados UKUSA.
- a prova de que existe uma associação entre os serviços de informação destes Estados que vai muito para além do que é habitual. Se esta actividade vai até ao ponto de efectuar operações de intercepção a pedido de parceiros e de transmitir directamente o material bruto interceptado sem aproveitamento próprio é irrelevante para provar a existência de uma associação. Esta questão apenas é importante, quando se trata de estabelecer as hierarquias dentro de uma tal associação.

5.1.1. Prova da actividade de intercepção por parte dos serviços de informações externas

Pelo menos nas democracias, os serviços de informações exercem as suas actividades com base em leis que enunciam os seus objectivos e/ou os seus poderes. É, assim, fácil provar que em muitos destes Estados existem serviços de informações externas que interceptam as comunicações civis. Tal aplica-se igualmente aos 5 Estados UKUSA indicados, que todos eles dispõem de tais serviços. No caso de cada um destes Estados, não é necessária qualquer prova adicional de que interceptam comunicações destinadas ao país ou provenientes do país. A partir do próprio território, é igualmente possível captar, no caso das comunicações por satélite, uma parte das mensagens enviadas a destinatários no estrangeiro. Em nenhum dos 5 Estados UKUSA, existe qualquer disposição legal que impeça os serviços de o fazer. A lógica interna do método do controlo estratégico das telecomunicações externas e o seu objectivo, conhecido pelo menos em parte, levam a que necessariamente se conclua que os serviços agem efectivamente desta forma.[41]

[41] O relator dispõe de informações de que tal é verdade. Fonte protegida.

5.1.2. Prova da existência de estações nas zonas geograficamente necessárias

O único entrave à tentativa de criação de uma vigilância à escala mundial das comunicações efectuadas por satélite resulta da própria tecnologia utilizada por esta comunicação. Não existe qualquer local a partir do qual seja possível captar **todas** as comunicações por satélite à escala mundial (ver capítulo 4, 4.2.5).

Um sistema de intercepção que opere a nível mundial apenas poderá ser criado se estiverem preenchidas três condições:

- o operador tem território próprio em todas as regiões do mundo necessárias para o efeito;
- o operador tem em todas as regiões do mundo necessárias para o efeito, por um lado, território próprio e, por outro, um direito de hospitalidade nas outras regiões do mundo que lhe faltam, podendo aí explorar estações ou utilizar estações locais;
- o operador é uma associação de Estados no domínio dos serviços de informações e explora o sistema nas regiões do mundo necessárias para o efeito.

Nenhum dos Estados UKUSA seria capaz de explorar a título individual um tal sistema global. Os EUA não têm, pelo menos formalmente, colónias. O Canadá, a Austrália e a Nova Zelândia não possuem igualmente qualquer território fora do seu país em sentido restrito. Também o Reino Unido não poderia explorar apenas para si próprio um tal sistema de intercepção global.

5.1.3. Prova da existência de uma associação estreita entre os serviços de informações

Em contrapartida, não é possível saber se e de que forma os Estados UKUSA cooperam no domínio dos serviços de informações. Habitualmente, a cooperação entre os serviços tem um carácter bilateral e processa-se com base no intercâmbio de material examinado. Uma associação multilateral é, já em si, algo muito excepcional; se lhe acrescentarmos ainda o intercâmbio regular de material bruto, teremos então uma dimensão totalmente nova. Uma associação desta natureza apenas pode ser provada com base em indícios

5.2. Como se reconhece uma estação de intercepção de comunicações por satélite?

5.2.1. Critério 1: acessibilidade da instalação

As instalações dos correios, das empresas de radiodifusão ou de centros de investigação equipadas com antenas de grandes dimensões são acessíveis aos visitantes, pelo menos com marcação da visita. As estações de intercepção, em contrapartida, não podem ser visitadas. Na maior parte dos casos, são formalmente geridas por militares que têm igualmente a seu cargo, pelo menos, em parte, o lado técnico da intercepção. Assim, nas estações operadas pelos EUA, essa gestão é feita, conjuntamente com a NSA, pelo "Naval Security Group" (NAVSECGRU), pelo "United States Army Intelligence and Security Command" (INSCOM) ou pela "Air Intelligence Agency" da Força Aérea norte-americana (AIA). Nas estações britânicas, a gestão das instalações é feita conjuntamente pelos serviços de informações britânicos GCHQ e pela "Royal Airforce" (RAF). Este modo de funcionamento permite um rigoroso controlo militar das instalações e serve simultaneamente para camuflar as actividades.

5.2.2. Critério 2: tipo de antena

Nas instalações que preenchem o critério 1, existem diversos tipos de antenas que se distinguem pela sua configuração característica. A sua forma é elucidativa para o objectivo perseguido pela instalação de intercepção. Assim, um conjunto de altas antenas de haste que formam um círculo de grande diâmetro (denominadas antenas Wullenweber) são utilizadas para captar a direcção dos sinais radioeléctricos. Um conjunto circular de antenas rombiformes (denominadas antenas Pusher) são utilizadas para o mesmo efeito. As antenas de recepção multidireccional ou antenas direccionais, que se assemelham a antenas de televisão tradicionais gigantescas, servem para interceptar sinais radioeléctricos não direccionados. **Para a recepção de sinais de satélites são, em contrapartida, utilizadas exclusivamente antenas parabólicas.** Se as antenas parabólicas se encontram a descoberto no terreno, é possível calcular, conhecendo a sua localização, o seu ângulo de inclinação (elevação), e o seu ângulo de direcção (azimute), que satélite é interceptado. Tal seria, por exemplo, possível em Morwenstow (UK), em Yakima (EUA) ou em Sugar Grove (EUA). Na maior parte dos casos, porém, as antenas parabólicas estão escondidas debaixo de um invólucro branco esférico, a chamada calote. Serve para proteger as antenas, mas também para camuflar a sua orientação.

Se no terreno de uma estação de intercepção se encontram antenas parabólicas ou calotes, é certo que aí são captados sinais de satélites. Todavia, tal não diz ainda de que tipo de sinais se trata.

5.2.3. Critério 3: dimensões da antena

As antenas de recepção de satélites numa instalação que preenche o critério 1 podem servir para diversos fins:
- Estações de recepção para satélites de comunicações militares
- Estações de recepção para satélites de espionagem (imagens, radar)
- Estações de recepção para satélites SIGINT
- Estações de recepção para intercepção de satélites de comunicações civis.

Pelo seu aspecto exterior, não é possível deduzir para que efeito servem as antenas/calotes. Não obstante, o respectivo diâmetro permite concluir qual a sua função. No respeitante aos satélites de comunicações civis, destinados a receber o denominado "global beam" na banda C das comunicações civis internacionais por satélite, existem dimensões mínimas requeridas por questões de ordem técnica. Na primeira geração destes satélites, eram necessárias antenas com um diâmetro que variava entre 25 e 30 metros, hoje é suficiente um diâmetro que varia entre 15 e 20 metros. Esta filtragem automática dos sinais interceptados por computador requer uma qualidade óptima dos sinais. Para serviços de informações, opta-se, por esse motivo, por uma antena com as dimensões máximas.

Também para fins de comunicação militar existem nas centrais de comando dois tipos de antenas com um diâmetro de cerca de 18 metros (AN/FSC-78 e AN/FSC-79). Todavia, a maioria das antenas para fins de comunicação militar tem um diâmetro muito menor, porquanto têm de ser portáteis (estações tácticas).

Nas estações terrestres de satélites SIGINT são apenas necessárias pequenas antenas em virtude das características do sinal retransmitido à estação (elevada concentração de energia e alta frequência). Tal aplica-se igualmente a antenas que recebem sinais de satélites de espionagem.

Se, numa estação, existirem, pelo menos, duas antenas de satélite com dimensões superiores a 18 metros, pode concluir-se que aí são interceptadas comunicações civis por satélite. Caso uma

estação seja utilizada por forças armadas norte-americanas, uma das antenas pode igualmente servir para fins de comunicação militar.

5.2.4. Critério 4: provas procedentes de fontes oficiais

Relativamente a algumas estações, existem descrições precisas procedentes de fontes oficiais. Por tal entendem-se informações emanadas do Governo e informações provenientes de unidades militares. Caso se observe este critério, os restantes critérios enunciados tornam-se supérfluos para classificar uma estação como estação de intercepção de comunicações civis.

5.3. Dados publicamente acessíveis sobre estações de intercepção conhecidas

5.3.1. Método

A fim de verificar quais são as estações que preenchem os critérios enunciados no capítulo 5.2., fazem parte do sistema global de intercepção e que missões têm a seu cargo, examinou-se a literatura pertinente, por vezes contraditória (Hager[42], Richelson[43], Campbell[44]), documentos desclassificados[45], a homepage" da Federação dos Cientistas Americanos[46] assim como as homepages dos operadores[47] (NSA, AIA, etc) e outras publicações Internet. No respeitante à estação neozelandesa cita em Waihopai, observa-se a existência de uma descrição oficial das suas funções emanadas do Governo da Nova Zelândia[48]. Além disso, foram agrupados os raios de acção dos satélites de comunicação, calculadas as dimensões das antenas necessárias e registadas em mapas do mundo juntamente com as eventuais estações.

5.3.2. Análise exacta

Para o exame, são aplicados os seguintes princípios relacionados com a física das comunicações por satélite (ver igualmente capítulo 4) :

---

[42] *Nicky Hager*: Exposing the global surveillance system http://www.ncoic.com/echelon1.htm
Nicky Hager: Secret Power. New Zealands´s Role in the international Spy Network, Craig Potton Publishing, 1996

[43] *Jeffrey T. Richelson*, Desperately seeking Signals, The Bulletin of the Atomic Scientists, vol. 56, nº 2, 47-51, http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html
Jeffrey T. Richelson, The U.S. Intelligence Community, Westview Press 1999

[44] *Duncan Campbell*, Tecnologia de ponta em matéria de espionagem de comunicações (COMINT) de processamento automatizado para fins de espionagem de sistemas, de operadores de rede pública ou alugada de banda larga multilingues interceptados e a respectiva aplicabilidade na procura e selecção de COMINT, incluindo o reconhecimento de voz, vol. 2/5, em: STOA (Ed), O desenvolvimento de tecnologias de vigilância e o risco de utilização abusiva de informações económicas (Outubro de 1999), PE 168.184
http://www.europarl.eu.int/dg4/stoa/en/publi/pdf/98-14-01-2en.pdf
Duncan Campbell: Inside ECHELON, 25.7.2000http://www.heise.de/tp/deutsch/special/ech/6928/1.html
Duncan Campbel: Interception Capabilities n- Impact and Exploitation – ECHELON and its role in COMINT, apresentada à Comissão Temporária do Parlamento Europeu "ECHELON" em 22 de Janeiro de 2001
Federation of American Scientists, http://www.fas.org/irp/nsa/nsafacil.html

[45] *Jeffrey T. Richelson*: Newly released documents on the restrictions NSA places on reporting the identities of US-persons: Declassified: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html

[46] Federation of American Scientists (FAS), http://www.fas.org/

[47] Military.com; *.mil-Homepages

[48] Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet, Securing our Nation's Safety (2000), http://www.dpmc.govt.nz/dess/securingoursafety/index.html

- Uma antena de satélite apenas pode captar o que se encontra dentro do seu raio de acção. A fim de poder receber comunicações que se processam principalmente nas bandas C e Ku, a antena deve situar-se dentro dos raios de acção que contêm as bandas C e Ku.
- Para cada "global-beam" é necessária uma antena de satélite, ainda que se sobreponham os beams de dois satélites.
- Caso um satélite tenha mais raios de acção que apenas o "global-beam", o que é característico para a actual geração de satélites, não é possível captar com uma única antena de satélite toda a comunicação processada através deste satélite, uma vez que uma única antena de satélite não pode estar em todos os raios de acção do satélite. Para captar o "hemi-beams" e o "global-beams" de um satélite, são, portanto, necessárias duas antenas de satélite em diversos territórios (ver descrição dos raios de acção no capítulo 4). Se forem acrescentados outros beams ("zone- e spotbeams"), são necessárias mais antenas de satélite. Diversos beams de um satélite que se sobreponham podem ser, em princípio, captados por uma antena de satélite, uma vez que é tecnicamente possível separar diversas bandas de frequência aquando da recepção. Tal prejudica, todavia, o *ratio* sinal/ruído.

Além disso, aplicam-se os pressupostos enunciados no capítulo 5.2.: não acessibilidade das instalações, uma vez que são geridas por militares[49], o facto de serem necessárias antenas parabólicas para captar sinais de satélite e as dimensões das antenas para captar a Banda C no "global-beam" terem de apresentar um diâmetro de, pelo menos, 30 metros, no caso da primeira geração INTELSAT, e de 15 – 18 metros, no caso das gerações subsequentes. No referente a uma parte das estações, as descrições oficiais das respectivas funções foram consideradas como prova do papel das mesmas enquanto estações de intercepção.

5.3.2.1. Paralelismo entre os desenvolvimento de INTELSAT e a construção de estações

Um sistema de intercepção global deve acompanhar os progressos da comunicação. O início da comunicação por satélite é necessariamente acompanhado da criação de estações, a introdução de novas gerações de satélites, da criação de novas estações, assim como da construção de novas antenas de satélite que preencham os requisitos necessários. O número de estações e o número de antenas de satélite tem de aumentar em função das necessidades de captação de informações. Inversamente, quando surgem novas estações e são construídas novas antenas de satélite nos locais em que são acrescentadas novos raios de acção, tal não constitui um acaso, podendo ser antes considerado como o indício da existência de uma estação de intercepção de comunicações. Uma vez que os satélites INTELSAT foram os primeiros satélites de comunicações, que, além disso, cobriam todo o globo terrestre, é lógico que a criação e ampliação de estações acompanhe as gerações INTELSAT.

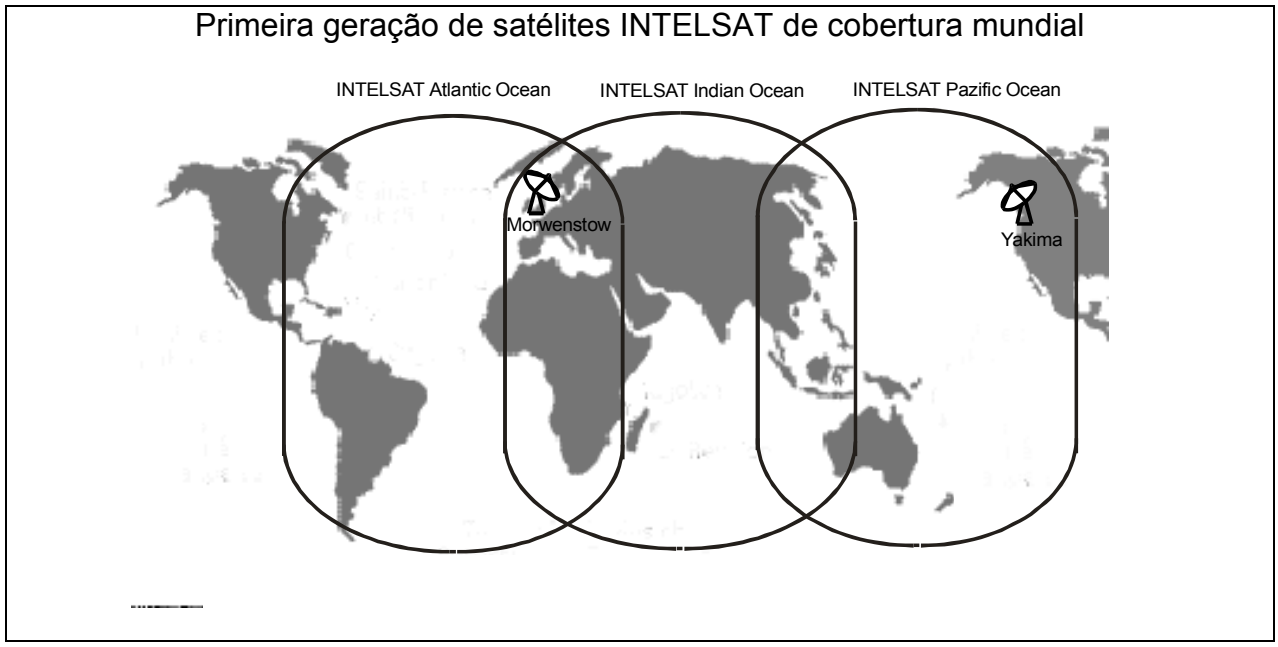
A primeira geração de satélites de cobertura mundial

O primeiro satélite INTELSAT (Early Bird) foi colocado na órbita geoestacionária já em 1965. A sua capacidade de transmissão era ainda reduzida e o seu raio de acção abrangia ainda apenas o hemisfério norte.

As gerações INTELSAT II e III, que começaram a ser exploradas em 1967 e 1968, permitiram alcançar, pela primeira vez, uma cobertura mundial. Os "global-beams" dos satélites cobriam as zonas do Atlântico, Pacífico e Índico. Não existiam ainda raios de acção de menores dimensões.

[49] Abreviaturas utilizadas: NAVSECGRU: Naval Security Group, INSCOM: United States Army Intelligence And Security Command, AIA: Air Intelligence Agency, IG: Intelligence Group, IS: Intelligence Sqadron, IW: Intelligence Wing, IOG: Information Operation Group, MIG: Military Intelligence Group

Para captar a totalidade das comunicações eram, assim, necessárias três antenas de satélite. Uma vez que dois "global-beams" se sobrepunham sobre o espaço europeu, era possível captar, neste território, numa estação equipada com duas antenas de satélite com orientação diferente as zonas de iluminação mundiais de dois satélites.

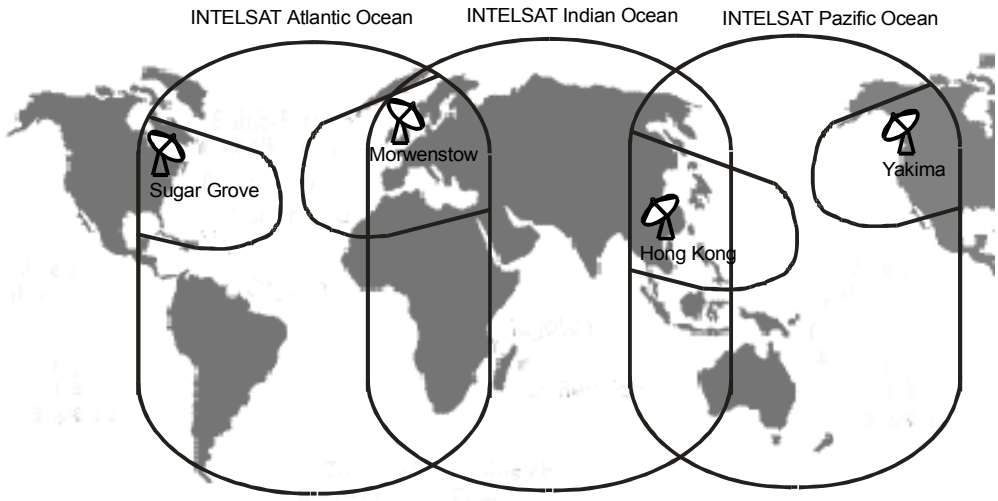


Nos primórdios dos anos 70, foi fundada **Yakima** no Noroeste dos Estados Unidos, em 1972/73 **Morwenstow** no Sul da Inglaterra. Yakima dispunha então de uma antena de grandes dimensões orientada para o Pacífico), Morwenstow dispunha de duas antenas de grandes dimensões (a primeira orientada para o Atlântico, a segunda para o Oceano Índico). A localização de ambas as estações permitia captar a totalidade das comunicações.

A segunda geração de satélites de cobertura mundial

A segunda geração de satélites INTELSAT (IV e IVA) foi desenvolvida nos anos 70 e colocada em órbita geoestacionária (1971 e 1975). Os novos satélites, que asseguravam igualmente uma cobertura mundial e dispunham de um número consideravelmente superior de canais (4000 a 6000), tinham no hemisfério norte igualmente "zone-beams", para além do "global-beams" (ver capítulo 4). Um "zone-beam" cobria a parte oriental do EUA, um segundo a parte ocidental dos EUA, um terceiro a Europa Ocidental e um outro último a Ásia Oriental. A captação da totalidade das comunicações deixou de ser possível através de duas estações com três antenas de satélite. Com as estações existentes em Yakima, era possível cobri o "zone-beam" na parte ocidental dos EUA, com Morwenstow o "zone-beam" sobre Europa. Para captar os outros dois "zone-beams", tornaram-se necessárias duas novas estações, uma na parte oriental dos EUA e outra na Ásia Oriental.

Segunda geração de satélites INTELSAT de cobertura mundial



No final dos anos 70, foi construída a estação de **Sugar Grove** na parte oriental dos EUA (a estação existia já para a intercepção de comunicações russas); entrou em funcionamento em 1980. Igualmente no final dos anos 70, foi criada uma estação em **Hong Kong** . Com as quatro estações – Yakima, Morwenstow, Sugar Grove e HongKong, - tornou-se possível, nos anos 80, uma intercepção global das comunicações via INTELSAT.

Os satélites INTELSAT seguintes, com "zone-beams" e "spot-beams" , para além do "global- e do hemi-beams", tornaram necessárias novas estações em diversas partes do mundo. Neste caso, é muito difícil documentar, com base nas informações existentes, uma relação entre a criação de novas estações e a instalação de novas antenas de satélite. Acresce que é muito difícil obter acesso a informações sobre estações e não é possível determinar exactamente que satélites com que "beams" são captados por que estação. É, no entanto, possível verificar em que "beams" se encontram estações conhecidas.

5.3.2.2. Cobertura mundial por estações que claramente interceptam satélites de comunicações

A comunicação global por satélite é hoje assegurada por satélites de INTELSAT, INMARSAT e INTERSPUTNIK. A repartição em três raios de acção (Índico, Pacífico e Atlântico) mantém-se, à semelhança da primeira geração de satélites. Em cada um dos raios de acção encontram-se estações às quais se aplicam os critérios característicos de estações de intercepção:

Satélites sobre o Oceano Índico :

INTELSAT 604 (60°E), 602 (62°E), 804 (64°E), 704 (66°E) EXPRESS 6A (80°E) INMARSAT zona do Índico	Geraldton, Austrália Pine Gap, Austrália Morwenstow, Reino Unido Menwith Hill, Reino Unido
INTELSAT APR1 (83°), APR-2 (110,5°)	Geraldton, Austrália Pine Gap, Austrália Misawa, Japão

Satélites sobre o Oceano Pacífico :

INTELSAT 802 (174°), 702 (176°), 701 (180°) GORIZONT 41 (130°E), 42 (142°E), LM-1 (75°E) INMARSAT zona do Pacífico	Waihopai, Nova Zelândia Geraldton, Austrália Pine Gap, Austrália Misawa, Japão Yakima, EUA - apenas Intelsat e Inmarsat

Satélites sobre o Oceano Atlântico :

INTELSAT 805 (304,5°), 706 (307°), 709 (310°) 601 (325,5°), 801 (328°), 511(330,5°), 605 (332,5°), 603 (335,5°), 705 (342°) EXPRESS 2 (14°W), 3A (11°W) INMARSAT zona do Atlântico	Sugar Grove, EUA Sabana Seca, Porto Rico Morwenstow, Reino Unido Menwith Hill, Reino Unido
INTELSAT 707 (359°)	Morwenstow, Reino Unido Menwith Hill, Reino Unido

Tal demonstra que é possível uma intercepção global de comunicações.

Existem, além disso, ainda outras estações às quais não se aplica o critério das dimensões da antena e relativamente às quais não existam quaisquer outros elementos probatórios inequívocos, mas que são, no entanto, parte do sistema global de intercepção. Com estas estações, podem ser por exemplo captados os "zone ou spot-beams" de satélites cujos "global-beams" são interceptados por outras estações ou para cujo "global-beam" não é necessária uma antena de satélite de grandes dimensões.

5.3.2.3. Descrição detalhada das estações

Na descrição detalhada das estações estabelece-se uma diferença entre estações que claramente procedem à intercepção de satélites de comunicações (critérios enunciados no capítulo 5.2.) e estações cuja missão não pode ser seguramente provada com base nos referidos critérios.

5.3.2.3.1. Estações de intercepção de satélites de comunicação

Os critérios descritos no capítulo 5.2., que podem ser utilizados como indícios da existência de uma estação de intercepção de satélites de comunicações, aplicam-se às seguintes estações:

Yakima, EUA (120°W, 46°N)
A estação foi criada nos primórdios dos anos 70, em simultâneo com a primeira geração de satélites. Desde 1995, encontra-se aí o 544th Intelligence Group (Destacamento 4) da Air Intelligence Agency (AIA). Aí estacionado está igualmente o Naval Security Group (NAVSECGRU). No terreno, estão instaladas seis antenas de satélite, não fornecendo as fontes quaisquer informações sobre as respectivas dimensões. Segundo Hager, as antenas de satélite têm grandes dimensões e estão orientadas para satélites Intelsat sobre o Pacífico (2 antenas de satélite) e satélites Intelsat sobre o Atlântico, bem como para o satélite Immarsat 2.
A data de criação de Yakima em simultâneo com a primeira geração de satélites Intelsat, assim como a missão geral do 544 Intelligence Group apontam para uma actividade de Yakima na vigilância global de comunicações. Um outro indício é a proximidade de Yakima de uma estação normal de recepção de satélite, situada 100 milhas a norte.

Sugar Grove, EUA (80°W, 39°N)
Sugar Grove foi fundada em simultâneo com a entrada em funcionamento da segunda geração de satélites Intelsat no final dos anos 70. Estão aqui estacionados o NAVSECGRU, assim como a AIA com o 544 Intelligence Group (Destacamento 3). Segundo as indicações de diversos autores, a estação dispõe de dez antenas de satélite, três das quais têm dimensões superiores a 18 metros (18,2 m, 32,3 m e 46 m) destinando-se claramente à intercepção de satélites de comunicações. Uma das missões do Destacamento 3 do 544 IG na estação é fornecer "Intelligence Support" para a recolha de informações de satélites de comunicações através das estações da Marinha.[50]
Além disso, Sugar Grove situa-se na proximidade (60 Milhas) da estação normal de recepção de satélites em Etam.

Sabana Seca, Porto Rico (66°W, 18°N)
Em 1952, a NAVSECGRU foi estacionada em Sabana Seca. Desde 1995, encontra-se aí também a AIA como o 544 IG (Destacamento 2). A estação dispõe, pelo menos, de uma antena de satélite com um diâmetro de 32 metros e outras 4 antenas de satélite de pequenas dimensões.

De acordo com as informações oficiais, a estação tem como missão o tratamento de comunicações por satélite ("performing satellite communication processing"), "cryptologic and communications service" assim como assistência à marinha e tarefas DoD (designadamente recolha de informações COMSAT (descrição do 544th IG)). Sabana Seca, deverá tornar-se, no futuro a primeira estação de campo para a análise e o processamento de comunicações por satélite.

Morwenstow, Reino Unido (4°W, 51°N)
Morwenstow foi, tal como Yakima, fundada em simultâneo com a primeira geração de satélites Intelsat, no início dos anos 70. Morwenstow é operada pelo Serviço de Informações britânico (GCHQ). Em Morwenstow encontram-se cerca de 21 antenas de satélite, três das quais com um diâmetro de 30 metros; sobre as dimensões das restantes antenas, não existem quaisquer informações. Quanto à missão da estação, nada se sabe de fonte oficial, mas as dimensões e o número de antenas de satélite, assim como a sua localização a uma distância de apenas 110 quilómetros da estação Telekom em Goonhilly não deixam qualquer dúvida de que tem como missão interceptar satélites de comunicações.

Menwith Hill, Reino Unido (2°W, 53°N)
Menwith Hill foi fundada em 1956, em 1974 existiam já 8 antenas de satélite. Entretanto, estão aí instaladas cerca de 30 antenas de satélite, 12 das quais com um diâmetro superior a 20 metros. Pelo menos uma das grandes antenas, mas seguramente não todas, constitui uma antena de recepção de comunicação militar (AN/FSC-78). Em Menwith Hill, tem lugar uma cooperação entre serviços britânicos e americanos. Os norte-americanos estacionaram aí a NAVSECGRU, a AIA (451st IOS), assim como o INSCOM, que tem a seu cargo o comando da estação. O terreno em que se encontra Menwith Hill pertence ao Ministério britânico da Defesa e está alugado ao governo norte-americano. De acordo com informações oficiais, Menwith Hill tem como missão "to provide rapid radio relay and to conduct communications research". Segundo Richelson e a Federação dos Cientistas Americanos, Menwith Hill é tanto estação terrestre para satélites de espionagem como estação terrestre de intercepção para satélites de comunicações russos.

[50] „It provides enhhanced intelligence support to Air Force operational commanders and other consumers of communications satellite information collected by Navy-commanded filed stations." Homepage do (44th Intelligence Group http://www.aia.af.mil

Geraldton, Austrália (114°O, 28°S)
A estação existe desde o início dos anos 90. A direcção da estação está confiada aos serviços secretos australianos (DSD), e os ingleses anteriormente estacionados em Hong Kong (ver supra) apenas pertencem ao pessoal da estação. Segundo Hager, quatro antenas de satélite de igual dimensão (diâmetro de cerca de 20 metros), estão orientadas para satélites sobre o Oceano Índico e para satélites sobre o Pacífico.
Segundo informações fornecidas por um perito sob juramento no Parlamento australiano, em Geraldton são interceptados satélites de comunicações civis.[51]

Pine Gap, Austrália (133°O, 23°S)
A estação de Pine Gap foi fundada em 1966. A direcção está confiada aos serviços secretos australianos (DSD); aproximadamente metade das cerca de 900 pessoas aí estacionadas são americanos da CIA e do NAVSECGRU.[52]
Pine Gap dispõe de 18 antenas de satélite, das quais uma com cerca de 30 metros e uma com cerca de 20 metros de diâmetro. De acordo com informações oficiais, bem como indicações de diversos autores, a estação é, desde o início, uma estação terrestre para os satélites SIGINT. A partir da estação, são controlados e dirigidos diversos satélites de espionagem, sendo os seus sinais recebidos, processados e analisados. As antenas de satélite de grandes dimensões apontam também para a intercepção de satélites de comunicações, uma vez que, para os satélites SIGINT, não são necessárias antenas de satélite de grandes dimensões. Até 1980, os australianos estavam excluídos do Departamento de Análise de Sinais, desde então têm acesso livre a todos os departamentos, exceptuando a sala de criptografia dos americanos.

Misawa, Japão (141°O, 40°N)
A estação de Misawa foi construída em 1948 para uma antena HFDF. Estão aí estacionados japoneses e americanos. Do lado norte-americano, encontram-se aí NAVSECGRU, INSCOM, assim como alguns grupos da AIA (544th IG, 301st IS,). No terreno, encontram-se cerca de 14 antenas de satélite, das quais algumas com um diâmetro de cerca de 20 metros (cálculo). Misawa serve oficialmente de "Cryptology Operations Center". Segundo Richelson, em Misawa são interceptados os satélites russos Molnyia, assim como outros satélites de comunicações russos.

Waihopai, Nova Zelândia (173°O, 41°S)[53]
Waihopai existe desde 1989. Desde essa data, existe uma grande antena com um diâmetro de 18 metros, tendo sido ulteriormente construída uma segunda. Segundo Hager, as antenas estão orientadas para Intelsat 701 sobre o Pacífico. Segundo indicações oficiais do GCSB ("General Communications Security Bureau"), a estação de Waihopai tem como missão a intercepção de satélites de comunicações, bem como a desincriptação e o processamento dos sinais[54].

---

[51] Proof Committee Hansard, Joint Standing Committee on Treaties, Reference: Pine Gap, 9 August 1999, Canberra; http://www.aph.gov.au/hansard

[52] Proof Committee Hansard, Joint Standing Committee on Treaties, Reference: Pine Gap, 9 August 1999, Canberra; http://www.aph.gov.au/hansard

[53] Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet "Securing our Nation's Safety", Dezembro 2000, http://www.dpmc.govt.nz/dess/securingoursafety/index.html

[54] Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet: "Securing our Nations Safety", Dezembro 2000, http://www.dpmc.govt.nz/dess/securingoursafety/index.html: "In 1989, [...] the GCSB opened its satellite communications interception station at Waihopai, near Blenheim. [...] The signals intelligence is obtained from a variety of foreign communications and other non-communications signals, such as radar. The GCSB not only intercepts the signals, it also processes, decrypts or decodes and/or translates the information the signals contain before passing it on as a report to the appropriate Minister or government department."

Uma vez que a estação apenas dispõe de duas antenas de satélite, os serviços secretos neozelandeses apenas podem captar uma parte restrita das comunicações na região do Pacífico. Assim, a estação só se reveste de utilidade em correlação com uma outra sita no mesmo espaço. Hager refere frequentemente a estação de Geraldton, na Austrália, como „estação geminada“ de Waihopai[55].

Hong Kong (22°N, 114°O)
A estação foi criada no fim dos anos 70, em simultâneo com a segunda geração INTELSAT e estava equipada com grandes antenas de satélite. Não existem quaisquer informações sobre as dimensões exactas. Em 1994, a estação de Hong Kong começou a ser desactivada e as antenas foram transportadas para a Austrália. É incerto qual das estações herdou as tarefas de Hong Kong: Geraldton, Pine Gap ou ainda Misawa, no Japão.
Eventualmente, as tarefas foram distribuídas por diversas estações.

5.3.2.3.2. Outras estações

No caso das seguintes estações, os critérios enunciados não permitem provar claramente a sua missão:

Leitrim, Canadá (75°W, 45°N)
Leitrim é parte de um programa de intercâmbio entre unidades militares canadianas e norte americanas. De acordo com informações da Marinha, estão estacionadas em Leitrim, cerca de 30 pessoas. Em 1985, foi instalada a primeira de quatro antenas de satélite, das quais apenas têm um diâmetro de cerca de 12 metros (cálculo). Segundo informações oficiais, a estação tem como missão "Cryptologic rating" e a intercepção de comunicações diplomáticas.

Bad Aibling, Alemanha (12°O, 47°N)
Na estação situada na proximidade de Bad Aibling trabalham actualmente cerca de 750 americanos. Em Bad Aibling estão estacionados o INSCOM (66th IG, 718 IG), que detém o comando, o NAVSECGRU, assim como diversos grupos da AIA (402nd IG, 26th IOG). Encontram-se aí 14 antenas de satélite, das quais nenhuma tem um diâmetro superior a 18 metros. De acordo com informações oficiais, Bad Aibling tem as seguintes tarefas: “Rapid Radio Relay and Secure Commo, Support to DoD and Unified Commands, Medium and Longhand Commo HF& Satellite, Communication Physics Research, Test and Evaluate Commo Equipment”. Segundo Richelson, Bad Aibling é estação terrestre para satélites SIGINT e estação de intercepção para satélites de comunicações russos. Em 30 de Setembro de 2002, a estação deverá, em conformidade com a decisão do „Department of Defense“, ser encerrada. O pessoal deverá ser afectado a outras unidades[56].

Ayios Nikolaos, Chipre (32°O, 35°N)
Ayios Nikolaos em Chipre é uma estação britânica. As tarefas da estação equipada com 14 antenas de satélite, cujas dimensões são desconhecidas, estão distribuídas por duas unidades, designadamente "Signals Regiment Radio" e (RAF). A localização de Agios Nikolaos na proximidade dos Estados árabes e o facto de Ayios Nikolaos ser a única estação dentro de alguns

[55] *Nicky Hager,* Secret Power. New Zealands´s Role in the International Spy Network, Craig Potton Publishing (1996), 182

[56] Comunicação de 31.5.2001, na *Homepage* do INSCOM, http://www.vulcan.belvoir.army.mil/bas_to_close.asp http://www.vulcan.belvoir.army.mil/bas_to_close.asp

raios de acção ("spot-beams") nesta região apontam para um papel importante desta estação na recolha de informações.

Shoal Bay, Austrália (134°O, 13°S)
Shoal Bay é uma estação operada apenas pelo Serviço de Informações Australiano. A estação dispõe, ao que parece, de 10 antenas de satélite, cujas dimensões não são descritas em detalhe. Das antenas de satélite que figuram nas fotografias, as 5 maiores têm um diâmetro máximo de 8 metros, a sexta visível é ainda mais pequena. Segundo Richelson, as antenas estão orientadas para os satélites indonésios PALAPA. Não é possível concluir se a estação faz parte do sistema global de intercepção de comunicações civis.

Guam, Pacífico (144°O, 13°S)
Guam existe desde 1898. Hoje, encontra-se aí uma "Naval Computer and Telecommunication Station", na qual está estacionado o 544th IG da AIA, assim como soldados da Marinha. Existem na estação, pelo menos, 4 antenas de satélite, duas das quais apresentam um diâmetro de cerca de 15 metros.

Kunia, Hawai (158°W, 21°N)
Esta estação é, desde 1993, um "Regional Security Operation Center" (RSOC), operada pelo NAVSECGRU e a AIA. As suas tarefas incluem o fornecimento de informações e comunicação, assim como apoio criptológico. A função de Kunia é incerta.

Buckley Field, EUA, Denver Colorado (104°W, 40°N)
A estação foi criada em 1972, encontrando-se aí estacionado o 544th IG (Det. 45). No terreno, erguem-se, pelo menos, 5 antenas de satélite, 4 das quais têm um diâmetro de cerca de 20 metros. A missão oficial da estação consiste em recolher, seleccionar e analisar dados sobre fenómenos nucleares obtidos por satélites SIGINT.

Medina Annex, EUA Texas (98°W, 29°N)
Medina é, tal como Kunia, um "Regional Security Operation Center", fundado em 1993 e operado pelo NAVSECGRU e unidades da AIA com missões nas Caraíbas.

Fort Gordon (81°W, 31°N)
Fort Gordon é igualmente um "Regional Security Operation Center", operado pelo INSCOM e AIA (702nd IG, 721st IB, 202nd IB, 31st IS), com tarefas incertas.

Fort Meade, EUA (76°W, 39°N)
Fort Meade é o quartel general da NSA.

5.3.3. Síntese dos resultados

Dos dados recolhidos sobre as estações e os satélites e com base nos pressupostos atrás descritos, é possível tirar as seguintes conclusões:
1. Em cada raio de acção, existem estações de intercepção para pelo menos alguns dos "global-beams", equipadas com, pelo menos, uma antena com um diâmetro de 20 metros; as estações são operadas por americanos ou ingleses, e americanos ou ingleses exercem aí actividades de serviços de informação.
2. O desenvolvimento da comunicação INTELSAT e a criação simultânea das respectivas estações de intercepção são uma prova da orientação global do sistema.

3. Algumas destas estações têm por missão, segundo descrição oficial, interceptar satélites de comunicações.
4. As indicações constantes dos documentos desclassificados devem ser consideradas como constituindo uma prova da existência das estações aí mencionadas.
5. Algumas estações estão situadas simultaneamente em "beams" e/ou "spots" de diversos satélites, pelo que é possível interceptar uma grande parte das comunicações.
6. Existem outras estações que não dispõem de antenas de grandes dimensões, mas podem ser parte do sistema, uma vez que podem receber comunicações dos "beams" e dos "spots". Neste caso, há que renunciar ao indício das dimensões da antena e procurar outros indícios.
7. Algumas das estações mencionadas situam-se comprovadamente na proximidade imediata de estações terrestres regulares de satélites de comunicações.

5.4. O Acordo UKUSA

Por Acordo UKUSA entende-se um acordo SIGINT assinado em 1948 entre a Grã-Bretanha (United Kingdom, UK), os Estados Unidos (USA), bem como a Austrália, o Canadá e a Nova Zelândia.

5.4.1. A evolução histórica do Acordo UKUSA[57]

O Acordo UKUSA constituiu a continuação da estreita cooperação já existente durante a Segunda Guerra Mundial entre os Estados Unidos e a Grã-Bretanha, cooperação essa já indiciada durante a Primeira Guerra Mundial.

A iniciativa de criação de uma aliança SIGINT surgiu em Agosto de 1940, no âmbito de um encontro entre Americanos e Britânicos, que teve lugar em Londres, iniciativa essa tomada pelos Americanos[58]. Em Fevereiro de 1941, os criptoanalistas norte-americanos forneceram à Grã-Bretanha uma máquina de encriptação (PURPLE). Na Primavera de 1941, teve início a cooperação criptoanalítica.[59] A cooperação em matéria de serviços de informações foi reforçada graças à intervenção comum das Armadas no Atlântico Norte, no Verão de 1941. Em Junho de 1941, os Britânicos conseguiram decifrar o código da armada alemã ENIGMA.

A intervenção da América na Guerra contribuiu para um novo reforço da cooperação SIGINT. Em 1942, os criptoanalistas norte-americanos da "Naval SIGINT Agency" começaram a operar na Grã-Bretanha.[60] A comunicação entre as salas de controlo dos submarinos em Londres,

---

[57] *Christopher Andrew*, "The making of the Anglo-American SIGINT Alliance" in *Hayden B.*, *Peake, Samuel Halpern* (Eds), In the Name of Inteligence. Essays in Honor of *Walter Pforzheimer*, (NIBC Press 1994) pp. 95 -109

[58] *Christopher Andrew, "*The making of the Anglo-American SIGINT Alliance", ibidem, p. 99: „At a metteing in London on 31 August 1940 between the British Chiefs of Staff and the American Military Observer Mission, the US Army representative, Brigadier General George V. Strong, reported that ´it had recently been arranged in principle between the British and the United States Governments that periodic exchange of information would be desirable,´ and said that ´the time had come or a free exchange of intelligence´. (COS (40)289, CAB 79/6, PRO. *Smith*, The Ultra Magic Deals, pp. 38, 43-4. *Sir F.H. Hinsley*, et al., British Intellgence in the Second World War, Vol.I, pp.312 e segs.)

[59] *Christopher Andrew, "*The making of the Anglo-American SIGINT Alliance", ibidem, p. 100: „ In the spring of 1941, Steward Menzies, the Chief of SIS, appointed an SIS liason officer to the British Joint Services Missin in Washington, Tim O´Connor, …, to advice him on cryptologic collaboration" (

[60] *Christopher Andrew, "*The making of the Anglo-American SIGINT Alliance", ibidem, p. 100 (*Sir F.H. Hinsley*, et al., British Intellgence in the Second World War, Vol II, p.56)

Washington, e, a partir de Maio de 1943, em Otava, no Canadá, tornou-se tão estreita que trabalhavam, segundo declaração de um dos intervenientes de então, como uma única organização.[61]

Na Primavera de 1943, foi assinado o acordo BRUSA-SIGINT, tendo igualmente tido lugar um intercâmbio pessoal. O conteúdo do acordo reporta-se, designadamente, à repartição nas actividades e encontra-se resumido nas suas primeiras três frases: intercâmbio de todas e quaisquer informações relacionadas com a descoberta, identificação e escuta de sinais, bem como decifragem e encriptação. Os Americanos eram fundamentalmente responsáveis pelo Japão, os Britânicos pela Alemanha e Itália[62] .

No pós-guerra, a iniciativa de manutenção de uma aliança SIGINT partiu essencialmente da Grã-Bretanha. A base para o efeito foi acordada aquando do périplo mundial efectuado por funcionários britânicos do serviço de informações (*inter alia*, Sir Harry Hinsley, cujos livros constituem a base do artigo citado) na Primavera de 1945. Um dos objectivos visados consistia em enviar pessoal SIGINT da Europa rumo ao Pacífico, para a guerra com o Japão. Neste contexto, foi acordado com a Austrália disponibilizar aos serviços australianos recursos e pessoal (britânicos). O regresso aos EUA foi feito passando pela Nova Zelândia e pelo Canadá.

Em Setembro de 1945, Truman assinava um memorando altamente confidencial, que constitui a pedra angular de uma aliança SIGINT em tempos de paz[63]. Seguidamente, foram entabuladas negociações entre os Britânicos e os Americanos sobre a conclusão do acordo. Para além disso, uma delegação britânica entrou em contacto com Canadianos e Australianos, no intuito de debater uma eventual participação. Em Fevereiro e Março de 1946, realizou-se uma conferência SIGINT anglo-americana altamente confidencial, tendente a discutir os pormenores. Os Britânicos tinham para o efeito recebido autorização dos Canadianos e Australianos. O resultado da conferência foi dado por um acordo secreto de cerca de 25 páginas, que selavam os pormenores de um acordo SIGINT, entre os Estados Unidos e a Commonwealth britânica. Nos dois anos subsequentes tiveram lugar outras negociações, tendo o texto definitivo, denominado Acordo UKUSA, sido assinado em Junho de 1948.[64]

---

[61] *Christopher Andrew, "*The making of the Anglo-American SIGINT Alliance", ibidem, p. 101 (*Sir F.H. Hinsley*, et al., British Intellgence in the Second World War, Vol. II, p 48)

[62] *Christopher Andrew, "*The making of the Anglo-American SIGINT Alliance", ibidem, p.101: Interivews mit Sir F.H. Hinsley, „Operations of the Military Intelligence Service War Department London (MIS WD London)," 11 June 1945, Tab A, RG 457 SRH-110, NAW

[63] Harry S. Truman, Memorandum for the Secretaries of the State, War and the Navy, 12 Sept. 1945: „The Secretary of War and the Secretary of the Navy are hereby authorised ti direct the Chief of Staff, U.S. Army and the Commander in Chief, U.S. Fleet; and Chief of Naval Oerations to continue collaboration in the field of communication intelligence between the United States Army and Navy and the British, and to extend, modify or discontinue this collaboration, as determined to be in the best interests of the United States." (*Bradley F. Smith*, The Ultra-Magic Deals and the Most Secret Special Relationship (Presidio 1993))

[64] *Christopher Andrew*, "The making of the Anglo-American SIGINT Alliance" in *Hayden*, *Peake and Samuel Halpern* (Eds), In the Name of Inteligence. Essays in Honor of *Walter Pforzheimer* (NIBC Press 1995) pp. 95 –109: Interviews with Sir Harry Hinsley, March/April 1994, who did a part of the negotiations; Interviews with Dr. Louis Tordella, Deputy Director of NSA from 1958 to 1974, who was present at the signing

5.4.2. Provas da existência do Acordo

5.4.2.1. Relatório anual 1999/2000 do "Intelligence and Security Committee"

Durante um longo período de tempo, não existiu qualquer reconhecimento oficial do acordo UKUSA por parte dos Estados signatários. No relatório anual do "Intelligence and Security Committee" inglês, órgão de controlo parlamentar do Reino Unido, o acordo UKUSA é, contudo, expressamente mencionado: "A qualidade da informação recolhida reflecte claramente o valor assumido pela estreita cooperação ao abrigo do acordo UKUSA. Esta tornou-se recentemente patente, quando o equipamento norte-americano da "National Security Agency" (NSA) colapsou e, durante três dias, quer a clientela norte-americana, quer a clientela britânica normal do GCHQ foram directamente servidas por este último[65].

5.4.2.2. Publicação do Gabinete do Primeiro-Ministro da Nova Zelândia

Também numa publicação emanada, no ano transacto, do Gabinete do Primeiro-Ministro da Nova Zelândia sobre a gestão dos serviços nacionais de segurança e de informações é feita referência expressa a essa cooperação: "As actividades do GCSB ("Government Communications Security Bureau") processam-se exclusivamente sob a direcção do Governo neozelandês. Não obstante, é o mesmo membro de uma parceria de cooperação internacional há muito existente em prol do intercâmbio de "intelligence" estrangeira e do aproveitamento comum das tecnologias de segurança das comunicações. Os outros membros da parceria são a "National Security Agency" (NSA) dos EUA o "Government Communications Headquarter" (GCHQ) do Reino Unido, o "Defence Signal Directorate" (DSD) da Austrália e o "Communications Security Establishment" (CSE) do Canadá. Este acordo propicia à Nova Zelândida consideráveis vantagens, e seria impossível ao país lograr, por si só, a eficácia desta parceria entre as cinco nações"[66]. Além disso, existem outras provas inequívocas da sua existência.

---

[65] Intelligence and Security Committee Annual Report 1999-2000. Presented to Parliament by the Prime Minister by Command of Her Majesty, November 2000, 8 Rz 14

Texto original: "The quality of intelligence gathered clearly reflects the value of the close co-operation under the UKUSA agreement. A recent illustration of this occurred when the US National Security Agency's (NSA) equipment accidentally failed and for some three days US customers, as well as GCHQ's normal UK customers, were served directly from GCHQ."

[66] Domestic and External Secretariat des Department of the Prime Minister and Cabinet von Neuseeland, Securing our Nation's Safety. How New Zealand manages its security and intelligence agencies (2000).

Texto original : "The operation of the GCSB is directed solely by the New Zealand Government. It is, however, a member of a long-standing collaborative international partnership for the exchange of foreign intelligence and the sharing of communications security technology. The other members of the partnership are the USA's National Security Agency (NSA), the UK's Government Communications Headquarters (GCHQ) Australia's Defence Signals Directorate (DSD), and Canada's Communications Security Establishment (CSE). New Zealand gains considerable benefit from this arrangement, as it would be impossible for New Zealand to generate the effectiveness of the five nation partnership on its own."

5.4.2.3. O anuário de acrónimos da Marinha

Segundo a marinha norte-americana[67], UKUSA constitui o acrónimo de "United Kingdom – USA" e designa um Acordo SIGINT entre 5 nações.

5.4.2.4. Declaração do Director do DSD

O Director do Serviço de Informações australiano (DSD) confirmou a existência do referido acordo no quadro de uma entrevista: de acordo com as informações por ele mesmo prestadas, os Serviços Secretos australianos cooperam com outros serviços de informações ultramarinos ao abrigo do Acordo UKUSA.[68]

5.4.2.5. Relatório do "Canadian Parliamentary Security and Intelligence Committee"

No relatório em epígrafe é referido cooperar o Canadá com alguns dos seus aliados mais antigos e mais próximos em matéria de serviços de informações. O relatório denomina esses aliados: os Estados Unidos (NSA), a Grã-Bretanha (GCHQ), a Austrália (DSD) e a Nova Zelândia (GCSB). O nome do acordo não é mencionado no relatório.

5.4.2.6. Declaração do ex-Director Adjunto da NSA, Dr. Louis Torella

No quadro de uma entrevista com Christopher Andrew, Professor da Universidade de Cambridge, em Novembro de 1987 e Abril de 1992, o ex-Director-Adjunto da NSA, Dr. Louis Torella, presente aquando da assinatura, confirmou a existência do acordo em causa.[69]

5.4.2.7. Carta do ex-Director do GCHQ, Joe Hooper

O então Director do GCHQ, Joe Hooper, refere numa carta de 22 de Julho de 1969 dirigida ao então Director da NSA Marechal S. Carter, o Acordo UKUSA.

5.4.2.8. Interlocutores do relator

O relator falou sobre o acordo em questão com várias pessoas que, por força das funções que exercem, deverão conhecer o Acordo UKUSA e o seu conteúdo. Nesse contexto, a natureza das respostas obtidas confirmou indirectamente, em todos os casos, a existência do mesmo.

---

[67] „Terms/Abbreviations/Acronyms“ publicado pela Marinha Norteamericana e pelo Nave and Marine Corps Intelligence Training Centre (NMITC) bei http://www.cnet.navy.mil/nmitc/training/u.html

[68] *Martin Brady*, Director do DSD, Carta de 16.3.1999 a Ross Coulthart, Sunday Program Channel 9

[69] *Christopher Andrew*, „The growth of the Australian Intelligence Community and the Anglo-American Connection“, pp. 223-4

5.5. Avaliação de documentos americanos que deixaram de ser considerados confidenciais

5.5.1. Natureza dos documentos

No âmbito do "Freedom of Information Acts" de 1966 (5 U.S.C. § 552) do Regulamento do Ministério da Defesa (DoD FOIA Regulamento 5400.7-R de 1997), documentos anteriormente classificados como secretos deixaram de o ser, tendo-se assim tornado acessíveis ao público.
O público pode ter acesso aos documentos por intermédio do "National Security Archive" instituído em 1985 (George Washington University, Washington D.C.). Jeffrey Richelson, ex-membro do "National Security Archives", transmitiu via Internet 16 documentos que veiculam uma ideia da génese, do desenvolvimento, da gestão e do mandato da NSA ("National Security Agency").[70] Além disso, dois dos documentos citam o nome ECHELON. Esses documentos são continuamente citados por diferentes autores de obras sobre o sistema ECHELON, e evocados como prova da existência do sistema de espionagem global ECHELON. Por outro lado, determinados documentos disponibilizados por Richelson confirmam a existência do NRO ("National Reconnaissance Office") e constatam que a sua missão consiste em gerir e em explorar os satélites de recolha de informações.[71] Após o encontro com Jeffrey Richelson, em Washington, este transmitiu à comissão outros documentos que deixaram de ser considerados confidenciais, entre os quais são igualmente tidos em conta, no presente documento, os que se revestem de relevância neste contexto.

5.5.2. Conteúdo dos documentos

Desses documentos constam descrições ou menções fragmentárias dos temas seguintes:

5.5.2.1 Missão e concepção do NSA (documentos 1, 2b, 4, 10, 16)

Na Directiva 9 do "National Security Council Intelligence Directive" (NSCID 9), de 10 de Março de 1950[72], a noção de comunicação externa é definida para fins de espionagem de comunicações (COMINT); assim, entende-se por **comunicação externa toda a comunicação governamental *lato sensu* (não unicamente militar), bem como toda e qualquer outra comunicação susceptível de conter informações de interesse militar, político, científico ou económico**.

A Directiva (NSCID 9 rev, de 9.12.1952)[73] estipula expressamente que o FBI é o único responsável pela segurança interna.

A Directiva do Ministério da Defesa, de 23 de Dezembro de 1971[74] (DoD), relativa à NSA e ao "Central Security Service" (CSS) define a natureza da NSA do seguinte modo:

---

[70] *Richelson, Jeffrey T.,* The National Security Agency Declassified, National Security Archive Electronic Briefing Book no. 24, George Washington University http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html
[71] *Richelson, Jeffrey T.,* The National Security Agency Declassified, National Security Archive Electronic Briefing Book no. 24, George Washington University http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB35/index.html

[72] Document 1. NSCID 9, "Communications Intelligence," March 10, 1950.

[73] Document 2b. National Security Council Intelligence Directive No. 9, Communications Intelligence, December 29, 1952.

[74] Document 4. Department of Defense Directive S-5100.20, "The National Security Agency and the Central Security Service," December 23, 1971.

- A NSA constitui um serviço distinto no seio do Ministério da Defesa, sob a tutela do Ministro da Defesa.
- A NSA assegura, por um lado, a missão SIGINT nos Estados Unidos, e disponibiliza, por outro a todos os ministérios e serviços sistemas de comunicação seguros.
- A actividade SIGINT da NSA não compreende a produção e a difusão de informações já tratadas. Essa tarefa recai no âmbito de competências de outros ministérios e serviços.

Por outro lado, a Directiva de 1971 apresenta, nas suas grandes linhas, a estrutura da NSA e do CSS.

Numa declaração feita em 12 de Abril de 2000[75] perante a "House Permanent Select Committee on Intelligence", o Director da NSA, Sr. Hayden descreve as missões da NSA como segue:
- a vigilância electrónica serve o objectivo de recolha das comunicações externas destinadas a militares e responsáveis políticos (dirigentes políticos);
- a NSA fornece aos consumidores governamentais americanos informações sobre o terrorismo internacional, os estupefacientes, a proliferação de armamento;
- a NSA não tem por missão recolher todas as comunicações electrónicas ;
- a NSA apenas pode transmitir informações a destinatários autorizados pelo Governo, não os podendo transmitir directamente às empresas americanas.

Num memorando do vice-almirante da Marinha Norte Americana, W.O. Studeman, estabelecido em nome do Governo, com data de 8 de Abril de 1992[76], é feita menção à missão crescentemente global ("access") da NSA, a par do "Support of military operations".

5.5.2.2. Poderes dos serviços de informações (Documento 7)[77]

Conclui-se da Directiva 18 "United States Signals Intelligence" (USSID 18) que, tanto os sinais transmitidos por cabo, como os sinais transmitidos via rádio, são interceptados.

5.5.2.3. Cooperação com outros serviços (Documentos 2a, 2b)

Entre as atribuições do "U.S. Communications Intelligence Board" figura, nomeadamente, a vigilância de todos os "arrangements" com os governos estrangeiros no domínio COMINT. O Director da NSA é também responsável por todos os contactos com os serviços COMINT estrangeiros[78].

5.5.2.4. Menção das unidades activas nos "Sites ECHELON" (Documentos 9 e 12)

As instruções C5450.48A[79] do NAVSECGRU descrevem o mandato, a função e o objectivo da "Naval Security Group Activity" (NAVSECGRUACT), o 544º "Intelligence Group" em Sugar

[75] Document 16. Statement for the Record of NSA Director Lt Gen Michael V. Hayden, USAF before the House Permanent Select Committee on Intelligence, April 12, 2000.

[76] Document 10. Farewell from Vice Admiral William O. Studeman to NSA Employees, April 8, 1992.

[77] Document 7. United States Signals Intelligence Directive [USSID] 18, "Legal Compliance and Minimization Procedures," July 27, 1993.

[78] Document 2a. Memorandum from President Harry S. Truman to the Secretary of State, the Secretary of Defense, Subject: Communications Intelligence Activities, October 24, 1952.

Document 2b. National Security Council Intelligence Directive No. 9, Communications Intelligence, December 29, 1952.

[79] Document 9. NAVSECGRU Instruction C5450.48A, Subj: Mission, Functions and Tasks of Naval Security Group Activity (NAVSECGRUACT) Sugar Grove, West Virginia, September 3, 1991.

Grove, Virginia Ocidental. Aí se indica que uma missão específica consiste em gerir e explorar um *site* ECHELON*;* uma outra missão citada reporta-se ao tratamento das informações procedentes dos serviços de informações.

No documento "History of the Air Intelligence Agency – 1 January to 31 December 1994"[80], é feita menção, no ponto "Activation of ECHELON Units", à "Air Intelligence Agency (AIA), Detachments 2 and 3:"

Os documentos não revelam em que consiste um "site ECHELON" , nem o que é feito num "site ECHELON", nem o que abrange o nome de código "ECHELON". Os documentos em questão não fazem qualquer referência ao Acordo UKUSA.

5.5.2.5. Menção das estações (Documentos 6, 9, 12, novos documentos)

- Sugar Grove, (Virgínia Ocidental), menção como estação SIGINT nas NAVSECGRU INSTRUCTIONs C5450.48A[81]
- Misawa Air Base, Japan, menção como estação SIGINT em "History of the Air Intelligence Agency - January to 31 December 1994" [82] e na descrição das actividades do "Naval Security Group" em documentos do „Department of the Navy" [83]
- Sabana Seca em Porto Rico, menção como estação SIGINT, ibidem, e na descrição das actividades do "Naval Security Group" em documentos do "Department of the Navy"[84]
- Guam, menção como estação SIGINT, ibidem
- Yakima, Washington, menção como estação SIGINT, ibidem
- Fort Meade, Maryland, um relatório COMINT da NSA emanado de Fort George G. Meade, Maryland, com data de 31 de Agosto de 1972, prova a existência de actividades COMINT no local em questão[85].
- Menwith-Hill, Reino Unido, descrição das actividades do "Naval Security Group" em documentos do "Department of the Navy"[86]
- Bad Aibling, Alemanha, descrição das actividades do "Naval Security Group" em documentos do "Department of the Navy"[87]
- Medina, Texas, descrição das actividades do "Naval Security Group" em documentos do "Department of the Navy"[88]
- Kunia, Hawaii, descrição das actividades do "Naval Security Group" em "Naval Security Group Instructions[89]

---

[80] Document 12. "Activation of ECHELON Units," from History of the Air Intelligence Agency, 1 January - 31 December 1994, Volume I (San Antonio, TX: AIA, 1995).

[81] Document 9. NAVSECGRU Instruction C5450.48A, Subj: Mission, Functions and Tasks of Naval Security Group Activity (NAVSECGRUACT) Sugar Grove, West Virginia, September 3, 1991.

[82] Document 12. "Activation of ECHELON Units," from History of the Air Intelligence Agency, 1 January - 31 December 1994, Volume I (San Antonio, TX: AIA, 1995).

[83] Department of the Navy, Naval Security Group Instruction C5450.32E vom 9.5.1996

[84] Naval Security Group Instruction C5450.33B vom 8.8.1996

[85] COMINT Report der NSA aus Fort George G. Meade, Maryland, de 31 de Agosto de 1972

[86] Department of the Navy, Fact and Justification Sheet for the Establishment of U.S. Naval Security Group Activity vom 23.2.1995 und Department of the Navy, Naval Security Group Instruction C5450.62 de 30.1.1996

[87] Department of the Navy, Naval Security Group Instruction C5450.63 de 25.10.1995

[88] Department of the Navy, Naval Security Group Instruction C5450.60A de 8.4.1996

[89] Naval Security Group Instruction C5450.55B de 8.8.1996

5.5.2.6. Protecção da vida privada dos cidadãos americanos (Documentos 7, 7a a f, 9, 11 e16)

Lê-se nas NAVSECGRU INSTRUCTIONs C5450.48A que cumpre assegurar a vida privada dos cidadãos[90].

Diferentes documentos explicam que a vida privada dos cidadãos norte-americanos deve ser protegida, indicando como fazê-lo (Baker, General Counsel, NSA, carta de 9 de Setembro de 1992, United States Signals Intelligence Directive (USSID) 18, 20 de Outubro de 1980, e diferentes suplementos[91].

5.5.2.7. Definições (Documentos 4, 5a,7)

A Directiva do Ministério da Defesa de 23 de Dezembro de 1971[92], bem como a Directiva nº 6 do "National Security Council Intelligence" de 17. de Fevereiro de 1972[93] estipulam definições precisas de SIGINT, COMINT, ELINT e TELINT.

De acordo com essas definições entende-se por COMINT a recolha e o tratamento das comunicações externas (encaminhadas por meios electromagnéticos), bem como a intercepção e o tratamento das comunicações escritas não encriptadas, da imprensa e para fins de propaganda, a não ser que seja encriptada.

5.5.3. Resumo

1. Já há 50 anos, as informações reputadas interessantes respeitavam a domínios, não só da política e da segurança, mas também da ciência e da economia.
2. Os documentos provam que a NSA colabora com outros serviços no domínio da COMINT.
3. Os documentos que fornecem informações sobre a organização da NSA, as missões desta última e os seus elos com o Ministério da Defesa não são verdadeiramente portadores de informações suplementares às procedentes de fontes de acesso público na "Homepage" da NSA.
4. A intercepção das comunicações por cabo é admissível.
5. O 544º "Intelligence group" e os "Detachments 2 e 3" da "Air Intelligence Agency" participam na recolha de informações dos Serviços Secretos.
6. O conceito "ECHELON" surge em diversos contextos.
7. Sugar Grove, na Virgínia Ocidental, Misawa Air Base no Japão, Porto Rico (i.e. Sabana Seca), Guam, Yakima (Estado de Washington) são designadas estações SIGINT.

---

[90] Document 9. NAVSECGRU Instruction C5450.48A, Subj: Mission, Functions and Tasks of Naval Security Group Activity (NAVSECGRUACT) Sugar Grove, West Virginia, September 3, 1991

[91] Dissemination of U.S. Government Organizations and Officials, Memorandum 5 February 1993; Reporting Guidance on References to the First Lady, 8 July 1993; Reporting Guidance on Former President Carter's Involvement in the Bosnian Peace Process, 15 December 1994; Understanding USSID 18, 30 September 1997; USSID 18 Guide 14 February 1998;
NSA/US IDENTITIES IN SIGINT, March 1994; Statement for the record of NSA Director Lt Gen. Michael V. Hayden, USAF, 12. April 2000)

[92] Document 4. Department of Defense Directive S-5100.20, "The National Security Agency and the Central Security Service," December 23, 1971

[93] Document 5a. NSCID 6, "Signals Intelligence," February 17, 1972.

8. Outras estações em que opera o "Naval Security Group" são objecto de menção, sem, no entanto, serem designadas como estações SIGINT.
9. Os documentos indicam como deve ser protegida a vida privada dos cidadãos americanos.

Os documentos não fornecem qualquer prova concreta, mas sim fortes indícios, que, conjuntamente com outros, permitem tirar ilações.

5.6. Informações divulgadas por autores especializados e jornalistas

5.6.1. Nicky Hager

O sistema ECHELON foi descrito em detalhe pela primeira vez no livro do autor neozelandês Nicky Hager "Secret Powers – New Zealand's role in the international spy network", publicado em 1996. O autor apoia-se em entrevistas efectuadas com mais de 50 pessoas que trabalharam no Serviço de Informações neozelandês GCSB ou que intervieram em actividades nesse domínio. Paralelamente, consultou numerosos documentos procedentes de arquivos nacionais, jornais e outras fontes de acesso público. Segundo Hager, o sistema de intercepção mundial é designado ECHELON, sendo os computadores da rede denominados "ECHELON Dictionaries".

De acordo com Hager, o início da cooperação entre os serviços de informações no quadro do acordo UKUSA remonta a 1947, quando, no prolongamento da sua cooperação durante a guerra, o Reino Unido e os EUA concluíram um acordo no sentido de prosseguirem à escala mundial as actividades COMINT. Os dois países propunham-se cooperar na criação de um sistema de intercepção mundial para o que compartilhariam as instalações especiais necessárias e os custos inerentes, tendo ambos acesso aos resultados. O Canadá, a Austrália e a Nova Zelândia aderiram subsequentemente ao acordo UKUSA.

Hager afirma que a intercepção das comunicações por satélite é a actividade nuclear do sistema **actual**. A intercepção por estações terrestres das mensagens enviadas através do Intelsat - o primeiro sistema mundial de comunicações por satélite[94]- começou nos anos 70. Essas mensagens eram então pesquisadas por computador através de palavras-chave e/ou endereços específicos a fim de filtrar as comunicações relevantes. A actividade de vigilância foi mais tarde alargada a outros satélites, como os de Inmarsat[95], que se concentra principalmente nas comunicações marítimas.
No seu livro, Hager indica que a intercepção das comunicações satélites representa apenas uma pequena parte, embora importante, do sistema global de intercepção. Paralelamente existiriam muitas outras instalações para vigiar as ligações por rádio e por cabo, embora estes aspectos estejam menos bem documentados e a sua existência seja mais difícil para provar, uma vez que, ao contrário das estações de terra, podem passar praticamente despercebidas. ECHELON é assim sinónimo de um sistema de intercepção mundial.

Na sua comunicação perante esta comissão, em 24 de Abril de 2001, Hager salientou que o sistema de intercepção não é omnipotente. Referiu que, dada a necessidade de aplicação tão eficaz quanto possível dos limitados recursos existentes, não é possível interceptar todas as comunicações, mas apenas as que são promissoras de informações importantes. Segundo Hager, os alvos são, por conseguinte, regra geral, os que revestem interesse político e diplomático.

[94] Ver http://www.intelsat.int/index.htm

[95] Ver http://www.inmarsat.org/index3.html

Frisou ainda que, quando o objectivo da intercepção consiste na obtenção de informações económicas, estão em causa mais propriamente interesses macro-económicos, e não micro-económicos.

No atinente ao *modus operandi* do sistema de intercepção, cada um dos parceiros possui listas próprias de termos de pesquisa, de acordo com os quais é interceptada a comunicação. Por outro lado, Hager afirma que a busca de comunicação se processa igualmente segundo palavras-chave que os EUA inserem no sistema mediante o denominado "dictionary manager". Assim, os Britânicos não terão, nomeadamente, qualquer controlo sobre essa situação, não sabendo igualmente que informações são recolhidas em Morwenstow, uma vez que estas são encaminhadas directamente para os EUA.

Neste contexto, Hager salientou o perigo que as estações de intercepção britânicas podem comportar para a Europa continental. Indicando vários exemplos, referiu que os parceiros UKUSA espionavam no Pacífico aliados e parceiros comerciais. Não abrangidos pelas acções de espionagem são, segundo Hager, exclusivamente os parceiros UKUSA. Em seu entender, os Serviços Secretos britânicos, à semelhança dos neozelandeses, não gostam de pôr em causa a parceria UKUSA, recusando-se a cooperar e a interceptar a Europa continental. Para a Grã-Bretanha não pode existir, segundo o mesmo, qualquer razão para prescindir de informações interessantes dos serviços secretos e, na medida em que as mesmas são sempre secretas, a espionagem no quadro de Acordo UKUSA não exluiria uma política oficial de lealdade para com a Europa.

5.6.2. Duncan Campbell

O jornalista britânico Duncan Campbell apoia-se, nas suas inúmeras publicações, nos trabalhos de Hager e Richelson, bem como em entrevistas com ex-colaboradores dos serviços de informações e noutras pesquisas. De acordo com as suas declarações, ECHELON constitui a parte do sistema de intercepção mundial que intercepta e processa comunicações internacionais por satélite. Todos os Estados-Membros dispõem de um "Dictionary" Computer", que faz a busca de notícias interceptadas segundo palavras-chave.

No Estudo 2/5 do STOA, de 1999, que fornece uma análise detalhada dos aspectos técnicos, Duncan Campbell descreveu em pormenor como qualquer meio utilizado para fins de comunicação pode ser interceptado. Num dos seus últimos escritos, contudo, afirma que mesmo ECHELON tem os seus limites e que a opinião inicial de que seria possível o controlo total das comunicações se revelou errónea. Segundo diz, nem ECHELON nem o sistema de espionagem electrónica (‘sigint') de que faz parte podem assegurar um controlo dessa ordem. Nem sequer existe equipamento com capacidade para processar e reconhecer o conteúdo de todas as mensagens orais ou chamadas telefónicas.[96]

Na sua alocução, perante a comissão, em 22 de Janeiro de 2001, Campbell sustentou que os EUA utilizam os serviços de informações para apoiar empresas norte-americanas no quadro da obtenção de contratos. Segundo o mesmo, através da CIA e com o apoio do "Advocacy Center" e do "Office of Executive Support im Department of Commerce" são transmitidas às empresas informações relevantes. Em apoio da tese sustentada, Campbell apresentou documentos que

[96] Duncan Campbell, Inside ECHELON. The history, structure and function of the global surveillance system known as ECHELON, 1 http://www.heise.de/tp/deutsch/special/ech/6928/1.html

permitem concluir da intervenção do "Advocacy Centers" em benefício de empresas norte-americanas, informação essa que, aliás, se encontra, quase na íntegra, também na "Homepage" do "Advocacy Centers".[97] O argumento segundo o qual o êxito das acções de intercepção do "Advocacy Center" acusa uma regressão constitui mera especulação, não podendo ser inferido dos documentos existentes.

Campbell salientou, no quadro da sua comunicação, que as capacidades de intercepção de vários países europeus aumentaram consideravelmente nos últimos anos, nomeadamente, na Suíça, Dinamarca e na França e que se registará igualmente um aumento da cooperação bilateral e multilateral no sector dos serviços de informações.

5.6.3. Jeff Richelson

O autor norte-americano Jeffrey Richelson, ex-membro do „National Security Archives", disponibilizou em Internet 16 documentos anteriormente classificados que dão uma visão da origem, evolução, gestão e mandato da NSA (National Security Agency)[98].

Além disso, Richelson é autor de diversos livros e artigos sobre actividades de espionagem dos EUA. Nos seus trabalhos, baseia-se em inúmeros documentos que deixaram de ser confidenciais, no trabalho de investigação de Hager, bem como em investigações que ele próprio levou a efeito. Aquando do seu encontro com a delegação da comissão em Washington D.C., em 11 de Maio de 2001, declarou que ECHELON designa uma rede informática com base na qual são filtrados dados que são intercambiados entre os serviços de informações.

No seu livro "The Ties That Bind"[99], publicado em 1985, o autor descreve em pormenor a origem do acordo UKUSA e a actividade dos serviços de espionagem dos EUA, do Reino Unido, Canadá, Austrália e Nova Zelândia que nele participam.

No seu vastíssimo livro "The U.S. Intelligence Community"[100], de 1999, o autor fornece um panorama sobre as actividades dos serviços de informação dos EUA, descreve as estruturas organizativas dos serviços, bem como os seus métodos de recolha e análise da informação. No capítulo 8 desse livro aborda em pormenor as capacidades SIGINT dos serviços de informação e descreve algumas estações terrestres. No capítulo 13 descreve as relações dos EUA com outros serviços de informação, nomeadamente o acordo UKUSA.

No artigo "Desperately seeking Signals"[101], que publicou em 2000, descreve brevemente o conteúdo do acordo UKUSA, refere instalações de escuta de satélites de comunicação e indica as possibilidades e limites da escuta das comunicações civis.

---

[97] Homepage do Advocay Centers, http://www.ita.doc.gov/td/advocacy/index.html

No quadro da sua visita a Washington DC, o relator propôs-se dar ao "Advocacy Center" a oportunidade de se pronunciar sobre as acusações em causa. O encontro agendado para o efeito foi, no entanto, cancelado, a curto prazo, pelo "Commerce Department Center".

[98] *Jeffrey T.Richelson,* The National Security Agency Declassified, National Security Archive Electronic Briefing Book no. 24, George Washington University, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html

[99] *Jeffrey T. Richelson, Desmond Ball* : The Ties That Bind, Boston UNWIN HYMAN (1985)

[100] *Jeffrey T. Richelson, Desmond Ball,* The Ties That Bind, Boston UNWIN HYMAN (1985)

[101] *Jeffrey T. Richelson,* Desperately Seeking Signals, The Bulletin of the Atomic Scientists, Vol. 56, No. 2/2000, 47-51, http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html

5.6.4. James Bamford

O autor norte-americano James Bamford, que fundamenta os seus trabalhos tanto em investigações levadas a cabo em arquivos, como na interpelação de colaboradores dos serviços de informações, foi uma das primeiras pessoas que se ocuparam com a actividade SIGINT da NSA. Já em 1982, publicava o livro intitulado "The Puzzle Palace"[102], cujo capítulo 8 "Partners" descreve circunstanciadamente o Acordo UKUSA. De acordo com o seu novo livro "Body of Secrets"[103], que assenta em conhecimentos expostos no "Puzzle Palace", a rede informática que estabelece a ligação entre os serviços de informações, é denominada "Plataforma". Por seu turno, ECHELON designará o "software" utilizado em todas as estações, que permite um processamento uniforme e um acesso directo aos dados[104]. Nos últimos capítulos, Bamford utiliza, contudo, a designação "ECHELON" igualmente para o sistema de intercepção no quadro do Acordo UKUSA.

Na obra "Body of Secrets" e, designadamente, no capítulo que, no presente contexto, se reveste do maior interesse, "Muscle", Bambord veicula uma panorâmica da evolução histórica da vigilância das comunicações por parte da NSA, bem como uma descrição do poder do sistema, do *modus operandi* da parceria UKUSA e dos respectivos objectivos. Frisa o mesmo que as entrevistas com dezenas de actuais e ex-funcionários do NSA permitem concluir que este organismo se não encontra actualmente envolvido em actividades de espionagem da concorrência.

Esta declaração foi pelo mesmo confirmada na sua audição perante a comissão ECHELON, realizada em 23 de Abril do ano em curso. A instrumentalização da NSA para fins de espionagem da concorrência exigiria uma decisão política unívoca ao mais alto nível, decisão essa que, até à data, não foi tomada. De acordo com o autor, os seus 20 anos de actividade de investigação não lhe permitiram obter qualquer prova de que a NSA transmite informações secretas às empresas norte-americanas, ainda que intercepte empresas privadas, nomeadamente, para fins de verificação da observância de embargos.

Segundo declarações proferidas por Bamford, o problema fundamental para a Europa não reside na questão de saber se o sistema ECHELON furta segredos empresariais e os transmite à concorrência, mas sim na violação do direito fundamental à vida privada. Na sua obra intitulada "Body of Secrets" descreve pormenorizadamente como se desenvolveu a protecção de "US persons" (ou seja, cidadãos dos EUA e pessoas que aí residem legalmente) e refere que também para outros "UKUSA-residents" existem, pelo menos, restrições internas. Simultaneamente, refere a inexistência de protecção para outras pessoas, não se observando sequer qualquer obrigatoriedade de eliminação dos dados e especifica ainda que as capacidades de armazenamento da NSA são incomensuráveis.

Bamford assinala também, porém, as fronteiras do sistema, as quais resultam, por um lado, do facto de apenas uma parte diminuta da comunicação internacional se processar por satélite e de os cabos de fibra óptica serem de muito mais difícil intercepção, e, por outro lado do facto de a

---

[102] *James Bamford,* The Puzzle Palace, Inside the National Security Agency, America's most secret intelligence organization (1983)

[103] *James Bamford,* Body of Secrets. Anatomy of the Ultra-Secret National Security Agency. From the Cold War Through the Dawn of a New Century, Doubleday Books (2001)

[104] *James Bamford,* Body of Secrets. Anatomy of the Ultra-Secret National Security Agency. From the Cold War Through the Dawn of a New Century, Doubleday Books (2001), 404.

NSA apenas dispor de capacidades restritas de avaliação final, sendo que a tal se contrapõe um fluxo permanentemente crescente de comunicações, sobretudo via Internet.

5.6.5. Bo Elkjaer e Kenan Seeberg,

Estes dois jornalistas dinamarqueses declararam perante a comissão, em 22 de Janeiro de 2001, que ECHELON estava já muito avançado nos anos 80 e que a Dinamarca, que, na última década, incrementou consideravelmente as suas capacidades de intercepção, coopera com os EUA desde 1984.

Tal como já observado num artigo publicado no Ekstra Bladet[105], no qual se reportam a uma comunicação feita com base numa apresentação de diapositivos (25) por um oficial do "544th Intelligence Group" da "Air Intelligence Agency", cujo nome é omitido, referem os autores que também diversas ONG (*inter alia,* a Cruz Vermelha) representam objectivos ECHELON.

5.7. Declarações de antigos colaboradores dos serviços de informações

5.7.1. Margaret Newsham (ex-colaboradora da NSA)[106]

Margaret Newsham foi empregada, entre 1974 e 1984, de Ford & Lockheed e declara ter trabalhado para a NSA nesse período. Afirma que foi treinada para essa actividade no quartel general da NSA em Fort George Meade, Maryland, EUA, e afectada, entre 1977 e 1981, a Menwith Hill, a estação terrestre dos EUA em território britânico. Ali teve ocasião de assistir à intercepção de uma conversa do Senador Strohm Thurmond . A partir de 1978, ECHELON era capaz de interceptar mensagens de telecomunicações de uma dada pessoa através do satélite.

Com respeito ao seu papel na NSA, esclareceu que era responsável por elaborar sistemas e programas, configurá-los e torná-los operacionais em grandes computadores. Os programas de "software" chamavam-se SILKWORTH e SIRE, enquanto ECHELON era o nome da rede.

5.7.2. Wayne Madsen (ex-colaborador da NSA)

Wayne Madsen[107] , ex-colaborador da NSA, confirma igualmente a existência de ECHELON. Em sua opinião a recolha de informação económica tem prioridade superior e é utilizado para proporcionar vantagens às empresas dos EUA. Receia nomeadamente que ECHELON possa ter espiado ONG como a Amnistia Internacional ou Greenpeace. Argumenta que a NSA teve que admitir que detinha mais de 1000 páginas de informações sobre a Princesa Diana, porque a sua conduta era negativa para a política dos EUA, devido à sua campanha contra as minas terrestres.

---

[105] *Bo Elkjaer, Kenan Seeberg,* ECHELON singles out the Red Cross, A bombshell in the surveillance scandal: The organization is a possible surveillance target, Ekstra Bladet, Denmark, 8.3.2000, http://cryptome.org/echelon-red.htm

[106] *Bo Elkjaer, Kenan Seeberg*, ECHELON was my baby – Interview with Margaret Newsham, Ekstra Bladet, 17.1.1999

[107] Entrevista à NBC "60 Minutes", 27.2.2000; http://cryptome.org/echelon-60min.htm

Aquando do encontro com a delegação da comissão, em Washington DC, manifestou particular preocupação relativamente ao perigo que o sistema mundial de espionagem representa para a esfera privada dos cidadãos europeus.

5.7.3. Mike Frost (ex-colaborador dos serviços secretos canadianos)

Mike Frost trabalhou mais de 20 anos para o CSE[108], os serviços secretos canadianos. A estação de escuta em Ottawa era apenas um elemento de uma rede mundial de estações de espionagem[109]. Numa entrevista à CBS disse que, em todo o mundo, todos os dias, conversas telefónicas, correios electrónicos e fax são controlados por ECHELON, uma rede secreta de vigilância do governo[110]. Também as comunicações civis são interceptadas. Numa entrevista que deu a um canal australiano de TV, citou como exemplo o facto de o CSE ter inscrito realmente o nome e número de telefone de uma mulher numa base de dados sobre possíveis terroristas porque esta utilizara uma frase ambígua num telefonema inofensivo a um amigo. Ao pesquisar as comunicações interceptadas, o computador tinha encontrado a palavra-chave e tinha reproduzido a conversação. O analista não tinha a certeza de como actuar e registou por conseguinte os seus dados pessoais.[111]

Os serviços de informações dos países UKUSA entreajudam-se, espiando por contra de outro, de modo que não pudessem ser acusados de nada os serviços de informações locais. Por exemplo, o GCHQ britânico teria pedido ao CSE que espiasse dois ministros do governo britânico quando a Primeira Ministra Thatcher quis saber se estavam do seu lado[112].

5.7.4. Fred Stock (ex-colaborador dos serviços secretos canadianos)

Fred Stock diz que foi expulso em 1993 do serviço secreto canadiano CSE, porque tinha criticado a nova orientação que dava maior ênfase às sobre a informações económicas e a objectivos civis. As comunicações interceptadas continham informação sobre o comércio com outros países, inclusive sobre as negociações relativas à NAFTA, à compra de cereais pela China e às vendas de armas francesas. Segundo Stock, o serviço recolhia também regularmente informações referentes aos protestos ambientais por embarcações de Greenpeace em alto mar[113].

5.8. Informações de fontes governamentais

5.8.1. Estados Unidos da América

James Woolsey, ex-director da CIA, declarou, numa conferência de imprensa[114] que deu a pedido do Departamento de Estado, que os EUA conduziam operações de espionagem na Europa

[108] Communication Security Establishment, sob tutela do Ministério da Defesa canadiano, opera SIGINT

[109] Entrevista à NBC "60 Minutes", 27.2.2000; http://cryptome.org/echelon-60min.htm

[110] Rötzer, Die NSA geht wegen ECHELON an die Öffentlichkeit;

http://www.heise.de/bin/tp/issue/download.cgi?artikelnr=6633&rub_ordner=special

[111] Entrevista à NBC "60 Minutes", 27.2.2000; http://cryptome.org/echelon-60min.htm

[112] Entrevista ao "Canal 9" australiano em 23.3.1999;

http://www.geocities.com/CapitolHill/Senate/8789/sunday1.htm

[113] *Jim Bronskill,* Canada a key snooper in huge spy network, Ottawa Citizen, 24.10.2000, http://www.ottawacitizen.com/national/990522/2630510.html

[114] James Woolsey, Remarks at the Foreign Press Center, Transcript, 7.3.2000, http://cryptome.org/echelon-cia.htm

continental. Contudo, 95% das informações económicas terão sido obtidos mediante a exploração de fontes de informação públicas, e apenas 5% proviria de segredos roubados. A espionagem incide sobre as informações económicas de outros países nos casos relacionados com as sanções e as mercadorias de dupla utilização, e a fim de combater a corrupção em matéria de concessão de contratos. Tal informação, contudo, não é facultada às empresas dos EUA. Woolsey sublinhou que, mesmo que a espionagem tornasse as informações economicamente úteis, um analista gastaria muito tempo a analisar o grande volume de informação disponível, e que seria irracional perder tempo a espionar parceiros comerciais amigos. Observou ainda que, mesmo que assim procedessem, tendo em conta as complexas interdependências internacionais, seria difícil saber que empresas são empresas norte-americanas a quem se deveria permitir obter essa informação.

5.8.2. Reino Unido

As respostas a várias questões colocadas na Câmara dos Comuns[115] revelam que a estação da RAF de Menwith Hill dependo do Ministério inglês da Defesa, mas é colocada à disposição do Departamento de Defesa dos EUA, especificamente da NSA[116], sendo um elemento desta o chefe da estação[117], como instalação de comunicações[118]. Em meados de 2000, operavam em Menwith Hill 415 militares americanos, 5 militares britânicos, 989 civil americanos e 392 civis britânicos, sem contar o pessoal GCHQ presente no local.[119] A presença de pessoal militar dos EUA rege-se pelo Tratado do Atlântico Norte e por acordos administrativos especiais confidenciais[120] considerados compatíveis com as relações que existem entre os governos do Reino Unido e dos EUA para objectivos de defesa comum[121]. A estação é parte integrante da rede mundial do Departamento norte-americano da Defesa que defende os interesses do Reino Unido, dos EUA e da OTAN.[122]

No relatório anual de 1999/2000, é destacado expressamente o valor da estreita cooperação desenvolvida no âmbito do acordo UKUSA e a qualidade da informação recolhida. Refere-se nomeadamente que, quando o equipamento da NSA esteve inoperacional durante cerca de três dias, os clientes dos EUA foram servidos directamente pelo GCHQ[123], tal como os clientes ingleses.

---

[115] Commons Written Answers, House of Commons Hansard Debates

[116] 12.7.1995.

[117] 25.10.1994

[118] 3.12.1997

[119] 12.5.2000

[120] 12.7.1995

[121] 8.3.1999, 6.7.1999

[122] 3.12.1997

[123] Intelligence and Security Committee,, Relatório Anual 1999-2000, parágrafo 14, apresentado ao parlamento pelo Primeiro Ministro em Novembro de 2000.

5.8.3. Austrália[124]

Martin Brady, Director do serviço de informações australiano DSD[125], confirmou numa carta ao programa "Sunday" do "Canal 9" australiano que o DSD cooperou com outros serviços de informações no âmbito do acordo UKUSA. Na mesma carta, sublinhou que todas as instalações australianas de informações são geridas ou pelos serviços australianos apenas ou em comum com os serviços dos EUA. Onde a utilização de tais instalações é compartilhada, o Governo australiano tem pleno conhecimento de todas as actividades e o pessoal australiano está envolvido a todos os níveis[126].

5.8.4. Nova Zelândia

Como já referido no ponto 5.4.2.2., é feita menção expressa, numa publicação emanada, nomeadamente, do Gabinete do Primeiro Ministro neozelandês sobre os serviços nacionais de segurança e de informações, à parceria em matéria de serviços de segurança existente entre cinco nações, nomeadamente os EUA, o Reino Unido, o Canadá, a Austrália e a Nova Zelândia, sendo assinaladas as vantagens daí decorrentes para a Nova Zelândia[127].

5.8.5 Países Baixos

Em 19 de Janeiro de 2001, o Ministro neerlandês da Defesa apresentou um relatório ao Parlamento dos Países Baixos sobre os aspectos técnicos e jurídicos da intercepção global dos modernos sistemas de telecomunicações[128]. Nele, o Governo dos Países Baixos considera que, embora não tenha ele próprio informações sobre este assunto, considera altamente provável, com base na informação de terceiros disponível, que exista a rede ECHELON, mas que é possível que existam outros sistemas com as mesmas capacidades. O Governo dos Países Baixos terá chegado à conclusão de que a intercepção global dos sistemas de comunicações não se limita aos países participantes no sistema ECHELON, mas é igualmente praticada por autoridades governamentais de outros países.

5.8.6. Itália

Luigi Ramponi, ex-director do SISMI, serviço de informações italiano, não deixa nenhuma dúvida, na entrevista que deu ao "Il Mondo", da existência do sistema ECHELON[129]. Ramponi diz explicitamente que, como Chefe do SISMI, sabia da existência de ECHELON. Desde 1992 estava ao corrente da intensa intercepção das frequências baixas, médias e altas. Quando se juntou ao SISMI, em 1991, a maioria da actividade relacionava-se com o Reino Unido e os EUA.

---

[124] *Martin Brady,* Director do DSD, carta de 16.3.1999 a Ross Coulthart, Sunday Program Channel 9, http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp; http://sunday.ninemsn.com/01_cover_stories/article_335.asp

[125] Defence Signals Directorate, Australian intelligence service engaged in SIGINT

[126] *Martin Brady,* Director do DSD, carta de 16.3.1999 a Ross Coulthart, Sunday Program Channel 9, http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp; http://sunday.ninemsn.com/01_cover_stories/article_335.asp

[127] Domestic and External Secretariat des Department of the Prime Minister and Cabinet von Neuseeland, Securing our Nation's Safety. How New Zealand manages its security and intelligence agencies (2000)

Texto original do excerto relevante : cf. nota de rodapé referente ao ponto 5.4.2.2.

[128] Brief aan de Tweede Kamer betreffende 'Het grootschalige afluisteren van moderne telecommunicatiesystemen', 19.1.2001

[129] *Francesco Sorti,* Dossier esclusivo. Caso ECHELON. Parla Luigi Ramponi. Anche i politici sapevano, Il mondo, 17.4.1998

5.9. Perguntas ao Conselho e à Comissão

Já em 17 de Fevereiro de 1998 teve lugar a apresentação pela Deputada Elly Plooij-van Gorsel[130] de uma primeira pergunta de carácter geral ao Conselho sobre o relatório STOA, bem como sobre a existência de um sistema global de intercepção dos EUA, no qual participa o Reino Unido, bem como ainda sobre os eventuais prejuízos daí decorrentes para os interesses comerciais das empresas europeias. Inúmeras foram as perguntas subsequentes sobre o mesmo tema[131]. A presidência do Conselho respondeu que o Conselho não dispõe, em si, de quaisquer informações, que não se encontra envolvido em tais assuntos e que, por conseguinte, se não encontra habilitado a transmitir quaisquer respostas.

Às perguntas de igual teor dirigidas à Comissão Europeia[132] retorquiu a mesma que o relatório é do seu conhecimento, mas que não existem quaisquer provas ou queixas de que um Estado-Membro viole, a este respeito, o Tratado CE[133]. A Comissão referiu estar, no entanto, atenta à situação, afirmando defender todos os interesses da Comunidade e envidar novos esforços tendentes a melhorar a segurança da sua rede de dados[134]
Na sessão plenária de 18 de Setembro, o Comissário Bangemann declarou não terem sido transmitidos à Comissão, nem pelos Estados-Membros, nem pelos cidadãos ou empresas, quaisquer indicações quanto à existência do sistema de intercepção tal como é descrito. "Se o sistema existisse, esse facto constituiria obviamente uma violação flagrante dos direitos individuais dos cidadãos e, obviamente, também um atentado à segurança dos Estados-Membros. Tal é absolutamente claro. No momento em que tal fosse objecto de confirmação oficial, quer o Conselho, quer, naturalmente, a Comissão e o Parlamento, teriam de reagir". Nesse caso, "a Comissão recorreria a todas as possibilidades de que dispõe para incitar os Estados-Membros a não procurarem obter informações deste modo ilegal"[135]

---

[130] Pergunta escrita P-0501/98 de Elly Plooij van Gorsel (ELDR) ao Conselho (17.1.1998). Já em 14 de Maio de 1997, Jonas Sjöstedt havia apresentado uma pergunta (H-0330/97) sobre a Resolução do Conselho de 17.1.1995 relativa à intercepção de telecomunicações e inquirido se a mesma se encontrava correlacionada com o Sistema ECHELON. A última parte da pergunta permaneceu sem resposta. As perguntas apresentadas por Mihail Papayannakis (G-004/98) e Nel van Dijk (H-0035/98) sobre a actividade de espionagem britânica foram objecto de resposta em 18.2.1998, nos termos da qual os assuntos respeitantes aos serviços de informações são da competência exclusiva das autoridades nacionais, não dispondo o Conselho de quaisquer informações sobre o assunto.

[131] Pergunta escrita E-0499/98 de Elly Plooij-van Gorsel (ELDR) ao Conselho (27.2.1998), Pergunta escrita E-1775/98 de Lucio Manisco (GUE/NGL) ao Conselho (8.6.1998), Pergunta oral H-1086/98, de Patricia McKenna ao Conselho (16.121998), pergunta oral H-1172/98 de Patricia McKenna ao Conselho (13.1.1999), pergunta oral H-1172/98 de Inger Schörling ao Conselho (13.1.1999), pergunta oral H-0526/99 de Pernille Frahm ao Conselho (6.10.1999), pergunta oral H-0621/99 de Lone Dybkjaer ao Conselho (19.11.1999), etc.

[132] Pergunta escrita E-1039/98 de Nel van Dijk (V) à Comissão (15.5.1998), pergunta escrita E-1306/98 de Cristiana Muscardini (NI) à Comissão (15.6.1998), pergunta escrita E-1429/98 de Daniela Raschhofer (NI) à Comissão (25.6.1998), perguntas escritas E-1987/98 e E-2329/98 de Nikitas Kaklamanis à Comissão (3.9.1998, 25.9.1998), pergunta escrita 1776/98 de Lucio Manisco (GUE/NGL) à Comissão, pergunta escrita 3014/98 de Paul Lannoye (V) à Comissão (6.11.1998), pergunta oral H-0547/99 de Pernille Frahm à Comissão, H-1067 de Patricia McKenna (V) à Comissão (16.12.1998), pergunta oral H-1237/98 de Inger Schörling à Comissão (13.1.1999), pergunta oral H-0092/99 de Ioannis Theonas à Comissão (13.1.1999), pergunta oral H-0547/99 de Pernille Frahm à Comissão (6.10.1999), pergunta oral H-0622/99 de Lone Dybkjaer à Comissão (17.12.1999), etc.

[133] Comissário Bangemann, em nome da Comissão, em resposta (25. 9. 1998) à pergunta escrita E-1776/98 do Deputado Lucio Manisco (GUE/NGL);

[134] Presidente da Comissão, J. Santer, em nome da Comissão, em 3.9.1998, na sua resposta à pergunta escrita E-1987/9.

[135] Negociações do Parlamento Europeu, sessão de segunda-feira, 14.9.1989, Ponto 7 da ordem do dia: Relações transatlânticas/Sistema ECHELON.

5.10. Relatórios parlamentares

5.10.1. Relatórios do Comité Permanente R, Comité de controlo da Bélgica

O Comité Permanente R de controlo belga já discutiu o ECHELON em dois relatórios.

O terceiro capítulo do seu relatório de actividades 1999 foi devotado às reacções dos serviços belgas de inteligência à possível existência de um sistema ECHELON de vigilância das comunicações. O relatório de 15 páginas conclui que os serviços de inteligência belgas, nomeadamente a Sûreté de l'Etat e o Service Général du Renseignement (SGR), apenas tiveram conhecimento de ECHELON através de documentos públicos.

O segundo relatório (rapport complémentaire d'activités 1999) trata do sistema ECHELON com muito mais pormenor. Aprecia o estudo do STOA e devota uma secção à explicação do historial técnico e jurídico do controlo de telecomunicações. Conclui que o ECHELON existe de facto e está em condições de escutar toda a informação transmitida por satélite (aproximadamente 1% de todas as comunicações telefónicas internacionais), na qual pesquisa palavras-chave, e ainda que a sua capacidade de descodificação é muito maior que a admitida pelos norte-americanos. A dúvida permanece sobre a veracidade das declarações de que nenhuma espionagem industrial é executada em Menwith Hill. O relatório salienta que é impossível verificar com qualquer grau de certeza o que ECHELON faz ou não faz.

5.10.2. Relatório da Comissão de Defesa Nacional da Assembleia Nacional francesa

A Comissão de Defesa Nacional da Assembleia Nacional francesa elaborou um relatório sobre sistemas de escuta[136]. Na reunião de 28. 11. 2000, o relator, Arthur Paecht, apresentou os resultados do relatório à comissão ECHELON do Parlamento Europeu.

No seguimento de um exame detalhado de uma enorme variedade de aspectos, o relator, Artur Paecht, chega à conclusão de que ECHELON existe e é, na sua opinião, o único sistema de intercepção multinacional conhecido. As capacidades do sistema são reais mas atingiram os seus limites, não só porque a despesa não pode acompanhar o ritmo da explosão das comunicações mas também porque certos alvos já se sabem agora proteger.

O sistema ECHELON "afastou-se" dos seus objectivos originais, que estavam ligados à Guerra Fria, e tal significa que não é impossível que a informação recolhida seja utilizada para objectivos políticos e industriais contra outros estados da OTAN.

O ECHELON pode certamente constituir um perigo para as liberdades fundamentais e, neste contexto, levanta muitos problemas que exigem as respostas adequadas. Seria errado imaginar que os Estados ECHELON abandonarão as suas actividades. Pelo contrário, há vários indícios que levam a crer que se constituiu um novo sistema para superar as limitações do ECHELON, graças a novos meios e, sem dúvida, a novas parcerias.

[136] Rapport d'information déposé en application de l'article 145 du règlement par la Commission de la défense nationale et des forces armées, sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale, No 2623 Assemblée nationale, enregistré à la Présidence de l'Assemblée nationale le 11 octobre 2000.

5.10.3 Relatório da Comissão Parlamentar italiana dos Serviços de Informação e Segurança e de Defesa do Estado

Na Itália, a Comissão Parlamentar dos Serviços de Informação e Segurança apresentou um relatório sobre o "Papel dos Serviços de Informação e Segurança no caso ECHELON"[137], o qual foi transmitido, em 19 de Dezembro de 2000, ao Presidente do Parlamento italiano".

As conclusões sobre a existência de um sistema chamado nome ECHELON revelam-se vagas. Segundo o relatório, "no quadro das audições havidas em comissão excluiu-se, em larga medida, a possibilidade da existência de um sistema de intercepção integrado com essa denominação, instituído pelos cinco Estados participantes no Acordo UKUSA (EUA, Reino Unido, Austrália, Nova Zelândia e Canadá) e destinado a interceptar as comunicações a nível mundial". Nos termos desse relatório, sendo embora clara a existência de uma estreita cooperação entre os países anglo-saxónicos, as investigações levadas a efeito pela comissão não permitiam afirmar que essa cooperação tivesse por objectivo a criação de um sistema de intercepção integrado ou mesmo de uma rede de intercepção de alcance mundial. No entender da comissão, afigura-se provável que a designação ECHELON seja sinónimo de um estádio de desenvolvimento tecnológico no domínio das técnicas de intercepção de comunicações por satélite. É explicitamente referido que os serviços secretos italianos SISMI excluíram a possibilidade de existir actualmente um processo de reconhecimento automático de palavras pronunciadas no quadro de diálogos, não sendo, por conseguinte, viável uma intercepção específica de comunicação oral que contenha essas palavras-chave.

[137] "Il ruolo dei servizi di informazione e sicurezza nel caso 'ECHELON'." Relazione del comitato parlamentare per i servizi di informatione e sicurezza e per il segreto di stato. Approvata nella seduta del 29 novembre 2000. Trasmessa alle Presidenze il 19 dicembre 2000.

6. Poderão existir outros sistemas de intercepção operantes a nível mundial?

6.1. Condições para a existência de um tal sistema

6.1.1. Condições técnicas e geográficas

Para escutar, a nível mundial, as comunicações internacionais transmitidas por satélites da primeira geração são indispensáveis estações de recepção no Atlântico, no Oceano Índico e na região do Pacífico. No caso da mais recente geração de satélites, susceptível de emitir por sub-regiões, teriam que ser preenchidas outras condições relativas à posição geográfica das estações de escuta, se se pretender interceptar todas as comunicações efectuadas através de satélite.

Qualquer outro sistema de intercepção funcionando a nível mundial seria forçado a estabelecer as suas estações fora do território dos Estados UKUSA.

6.1.2. Condições políticas e económicas

Ora o estabelecimento de um sistema de intercepção deste tipo que funcione a nível mundial , teria igualmente que fazer sentido do ponto de vista económico e político, para o operador ou operadores. O beneficiário, ou os beneficiários de tal sistema teriam que ter interesses de segurança mundiais, económicos, militares ou outros, ou crer pelo menos que se contam entre as superpotências mundiais. Por conseguinte, estamos a falar essencialmente da China e dos Estados do G8, com exclusão dos Estados Unidos e do Reino Unido.

6.2. França

A França tem territórios, departamentos e autoridades regionais nas três regiões citadas anteriormente.

No Atlântico, há, a este do Canadá, Saint Pierre e Miquelon (65º W/47º N), a nordeste da América do Sul a Guadalupe (61º W/16º N) e a Martinica (60º W/14º N) e ao largo da costa nordeste da América do Sul a Guiana francesa (52º W/5º N).

No Oceano Índico, há, a leste da África Austral, Mayotte (45º E/12º S) e a Reunião (55º E/20º S) e, no extremo sul, os Territórios Austrais e Antárcticos franceses. No Pacífico, há a Nova Caledónia (165º E/20º S), Wallis e Futuna (176º W/12º S) e a Polinésia francesa (150º W/16º S).

Muito pouca informação está disponível sobre as eventuais estações operadas pelo serviço de informações francês (DGSE) nestas regiões ultramarinas. De acordo com relatos de jornalistas franceses[138], existem estações em Kourou, na Guiana francesa, e em Mayotte. Não há nenhuma informação precisa quanto à dimensão das estações, ao número ou dimensão das antenas de satélite. Na França continental existirão aparentemente outras estações, em Domme, perto de Bordéus, e em Alluetts-le-Roi, perto de Paris. Vincent Jauvert calcula que exista um total de 30 antenas de satélite. O autor Erich Schmidt-Enboom[139] afirma que também na Nova Caledónia funciona uma estação e que o serviço de informações alemão é um dos seus utilizadores.

Teoricamente, a França poderia igualmente explorar um sistema de intercepção mundial, uma vez que, a par das condições geográficas, também dispõe dos pressupostos ténicos e financeiros para o efeito. Contudo, não há um número suficiente de informação disponível no domínio público para o vosso relator poder afirmar seriamente que esse é o caso.

6.3. Rússia

O serviço de informações russo FAPSI ("Federal Agency of Government Communications and Information, Federalnoye Agentstvo Pravitelstvennoy Svyazi"), que é responsável pela segurança das comunicações e pelo SIGINT, explora estações terrestres na Letónia, no Vietname e em Cuba, em colaboração com o serviço russo de informação militar GRU.

De acordo com a base legal aplicável, o objectivo do serviço de informações russo FAPSI consiste na recolha de informações nos domínios político, económico, militar e técnico-científico, visando o apoio ao desenvolvimento económico e ao progresso técnico-científico, e militar[140]. Além disso, o director do FAPSI estabeleceu em 1997 como função primordial do serviço em questão a intercepção de comunicações encriptadas com o estrangeiro, bem como a intercepção geral[141].

No Atlântico, a Estação situa-se em Lourdes, Cuba (82º W/23º N), sendo explorada em comum com o serviço de informações cubano. Esta estação permite à Rússia a recolha, quer de informações estratégicas, quer de comunicações militares e comerciais[142]. No Oceano Índico há estações na Rússia, sobre as quais não há nenhuma informação disponível. Uma outra estação sita em Skundra, na Letónia, foi encerrada em 1998[143]. No Pacífico existirá uma estação em Cam Ranh, no norte do Vietname. Não existe informação precisa sobre as estações do ponto de vista do número e dimensão das antenas.

---

[138] *Jean Guisnel*, L'éspionage nést plus un secret, The Tocqueville Connection, 10.7.1998.

Vincent Jauvert, La Espionnage comment la France, Le Nouvel Observateur, 5.4.2001, Nº 1900, p. 14 e segs..

[139] *Erich Schmidt-Eenboom*, in : Streng Geheim, Museumsstiftung Post und Telekommunikation, Heidelberg 1999, p.180.

[140] Russian Federation Federal Law on Foreign Intelligence, aprovada pela "Duma" em 8.12.1995, Secções 5 e 11

[141] Citação ib. *Gordon Benett*, Conflict Studies and Research Center, The Federal Agency of Government Communications and Information, August 2000, http://www.csrc.ac.uk/pdfs/c105.pdf

[142] Citação in *Gordon Bennett*, UK Ministry of Defence, The Federal Agency of Government Communications and Information, und Homepage der Federation of American Scientists

[143] Homepage der Federation of American Scientists (FAS), http://www.fas.org

Conjuntamente com as estações existentes na própria Rússia, é teoricamente possível a cobertura mundial. Contudo, também neste caso, a informação disponível é insuficiente para tirar conclusões sólidas.

6.4. Os outros Estados do G8 e a China

Nem os outros Estados do G8 nem a China têm territórios próprios ou aliados nas regiões do mundo que lhes permitiriam explorar um sistema de intercepção mundial.

7. Compatibilidade de um sistema de intercepção de comunicações do tipo "ECHELON" com o direito comunitário

7.1 Observações preliminares

De acordo com o mandato que lhe foi cometido, a comissão foi também expressamente incumbida de ajuizar da compatibilidade de um sistema de intercepção de comunicações do tipo "ECHELON" com o direito comunitário.[144] Para o efeito, cumpre nomeadamente avaliar se um tal sistema não colidirá com as duas directivas existentes relativas à protecção dos dados (95/46/CE e 97/66/CE), bem como com o disposto no artigo 286º do Tratado CE e do nº 2 do artigo 8º do Tratado da União Europeia.

Parece necessário proceder à presente análise sob dois ângulos distintos. O primeiro aspecto decorre das provas circunstanciais constantes do capítulo 5 que permitem concluir que o sistema designado de "ECHELON" foi concebido como um sistema de intercepção das comunicações destinado a fornecer aos serviços secretos norte-americano, canadiano, australiano, neozelandês e britânico informações sobre factos ocorridos em território estrangeiro mediante a recolha e a avaliação dos dados constantes das comunicações. No caso vertente, trata-se de um instrumento de espionagem clássico dos serviços estrangeiros de informações de segurança[145]. Assim sendo, importa, numa primeira fase, examinar a questão da compatibilidade de um tal sistema de informações de segurança com o direito da União.

Além disso, no relatório que apresentou ao grupo STOA, Duncan Campbell formula uma acusação segundo a qual este sistema é utilizado abusivamente para fins de espionagem económica, o que teria estado na origem de graves prejuízos para a economia de países europeus. Ademais, existem declarações do antigo Director da CIA, R. James Woolsey, segundo as quais os Estados Unidos espionariam empresas europeias, embora com o intuito exclusivo de restabelecer condições equitativas de mercado, uma vez que os contratos seriam obtidos graças a práticas de corrupção activa.[146] Se for verdade que os sistemas são utilizados no intuito de espionar a concorrência, coloca-se, mais uma vez, a questão da compatibilidade com o direito comunitário. Este segundo aspecto, deve, por conseguinte, ser analisado separadamente.

7.2. Compatibilidade de um sistema de informações de segurança com o direito da União

7.2.1. Compatibilidade com o direito comunitário

Em princípio, as actividades e medidas levadas a efeito para fins de segurança de Estado ou de acção penal não se inserem no âmbito de aplicação do Tratado CE. Uma vez que, com base no princípio da autoridade circunscrita, só é dado à Comunidade Europeia actuar nos domínios para os quais que foi habilitada a fazê-lo, a Comunidade excluiu consequentemente estes domínios do âmbito de aplicação das directivas relativas à protecção de dados, que se alicerçam no Tratado

[144] Cf., capítulo 1, 1.3 *supra*

[145] Cf Capítulo 2 *supra*

[146] Cf. Capítulos 5, 5.6. e 5.8.

CE e, em particular, no seu artigo 95º (ex-artigo 100º-A). A Directiva 59/46/CE do Parlamento Europeu e do Conselho relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados [147] e a Directiva 97/66/CE relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das telecomunicações [148] não se aplicam, em caso algum, "ao tratamento de dados[149] / actividades[150] que tenha como objecto a segurança pública, a defesa, a segurança do Estado (incluindo o bem-estar económico do Estado quando esse tratamento disser respeito a questões de segurança do Estado), e as actividades do Estado no domínio do direito penal ". A proposta de directiva do Parlamento Europeu relativa ao tratamento de dados de natureza pessoal e à protecção da privacidade no sector das comunicações electrónicas [151], pendente para deliberação no Parlamento, retoma esta mesma formulação. Assim, a participação de um Estado-Membro num sistema de intercepção por razões de segurança de Estado não é *per se* incompatível com as directivas da CE relativas à protecção dos dados.

Do mesmo modo, não poderá estar em causa uma violação do artigo 286º do Tratado CE, que alarga o âmbito de aplicação das directivas relativas à protecção dos dados ao tratamento dos dados por parte dos órgãos e instituições comunitárias. O mesmo se aplica ao Regulamento (CE) nº 45/2001 do Parlamento e do Conselho relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados .[152] O regulamento em referência apenas é aplicável na medida em que os órgãos e instituições actuem no quadro do Tratado CE.[153] A fim de evitar todo e qualquer mal-entendido, cumpriria sublinhar expressamente que uma participação dos órgãos e instituições comunitárias num sistema de intercepção jamais foi alegada e que o relator não dispõe de qualquer elemento que lhe permita pressupor uma tal participação.

7.2.2. Compatibilidade com outra legislação comunitária

No concernente aos domínios abrangidos pelos títulos V (Política Externa e de Segurança Comum) e VI (Cooperação Policial e Judiciária em matéria penal), não existem quaisquer disposições relativas à protecção dos dados susceptíveis de serem comparáveis com as directivas comunitárias. O Parlamento Europeu teve oportunidade de sublinhar reiteradamente a necessidade imperiosa de intervir neste domínios.[154]

Nestes domínios, a protecção dos direitos e liberdades fundamentais das pessoas é salvaguardada pelos artigos 6º e 7º e, nomeadamente, pelo nº 2 do artigo 6º do Tratado da União Europeia, no âmbito do qual a União se compromete a respeitar os direitos fundamentais, tal como garantidos

[147] JO L 281 de 23.11.1995, p. 31

[148] JO L 24 de 30.1.1998, p. 1

[149] Directiva 95/46/CE, nº 2 do artigo 3º

[150] Directiva 97/66/CE, nº 3 do artigo 1º

[151] COM (2000) 385 final, JO C 365 E/223

[152] Regulamento (CE) nº 45/2001, JO L 8, 12.1.2001, p. 1

[153] Nº 1 do artigo 3º; cf. também considerando 15 „ Quando esse tratamento for efectuado pelas instituições e órgãos comunitários para o exercício de actividades que não se enquadram no âmbito de aplicação do presente Regulamento, em especial para as previstas nos títulos V e VI do Tratado da União Europeia, a protecção das liberdades e dos direitos fundamentais das pessoas é assegurada no respeito do artigo 6.o do Tratado da União Europeia."

[154] cf. , por exemplo, ponto 25 da Resolução sobre o Plano de Acção do Conselho e da Comissão sobre a melhor forma de aplicar as disposições do Tratado de Amesterdão relativas à criação de um espaço de liberdade, de segurança e de justiça (13844/98 - C4-0692/98 - 98/0923(CNS), JO C 219 de 30.7.1999, p. 61 e seguintes

pela Convenção Europeia de Salvaguarda dos Direitos do Homem e das Liberdades Fundamentais (CEDH) e tal como resultam das tradições constitucionais comuns aos Estados-Membros. Assim, se os Estados-Membros são obrigados a respeitar os direitos fundamentais e, em particular, a CEDH (cf. neste contexto o capítulo 8 *infra*). A União é igualmente obrigada a respeitar os direitos fundamentais no exercício das suas competências legislativas e administrativas. Não obstante, não se observa, até à data, a existência, na União Europeia, de regulamentação que incida sobre a legalidade da intercepção das telecomunicações para fins de protecção da segurança de Estado ou para fins de obtenção de informações de segurança.[155] Consequentemente, a questão da violação do disposto no nº 2 do artigo 6º do Tratado da União Europeia não se coloca directamente.

7.3. Questão da compatibilidade em caso de utilização abusiva de um sistema de intercepção para fins de espionagem da concorrência

Caso um Estado-Membro promovesse a utilização de um sistema de intercepção *inter alia* para efeitos de espionagem económica, autorizando os seus próprios serviços de informações de segurança a operarem um tal sistema ou concedendo a serviços estrangeiros de informações acesso ao seu próprio território para este mesmo fim, tal constituiria categoricamente uma violação do direito comunitário. Com efeito, em conformidade com o disposto no artigo 10º do Tratado CE, os Estados-Membros estão obrigados a um dever de lealdade geral e devem, em particular, abster-se de toda e qualquer acção susceptível de lesar a realização dos objectivos do Tratado. Mesmo que a intercepção de comunicações não tivesse lugar em benefício da economia nacional (o que, na realidade, teria um efeito comparável ao de uma ajuda estatal e seria, consequentemente, uma violação do disposto no artigo 86º do Tratado CE), mas, sim, em benefício de um Estado terceiro, uma tal actividade seria, por princípio, contrária ao princípio do mercado comum em que se alicerça o Tratado CE, na medida em que tal implicaria uma distorção da concorrência.

No entender do relator, uma tal atitude constituiria, além disso, uma violação da directiva relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das telecomunicações [156], porquanto a questão da aplicabilidade das directivas deve ser solucionada com base em considerações de tipo funcional e não organizacional. Tal decorre não apenas da letra das disposições relativas ao âmbito de aplicação, mas também do espírito da lei. Se os serviços de informações de segurança lançam mão da sua capacidade para fins de espionagem da concorrência, a sua actividade não se exerce no interesse da segurança ou da acção penal, mas sim para outros fins abusivos, e a sua actividade recai plenamente no âmbito de aplicação da

[155] Em matéria de vigilância existem actualmente, no quadro da União Europeia, apenas dois actos legislativos, os quais não abordam a questão da legalidade:

- a Resolução do Conselho de 17 de Janeiro de 1995 relativa à intercepção legal de comunicações (JO C 329 de 4.11.1996), cujo anexo comporta uma inventariação dos requisitos técnicos relativos à realização de medidas de intercepção admissíveis nos sistemas modernos de telecomunicações e

- o acto do Conselho de 29 de Maio de 2000 que estabelece, em conformidade com o artigo 34º do Tratado da União Europeia, a Convenção relativa ao auxílio judiciário mútuo em matéria penal entre os Estados-Membros da União Europeia (JO C 197 de 12.7.2000, p. 1, artigo 17º e seguintes) que preceitua as condições nas quais o auxílio judiciário mútuo é possível no tocante à intercepção das comunicações. Estes disposições não afectam, de modo algum, os direitos de todos aqueles cujas comunicações são objecto de escuta, na medida em que o Estado onde as pessoas visadas se encontram dispõe do direito de recusar o auxílio judiciário mútuo, caso não esteja habilitado a fazê-lo ao abrigo da sua legislação nacional.

[156] Directiva 97/66/CE, JO L 24 de 30.1.1998 p. 1

directiva. Nos termos do artigo 5º da directiva em referência, os Estados-Membros são obrigados a garantir a confidencialidade das comunicações, devendo, nomeadamente, proibir " a escuta, a colocação de dispositivos de escuta, o armazenamento ou outros meios de intercepção ou vigilância de comunicações por terceiros, sem o consentimento dos utilizadores". Nos termos do disposto no artigo 14º, apenas são admissíveis excepções quando estejam em causa a segurança nacional, a defesa ou acções penais. Na medida em que a espionagem económica não legitima qualquer excepção, constituiria, neste caso, uma violação do direito comunitário.

7.4. Conclusões

À guisa de conclusão, poderá assinalar-se que, face à situação jurídica actual, um sistema de intercepção de comunicações do tipo ECHELON não viola, em princípio, a legislação comunitária na medida em que não afecta aspectos do direito da União em que uma incompatibilidade se pudesse alicerçar. Todavia, tal aplica-se apenas quando o sistema é exclusivamente utilizado para fins de segurança de Estado *lato sensu*. Se, em contrapartida, for utilizado para outros fins, nomeadamente para a espionagem económica de empresas estrangeiras, observa-se uma violação do direito comunitário. Caso um Estado-Membro se encontre envolvido numa tal acção, esse Estado-Membro estará a violar o direito comunitário.

8. Compatibilidade da intercepção de comunicações por parte dos serviços de informações de segurança com o direito fundamental ao respeito pela vida privada

8.1. Intercepção das comunicações enquanto ingerência no direito fundamental ao respeito pela vida privada

Todo e qualquer acto que envolva a intercepção de comunicações e mesmo o registo de dados por parte dos serviços de informações de segurança com esse objectivo[157] representa uma grave ingerência na vida privada de um indivíduo. A escuta ilimitada pelos poderes públicos apenas é admissível num "Estado policial". Em contrapartida, nos Estados-Membros da UE, que constituem democracias evoluídas, a necessidade de os órgãos de Estado e, concomitantemente, os serviços de informações de segurança, respeitarem a vida privada é incontestada, encontrando-se, por regra, consagrada nas diferentes constituições nacionais. A vida privada beneficia assim de uma protecção particular, sendo que as possibilidades de ingerência apenas são autorizadas após avaliação das considerações jurídicas e atento o princípio da proporcionalidade.

Os Estados que integram o sistema UKUSA estão também bem cientes do problema em referência. Todavia, as disposições de protecção previstas visam o respeito da vida privada dos cidadãos nacionais, pelo que os cidadãos europeus se encontram geralmente excluídos das mesmas. Por exemplo, nos Estados Unidos, nas disposições que regem as condições da vigilância electrónica, aos interesses do Estado no que se refere ao bom funcionamento do serviço de informações de segurança não se opõem os interesses de uma protecção geral eficaz dos direitos fundamentais, mas, sim, a necessidade de proteger a vida privada dos "cidadãos americanos" ("US-Persons").[158]

8.2. A protecção da vida privada ao abrigo dos acordos internacionais

O respeito da vida privada enquanto direito fundamental encontra-se consagrado em inúmeras convenções do direito internacional público.[159] A nível mundial, o Pacto Internacional sobre os

[157] Tribunal Constitucional Federal, 1BvR 2226/94 de 14.7.1999, Rz 187 "O registo de dados representa já uma ingerência, na medida em que torna as comunicações disponíveis para o Serviço Federal de Informações de Segurança e constitui a base da análise subsequente recorrendo aos termos de procura."

[158] Cf., Relatório destinado ao Congresso dos Estados Unidos de fins de Fevereiro de 2000 "Legal Standards for the Intelligence Community in Conducting Electronic Surveillance", http://www.fas.org/irp/nsa/standards.html, que remete para o "Foreign Intelligence Surveillance Act" (FISA), impresso no Título 50, capítulo 36, U.S.C. § 1801 e seguintes e Exec. Order No. 12333, 3 C.F.R. 200 (1982), impresso no título 50, capítulo 15 U.S.C. § 401 e seguintes, http://www4.law.cornell.edu/uscode/50/index.html.

[159] Artigo 12º. Declaração Universal dos Direitos do Homem; artigo 17º, Pacto Internacional sobre os direitos civis e políticos; artigo 7º da Carta dos Direitos Fundamentais da UE; artigo 8º da Convenção Europeia dos Direitos do Homem, Recomendação do Conselho da OCDE sobre as directrizes aplicáveis à segurança dos sistemas de informação, adoptada em 26./27.11.1993 C(92) 188/Final; artigo 7º da Convenção do Conselho da Europa sobre a protecção das pessoas relativamente ao tratamento automático de dados pessoais; cf. o estudo encomendado pelo Grupo STOA "Development of surveillance tehnology and risk of abuse of economic information; Vol 4/5: The legality of the interception of electronic communications: A concise survey of the principal legal issues and instruments under international, European and national law" (Chris Elliot), Outubro de 1999, 2

direitos civis e políticos[160], celebrado em 1966 sob os auspícios da ONU, merece referência particular, consagrando, no seu artigo 17º, a protecção da vida privada. No contexto das queixas apresentadas por outros Estados, todos os países que integram o sistema UKUSA têm acatado as decisões adoptadas pela Comissão dos Direitos do Homem instituída em conformidade com o disposto no artigo 41º do Pacto destinado a regular as violações ao abrigo do direito internacional. O protocolo adicional [161], que alarga os poderes da Comissão dos Direitos do Homem por forma a cobrir as queixas apresentadas a título individual, ainda não foi assinado pelos Estados Unido da América, razão pela qual esses requerentes não poderão apelar perante a Comissão dos Direitos do Homem em caso de violação dos direitos do Homem por parte dos EUA.

A nível da UE, foram envidados esforços no sentido de consagrar uma protecção europeia específica dos direitos fundamentais mediante a elaboração de uma Carta dos Direitos Fundamentais da UE. De acordo com o disposto no artigo 7º dessa Carta, que se intitula "Respeito pela vida privada e familiar", encontra-se também explicitamente regulado o direito de respeito pelas comunicações.[162] Além disso, o artigo 8º regula o direito fundamental à protecção dos dados de natureza pessoal. Esta disposição protege toda e qualquer pessoa em caso de tratamento de dados (por via informática ou não) que lhe digam respeito, o que ocorre geralmente sempre que se observa a escuta de comunicações e que é sistematicamente o caso sempre que são interceptadas outras formas de comunicação.

A despeito das considerações supramencionadas, e na medida em que não foram tomadas quaisquer providências no sentido de integrar a Carta no Tratado, pelo menos, no âmbito da próxima reforma, a carta não oferece qualquer protecção suplementar aos cidadãos europeus. A assinatura da Carta pelos presidentes do Parlamento, da Comissão e do Conselho em 7 de Dezembro de 2000 em Nice terá sido portadora de uma considerável importância política. Não obstante, no plano jurídico, apenas representa uma declaração das instituições que se sentem vinculadas ao respeito pelos direitos fundamentais nela enunciados.

O único instrumento eficaz a nível internacional em matéria de protecção global da vida privada é a Convenção Europeia dos Direitos do Homem.

8.3. As disposições consagradas na Convenção Europeia dos Direitos do Homem (CEDH)

8.3.1. *A importância da Convenção na UE*

A protecção dos direitos fundamentais garantida pela Convenção reveste uma importância particular, na medida em que a Convenção foi ratificada por todos os Estados-Membros da UE. Assim sendo, a Convenção salvaguarda um nível de protecção uniforme em toda a Europa. Os Estados signatários da Convenção comprometeram-se, ao abrigo do direito internacional, a garantirem os direitos consagrados na Convenção e a acatarem a jurisdição do Tribunal Europeu dos Direitos do Homem sediado em Estrasburgo. Assim sendo, as disposições jurídicas nacionais

[160] Pacto Internacional sobre os direitos civis e políticos, adoptado pela Assembleia Geral das Nações Unidas em 16.12.1966

[161] Protocolo adicional ao Pacto Internacional sobre os direitos civis e políticos, adoptado pela Assembleia Geral das Nações Unidas, em 19 de Dezembro de 1966

[162] "Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações".

relevantes são susceptíveis de serem apreciadas pelo Tribunal Europeu dos Direitos do Homem relativamente à respectiva conformidade com a Convenção Europeia dos Direitos do Homem. Em caso de violação dos direitos do Homem, o Tribunal pode condenar os Estados signatários e obrigá-los ao pagamento de indemnizações. A Convenção dos Direitos do Homem assumiu ainda uma maior importância ao ser reiteradamente invocada pelo Tribunal de Justiça das Comunidades Europeias, paralelamente aos princípios jurídicos gerais dos Estados-Membros, sempre que se trata de proceder a verificações de disposições legislativas. O Tratado de Amesterdão (nº 2 do artigo 6º do Tratado UE) prevê, além disso, a obrigação de a UE respeitar os direitos fundamentais, tal como se encontram consagrados na Convenção.

8.3.2. Âmbito territorial e pessoal da protecção consagrada na CEDH

Os direitos consignados na CEDH constituem direitos do Homem geralmente reconhecidos, razão pela qual não se encontram vinculados à nacionalidade. Esses direitos devem ser reconhecidos a todas as pessoas abrangidas pela jurisdição das partes contratantes. Tal significa que os direitos do Homem devem ser garantidos em todo o território do Estado signatário, pelo que toda e qualquer excepção, a nível local, constitui uma violação da Convenção. Além disso, estes direitos aplicam-se também fora do território nacional dos Estados signatários desde que a autoridade Estado aí seja exercida. Os direitos consignados na CEDH relativamente aos Estados signatários assistem também às pessoas fora do território desse Estado desde que um Estado signatário interfira na sua vida privada fora do território nacional[163].

O último aspecto enunciado é particularmente importante neste contexto, na medida em que o problema dos direitos fundamentais no domínio da vigilância de telecomunicações apresenta a particularidade de o Estado responsável por essa actividade, a pessoa objecto da vigilância e o processo de intercepção propriamente dito não coexistirem no mesmo local. Tal aplica-se, nomeadamente às comunicações internacionais, mas também, em determinados casos, às comunicações nacionais, sempre que as informações são transmitidas através de ligações situadas no estrangeiro. Trata-se mesmo da situação padrão observada nas actividades dos serviços de informações no estrangeiro. Por outro lado, não se pode excluir que as informações obtidas graças às actividades de intercepção por intermédio de um serviço de informações de segurança sejam transmitidas a outros países.

8.3.3. *Admissibilidade da vigilância das telecomunicações ao abrigo do artigo 8º da CEDH*

O nº 1 do artigo 8º da Convenção preceitua o seguinte "Qualquer pessoa tem o direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência". Não é feita qualquer referência explícita à protecção das comunicações telefónicas e das telecomunicações. Não obstante, em virtude da jurisprudência do Tribunal Europeu dos Direitos do Homem, estes aspectos encontram-se igualmente cobertos pelo conceito de "vida privada" e de "correspondência" e beneficiam, por essa razão, da protecção do artigo 8º da Convenção.[164] A

[163] Acórdão do Tribunal Europeu dos Direitos do Homem Loizidou/Turquia, 23.3.1995, linha 62 com a seguinte referência: "...the concept of 'jurisdiction' under this provision is not restricted to the national territory of the High Contracting Parties.[...] responsibility can be involved because of acts of their authorities, whether performed within or outside national boundaries, which produce effects outside their own territory" com referência ao Tribunal Europeu dos Direitos do Homem, Drozd e Janousek, 26.6.1992, linha 91; cf. texto circunstanciado *in Francis G.* Jacobs, *Robin C. A. White,* The European Convention on Human Rights (1996)^2, Clarendon Press(1996), p. 21 e seguintes, *Jochen Abr. Frowein, Wolfgang Peukert,* Europäische Menschenrechtskonvention, N. P. Engel Verlag (1996), Rz 4ff.

[164] Tribunal Europeu dos Direitos do Homem, Klass *et al.*, 6.9.1978, linha 41.

protecção dos direitos fundamentais alarga-se não apenas ao conteúdo das comunicações, mas também ao registo de elementos externos. Por outras palavras, ainda que um serviço de informações de segurança apenas registe dados como sejam a hora e a duração das comunicações ou ainda os números compostos, trata-se, ainda assim, de uma ingerência na vida privada.[165]

O direito fundamental consagrado no nº 2 do artigo 8º da Convenção não é ilimitado. São admissíveis ingerências no direito fundamental ao respeito da vida privada sempre que as mesmas se alicercem numa base jurídica existente no direito nacional.[166] O direito deve ser acessível a todos e previsível nos seus efeitos.[167]

Os Estados-Membros não dispõem, por conseguinte, de uma liberdade total para interferirem no exercício deste direito fundamental da forma que entenderem. O artigo 8º da Convenção apenas autoriza uma tal ingerência para efeitos da realização dos objectivos enunciados no nº 2, nomeadamente a segurança nacional, a segurança pública, a prevenção de infracções penais, bem como o bem-estar económico do país[168], o que não justifica, em todo o caso, a espionagem económica, na medida em que apenas se encontram cobertas as "intervenções necessárias numa sociedade democrática". Para toda e qualquer intervenção, é necessário recorrer aos meios mínimos que permitam atingir o objectivo e, além disso, prever garantias suficientes contra quaisquer abusos.

8.3.4. A importância do artigo 8º da CEDH para as actividades dos serviços de informações

Do ponto de vista da organização das actividades dos serviços de informações consentânea com os direitos fundamentais, estes princípios gerais implicam o seguinte: se se revelar necessário, a fim de garantir a segurança nacional, autorizar os serviços de informações de segurança a interceptarem o conteúdo das telecomunicações ou, pelo menos, os dados relativos às comunicações, tal deve estar previsto no direito nacional e as disposições de execução devem ser acessíveis a todos. As consequências para as pessoas a título individual devem ser previsíveis, embora os requisitos do segredo devam ser tidos em consideração. Assim, num acórdão relativo à conformidade com o artigo 8º de controlos secretos de funcionários em domínios pertinentes para a segurança nacional, o Tribunal Europeu dos Direitos do Homem teve oportunidade de constatar que, neste caso específico, as disposições aplicáveis ao requisito da previsibilidade não devem ser idênticos aos observados em outros domínios.[169] No caso em apreço, o Tribunal considerou que a lei deve, em qualquer dos casos, preceituar as circunstâncias e as condições em

---

[165] Tribunal Europeu dos Direitos do Homem, Malone, 2.8.1984, linha 83 e seguintes, cf. também Davy, B/Davy/U, Aspectos da recolha estatal de informações e artigo 8º da CEDH, JB1 1985, 656.

[166] Segundo a jurisprudência do Tribunal dos Direitos do Homem (nomeadamente Sunday Times, 26.4.1979, p. 46 e seguintes, Silver *et al.*, 25.3.1983, p. 85 e seguintes) a noção de „lei" a que se refere o nº 2 do artigo 8º engloba não apenas as leis no sentido formal, mas também as disposições de hierarquia inferior, ou seja o direito consuetudinário escrito. É, todavia, essencial que o sujeito de direito possa reconhecer claramente em que circunstâncias é admissível uma tal ingerência. Para informações mais detalhadas Cf. *Wolfgang Wessely*, Privacidade nas telecomunicações. Um direito fundamental desconhecido? ÖJZ 1999, 491 e seguintes, 495

[167] Silver *et al.*, 25.3.1983, linha 87 e seguintes

[168] O argumento do bem-estar económico foi admitido pelo tribunal num caso que se reportava à comunicação de dados médicos importantes do ponto de vista da concessão de prestações públicas: MS/Suécia, 27.8.1997, p. 38, bem como num caso relativo à expulsão dos Países Baixos de uma pessoa que se encontrava dependente da segurança social depois de a justificação da sua autorização de residência se ter tornado caduca, Ciliz/Países Baixos, 11.7.2000, p. 65.

[169] Tribunal Europeu dos Direitos do Homem, Leander, 26.3.1987, linha 51

que o Estado pode interferir de forma secreta e, por isso, eventualmente perigosa, na vida privada.[170]

Relativamente à organização das actividades dos serviços de informações de uma forma consentânea com os direitos humanos, cumpre ter em consideração o facto de, embora a segurança nacional possa ser invocada para justificar uma ingerência na vida privada, o princípio da proporcionalidade, tal como definido no nº 2 do artigo 8º da CEDH, aplica-se igualmente: a segurança nacional constitui uma justificação válida apenas nos casos em que o intuito de proteger se afigura necessário numa sociedade democrática. Neste contexto, o Tribunal Europeu dos Direitos do Homem considerou inequivocamente que o interesse visado por um Estado na protecção da sua segurança nacional deve ser sopesado face aos interesses da pessoa no tocante ao respeito da vida privada.[171] As ingerências não são circunscritas a um mínimo absoluto, muito embora não seja suficiente invocar serem as mesmas oportunas ou desejáveis [172]. A ideia segundo a qual a intercepção de todas as comunicações, ainda que admissíveis ao abrigo do direito nacional, representa a melhor protecção contra a criminalidade organizada seria contrária ao disposto no artigo 8º da Convenção.

Além disso, dada a natureza específica das actividades levadas a efeito pelos serviços de informações de segurança, que pressupõem actividades que requerem segredo e, consequentemente, uma avaliação cuidadosa dos interesses em jogo, cumpre prever possibilidades de controlo mais rigorosas. O Tribunal Europeu dos Direitos do Homem teve oportunidade de sublinhar que um sistema de vigilância secreto destinado a garantir a segurança nacional comporta *per se* o risco de inviabilizar ou mesmo destruir o sistema democrático sob pretexto de o defender, razão pela qual são necessárias garantias mais apropriadas e mais eficazes para obstar a uma tal utilização abusiva de poderes.[173] As actividades legítimas dos serviços de informações de segurança só são consentâneas com os direitos fundamentais se o Estado signatário da Convenção tiver previsto sistemas de controlo suficientes e outras garantias contra todos e quaisquer abusos. Neste contexto, o Tribunal salientou, no contexto das actividades dos serviços de informações suecos, atribuir uma importância particular à presença de deputados nos organismos de controlo policial, bem como à supervisão exercida pelo Ministro da Justiça, pelo Provedor de Justiça parlamentar e pela Comissão dos Assuntos Jurídicos do Parlamento. Nestas condições, o facto de a França, a Grécia, a Irlanda, o Luxemburgo e a Espanha não disporem de comissões parlamentares incumbidas do controlo dos serviços secretos [174] , nem tão-pouco disporem de um sistema de controlo comparável ao provedor de justiça parlamentar dos países nórdicos merece ser criticado.[175] Assim sendo, o relator saúda os esforços envidados pela Comissão da Defesa da Assembleia Nacional francesa no sentido de instituir uma comissão de controlo,[176] tanto mais que a França dispõe de

[170] Tribunal Europeu dos Direitos do Homem, Malone, 2.8.1984, linha 67

[171] Tribunal Europeu dos Direitos do Homem, Leander, 26.3.1987, linha 59, Sunday Times, 26.4.1979, linha 46 e seguintes

[172] Tribunal Europeu dos Direitos do Homem, Silver *et al.*, 24.10.1983, linha 97

[173] Tribunal Europeu dos Direitos do Homem, Leander, 26.3.1987, linha 60.

[174] O relator tem conhecimento do facto de nem o Luxemburgo nem a Irlanda disporem de serviços de informações externas. A necessidade de uma instância do controlo específica apenas se reporta às actividades de informação no interior dos respectivos países.

[175] A propósito do controlo dos serviços de informações de segurança nos Estados-Membros, cf. capítulo 9.

[176] Proposta de lei "Proposition de loi tendant à la création de délégations parlementaires pour le renseignement" e respectivo relatório do Deputado *Arthur Paecht*, Rapport fait au nom de la Commission de la défense nationale et des forces armées sur la proposition de loi (N° 1497) de M. Paul Quilès et plusieurs de ses collègues tendant à la

capacidades de informações de segurança notáveis, quer do ponto de vista técnico, quer do ponto de vista geográfico.

8.4 Obrigação de controlo das actividades desenvolvidas pelos serviços de informações estrangeiros

8.4.1. Inadmissibilidade da não-observância do disposto no artigo 8º da CEDH através do recurso a serviços de informações de segurança de outros países

Tal como descrito mais atrás, as partes signatárias devem satisfazer várias condições para que as actividades desenvolvidas pelos seus serviços de informações sejam compatíveis com o disposto no artigo 8º da Convenção em referência. Afigura-se óbvio que os serviços de informações não podem eximir-se a estas obrigações, recorrendo aos serviços de outros organismos de informações sujeitos a disposições menos rigorosas. Caso contrário, o princípio da legalidade e respectivas duas faces – possibilidade de acesso e previsibilidade – constituiria letra morta, ao passo que a jurisprudência do Tribunal Europeu dos Direitos do Homem seria esvaziada da sua substância.

Tal significa, por um lado, que o intercâmbio de dados entre os serviços de informação apenas é admissível numa base muito circunscrita. Um serviço de informações poderá apenas solicitar a um serviço homólogo dados obtidos de uma forma consentânea com as condições enunciadas no seu próprio direito nacional. O raio de acção geográfico definido pela lei não pode ser alargado mediante a celebração de acordos com outros serviços. Do mesmo modo, um serviço de informação poderá levar a cabo operações em nome de um serviço de informações de um outro país, de acordo com as instruções deste último, apenas no caso de ter concluído que as operações são consentâneas com o direito nacional do seu próprio país. Mesmo se as informações se destinarem a um outro país, tal não altera, de modo algum, o facto de uma ingerência na vida privada, não previsível pelo sujeito de direito em causa, constituir uma violação dos direitos fundamentais.

Por outro lado, os Estados signatários da Convenção não podem autorizar os serviços de informação estrangeiros a levarem a cabo operações no seu território caso tenham razões para acreditar que as suas actividades não são conformes às disposições da referida Convenção.[177]

8.4.2. Exercício tolerado de actividades por parte de serviços de informações não europeus no território de partes contratantes da CEDH: consequências

8.4.2.1. Jurisprudência do Tribunal Europeu dos Direitos do Homem

Ao ratificarem a Convenção, as partes signatárias comprometeram-se a submeter o exercício da sua soberania a uma verificação do respeito pelos direitos fundamentais. Essas partes não podem subtrair-se a esta obrigação, renunciando à sua soberania. Com efeito, mantêm a responsabilidade pelo seu território, bem como as suas obrigações perante o sujeito de direito

---

création d'une délégation parlementaire pour les affaires de renseignement, enregistré à la Présidence de l'assemblée nationale le 23. novembre 1999

[177] *Dimitri Yernault*, "ECHELON" e l'Europe. A protecção da vida privada face à espionagem das comunicações, Journal des tribunaux, Droit Européen 2000, 187 e seguintes.

europeu, quando o exercício do poder público é assegurado pelo serviço de informações de um outro país. A jurisprudência constante do Tribunal confirma que os países signatários são obrigados a adoptar medidas positivas tendo em vista proteger a vida privada, por forma a que as pessoas privadas (!) não violem o disposto no artigo 8º da Convenção. Por outras palavras, não devem tomar toda e qualquer acção, mesmo a nível horizontal, no âmbito do qual a pessoa não se encontra perante um poder público, mas, sim, perante uma outra pessoa.[178] Se um país autorizar o serviço de informações estrangeiro a intervir no seu território, o requisito de protecção é bastante maior, na medida em que, nesse caso, é uma outra autoridade que exerce a sua soberania. A única conclusão lógica que se pode extrair é a seguinte: os Estados devem velar pela conformidade das actividades dos serviços de informação com os direitos do Homem no seu próprio território.

8.4.2.2. Consequências paras as estações

Na Alemanha, os Estados Unidos da América dispõem, em Bad Aibling, de um território próprio que utilizam exclusivamente para a recepção das emissões de satélite. Em Menwith Hill, no Reino Unido, existe uma utilização partilhada de terrenos com o mesmo objectivo. Se um serviço de informações norte-americano interceptar, nestas estações, comunicações não-militares procedentes de pessoas privadas ou de empresas procedentes de um país signatário da Convenção, tal daria lugar a requisitos de controlo ao abrigo da CEDH. Na prática, tal significa que a Alemanha e o Reino Unido, signatários da Convenção, são obrigados a certificarem-se de que as actividades dos serviços de informação norte-americanos sejam consentâneas com os direitos fundamentais. Tal é tanto mais pertinente quanto os representantes das ONG e da imprensa já patentearam reiteradamente a sua apreensão face às actividades da Agência de Segurança Nacional dos Estados Unidos (NSA).

8.4.2.3. Consequências no concernente às escutas efectuadas com base em instruções de um país estrangeiro

Em Morwenstow, no Reino Unido, o GCHQ efectua, em cooperação com a NSA, com base em instruções desta última, a intercepção de comunicações civis que são transmitidas sem qualquer outro filtro aos Estados Unidos. Ainda que as actividades sejam efectuadas em nome de terceiros, cumpre verificar se as mesmas são conformes aos direitos internacionais.

8.4.2.4. Obrigação de vigilância relativamente a países terceiros

No caso de operações que envolvam dois países signatários da Convenção, poderá partir-se, até certo ponto, do princípio recíproco de que o outro Estado respeita também a Convenção. Não obstante, tal aplica-se apenas até ao momento em que é possível apurar que um país signatário da Convenção a viola de forma sistemática e repetida. Os Estados Unidos não são signatários da Convenção e não estão sujeitos a um dispositivo de controlo equiparável. As actividades dos seus serviços de informação encontram-se regulamentadas de forma bastante circunstanciada, pelo menos no que diz respeito aos cidadãos dos Estados Unidos, ou seja pessoas que residem de forma regular nos Estados Unidos. As actividades da NSA no estrangeiro constituem objecto de outras disposições, muitas das quais são confidenciais e, consequentemente, inacessíveis ao público. Uma outra questão que suscita grande preocupação é o facto de os serviços de informação norte-americanos estarem sujeitos ao controlo das comissões da Câmara dos Representantes e do Senado, muito embora as comissões parlamentares manifestem um interesse muito circunscrito pelas actividades que a NSA efectua no estrangeiro.

[178] Tribunal Europeu dos Direitos do Homem, Cabales e Balkandali, 28.5.1985, linha Z 67; Gaskin/Reino Unido 7.7.1989, linha 38; Powell e Rayner, 21.2.1990, linha 41

Afigura-se-nos, por conseguinte, oportuno lançar um apelo à Alemanha e ao Reino Unido para que tenham devidamente em conta as obrigações decorrentes da Convenção e para que façam depender a autorização de actividades dos serviços de informação da NSA no seu território do respeito da Convenção neste contexto. Para o efeito, importa ter em consideração três aspectos importantes:

1. A Convenção prevê que as ingerências na vida privada apenas sejam admissíveis com base em disposições jurídicas acessíveis a todos e cujas consequências sejam previsíveis. Esta condição apenas poderá ser satisfeita se os Estados Unidos da América informarem a população europeia da forma e das circunstâncias em que a recolha de informações é efectuada. Caso se vislumbrem incompatibilidades com a Convenção Europeia dos Direitos do Homem, as normas americanas devem ser adaptadas ao nível de protecção consignado na Europa.

2. Ao abrigo da Convenção, as intervenções devem ser proporcionadas, sendo necessário recorrer a meios mínimos. Para o cidadão europeu, uma intervenção europeia deve ser considerada menos grave do que uma efectuada por um serviço de informações norte-americano, na medida em que, no primeiro caso, podem apelar para as vias de recurso nacionais.[179] Consequentemente, as intervenções devem, na medida do possível, ser exercidas por autoridades alemãs ou do Reino Unido, nomeadamente quando está em causa a instrução de investigações visando o início de acções penais. Os norte-americanos tentaram reiteradamente justificar as escutas acusando os europeus de corrupção activa e passiva[180] .Cumpre chamar a atenção dos americanos para o facto de todos os países da UE disporem de sistemas penais que funcionam. Em caso de suspeita, os Estados Unidos devem confiar as questões das acções penais aos países anfitriões. Caso não existam quaisquer suspeitas, a vigilância deve ser considerada desproporcionada e, logo, contrária aos direitos do Homem, o que a torna inadmissível. Assim sendo, a compatibilidade com a Convenção pode ser observada apenas no caso de os Estados Unidos se circunscreverem a medidas de vigilância úteis à sua própria segurança nacional, ou seja se forem desprovidas de finalidade penal.

3. Tal como supramencionado, a jurisprudência do Tribunal Europeu dos Direitos do Homem estipulou que a compatibilidade com os direitos fundamentais decorre da existência de sistemas de controlo e garantias suficientes contra todos e quaisquer abusos. Tal significa que a intercepção das comunicações efectuadas por norte-americanos em território europeu apenas é conforme aos direitos do Homem se os Estados Unidos previrem controlos eficazes nos casos em que procedam à intercepção de comunicações com o propósito de salvaguardarem a sua própria segurança nacional ou se NSA submeter as operações que desenvolve em território europeu à autoridade dos organismos de controlo instituídos por esse Estado anfitrião (ou seja a Alemanha ou o Reino Unido).

[179] Tal é também necessário para efeitos de conformidade com o artigo 13º da CEDH, que confere à pessoa cuja privacidade é invadida o direito de recurso perante uma instância nacional.

[180] *James Woosley* (antigo Director da CIA), Why America Spies on its Allies, The Wall Street Journal Europe, 22.3.2000, 31; ders., Remarks at the Foreign Press Center, Transskript, 7.3.2000, http://cryptome.org/echelon-cia.htm

A conformidade das operações de intercepção desenvolvidas pelos EUA com o disposto na CEDH apenas poderá ser satisfeita e o nível de protecção uniforme garantido na Europa pela mesma Convenção só poderá ser mantido se os requisitos enunciados nestes três pontos *supra* foram respeitados.

9.Beneficiam os cidadãos da UE de uma protecção adequada no tocante às actividades dos serviços de informações?

9.1. Protecção no tocante às actividades dos serviços de informações: uma função dos parlamentos nacionais

Uma vez que as actividades dos serviços de informações poderão futuramente ser cobertas pela PESC, mas não existem actualmente quaisquer disposições comunitárias na matéria[181], a organização da protecção dos cidadãos contra as actividades dos serviços de informações incumbe apenas aos sistemas jurídicos nacionais.

Neste contexto, os parlamentos nacionais desempenham um papel duplo: enquanto legisladores, tomam decisões sobre a natureza e os poderes dos serviços de informações, bem como sobre a organização do controlo das suas actividades. Tal como exposto pormenorizadamente no capítulo anterior, quando abordam a questão da admissibilidade da vigilância das telecomunicações, os parlamentos nacionais devem respeitar os limites fixados no artigo 8º da CEDH, isto é, as disposições devem ser necessárias e proporcionais e as suas implicações para os indivíduos devem ser previsíveis. Além disso, os poderes das agências de vigilância devem ser submetidos a mecanismos de controlo adequados e eficazes.

Por outro lado, os parlamentos nacionais desempenham na maior parte dos países um papel activo de controlo, dado que, a par da adopção de legislação, o controlo do executivo (e, por conseguinte, também dos serviços de informações) é a segunda função "clássica" de um parlamento. Contudo, os parlamentos dos Estados-Membros da UE desempenham esta tarefa de maneiras muito diferentes, frequentemente com base na cooperação entre órgãos parlamentares e não parlamentares.

9.2. Poderes das autoridades nacionais em matéria de execução de medidas de vigilância

De um modo geral, o Estado pode tomar medidas de vigilância num contexto penal, para preservar a ordem e para garantir a segurança nacional (em relação ao estrangeiro).[182]

No contexto penal, o sigilo das telecomunicações pode ser quebrado em todos os Estados-Membros, desde que exista uma suspeita fundamentada de que um crime foi perpetrado (eventualmente em circunstâncias particularmente agravantes) por uma pessoa específica.

[181] *Vide* capítulo 7.

[182] Estes objectivos são reconhecidos como justificação para a ingerência na vida privada pelo nº 2 do artigo 8º da CEDH. *Vide* ponto 8.3.2 supra.

Atendendo à gravidade da intervenção, é geralmente exigida a autorização de um magistrado[183]. Existem indicações precisas quanto à duração da vigilância, ao controlo da mesma e à eliminação dos dados recolhidos.

Para garantir a segurança nacional e a ordem pública, as possibilidades de intercepção são alargadas para além de investigações individuais em caso de suspeitas concretas. Com vista a detectar antecipadamente os movimentos extremistas ou subversivos, o terrorismo ou a criminalidade organizada, o legislador nacional autoriza a recolha de informações sobre determinadas pessoas ou grupos. A recolha dessas informações e a sua análise são efectuadas por serviços especiais internos de informações.

Por último, uma proporção substancial das medidas de vigilância é executada com o objectivo de garantir a segurança do estado. De um modo geral, a responsabilidade pelo tratamento, a análise e a apresentação das informações sobre indivíduos ou países estrangeiros cabe a um serviço de informações externo[184]. Em geral, os objectivos da vigilância não são pessoas específicas, mas determinados sectores ou frequências. Em função dos meios de que dispõe o serviço de informações externo, bem como dos seus poderes legais, as operações de vigilância podem cobrir um amplo espectro que vai das informações via rádio de carácter puramente militar (ondas curtas) à vigilância de todos os tipos de telecomunicações com o estrangeiro. Em alguns Estados-Membros, a vigilância das telecomunicações para fins puramente de espionagem é simplesmente proibida[185]. Noutros, essa vigilância pode, em alguns casos, sob reserva de autorização de uma comissão independente[186], ser autorizada por um ministro[187], sem restrições relativamente a alguns meios de comunicação[188]. Os poderes relativamente importantes de muitos serviços de informações externos podem ser explicados pelo facto de assegurarem a vigilância das comunicações com o estrangeiro, que apenas dizem respeito a uma pequena proporção dos seus cidadãos, pelo que suscitam pouco interesse.

9.3. Controlo dos serviços de informações

Um controlo eficaz e global é particularmente importante para duas razões: por um lado, porque os serviços de informações trabalham em segredo e numa base a longo prazo, pelo que as pessoas interessadas ignoram durante muito tempo ou (em função da sua situação jurídica) nada sabem sobre a vigilância efectuada; por outro lado, porque a vigilância diz com frequência

---

[183] Com excepção do direito britânico, que confia a decisão de autorização ao Ministro do Interior (Regulation of Investigatory Powers Act 2000, section 5 (1) and (3) (b).

[184] Sobre a actividade dos serviços de informações estrangeiros v*ide* a explanação circunstanciada constante do capítulo 2.

[185] Por exemplo, Áustria e Bélgica.

[186] Por exemplo, na Alemanha, ("Gesetz zur Beschränkung des Brief-, Post-, und Fernmeldegeheimnisses (Gesetz zu Artikel 10 Grundgesetz)". Nos termos do nº 9, excepto nos casos em que exista o risco de o atraso frustrar a operação, a comissão deve ser informada antes de a vigilância ser levada a cabo.

[187] Por exemplo, no Reino Unido ("Regulation of Investigatory Powers Act, Section 1") e em França ("Art. 3 une 4 Loi 91-646 du 10 Juillet 1991, loi relative au secret des correspondances émises par la voie des télécommunications").

[188] Por exemplo, em França ("Art. 20 Loi 91-646 du 10 Juillet 1991, loi relative au secret des correspondances émises par la voie des télécommunications").

respeito a grupos de grandes dimensões e de contornos mal definidos, por forma a que o Estado possa obter rapidamente um volume muito grande de dados pessoais.

Independentemente da sua estrutura, todos os organismos de controlo se defrontam com o mesmo problema: devido à natureza particular dos serviços secretos, é frequentemente muito difícil determinar se todas as informações necessárias foram de facto fornecidas, ou se uma parte das mesmas foi retida. Por conseguinte, a regulamentação deve ser feita com muito cuidado. Em princípio, podemos considerar que a eficácia dos controlos e, por conseguinte, a garantia da sua legalidade, é assegurada quando a possibilidade de ordenar uma vigilância das telecomunicações cabe às mais altas autoridades administrativas, quando a sua realização necessita da autorização prévia de um juiz e quando um órgão independente controla a realização das operações. Além disso, é desejável, por razões que se prendem com a democracia e o Estado de direito, que os serviços de informações no seu conjunto sejam submetidos ao controlo de um órgão parlamentar, em conformidade com o princípio da divisão de poderes.

Na Alemanha, estas condições encontram-se largamente preenchidas. Neste país, as medidas de vigilância das telecomunicações são ordenadas, a nível nacional, pelo ministro federal competente. Salvo em caso de urgência, uma comissão independente, não vinculada por instruções do governo (Comissão G10[189]), deve ser informada e é ela que decide da necessidade e da admissibilidade da medida proposta. Nos casos em que os Serviços Federais de Informações (BND) são autorizados a praticar uma vigilância das telecomunicações não-cabo recorrendo à filtragem com base em chaves de pesquisa, a comissão decide igualmente quanto à admissibilidade dessas chaves. Incumbe ainda à Comissão G10 controlar a notificação, prevista pela lei, ao interessado, bem como a destruição dos dados recolhidos pelos BND.

Existe ainda um órgão de controlo parlamentar (PKGr)[190] composto por nove deputados do Bundestag, encarregado de fiscalizar as actividades dos três serviços de informações alemães. O PKGr tem o direito de consultar os dossiês, de ouvir os agentes dos serviços de informações, de visitar as instalações dos serviços e de ser informado; este último direito só lhe pode ser negado por razões imperativas de acesso à informação ou por razões de protecção dos direitos à privacidade de terceiros, ou quando está em jogo a responsabilidade do próprio executivo. As deliberações do PKGr são secretas e os seus membros têm o dever de guardar sigilo, mesmo depois de cessarem funções. A meio e no final da legislatura, este órgão apresenta ao Bundestag um relatório das suas actividades de controlo.

Contudo, um controlo de tal modo abrangente dos serviços de informações constitui uma excepção entre os Estados-Membros.

Em França[191], por exemplo, apenas as medidas de vigilância que implicam a intercepção de um cabo exigem a autorização do Primeiro-Ministro. Apenas estas actividades são submetidas à fiscalização de uma comissão criada para o efeito (Commission nationale de contrôle des interceptions de sécurité), que é composta por um deputado e um senador. A autorização de uma

---

[189] Para mais pormenores, ver "O Controlo Parlamentar dos Serviços de Informações na Alemanha", situação em 9.9.2000, publicado pelo Bundestag, Secretariado do Órgão de Controlo Parlamentar.

[190] Lei sobre o controlo das actividades dos serviços federais de informação (PKGrG) de 17 de Junho de 1999 BGBI I 1334 idgF.

[191] Loi 91-646 du 10 Juillet 1991, loi relative au secret des correspondances émises par la voie des telécommunications.

escuta solicitada por um ministro ou o seu delegado é submetida ao presidente da comissão, que, em caso de dúvida quanto à legalidade da operação, pode consultar a comissão, que formula recomendações e, caso haja suspeitas de violação de uma lei susceptível de procedimento penal, informa o Ministério Público. As operações de escuta para fins de defesa dos interesses nacionais que implicam a intercepção de comunicações via rádio, bem como as comunicações por satélite, não estão sujeitas a qualquer restrição e escapam, por conseguinte, ao controlo de uma comissão.

Além disso, as actividades dos serviços de informações franceses não estão sujeitas ao controlo de uma comissão parlamentar especial; contudo, estão em curso diligências nesse sentido. A Comissão da Defesa da Assembleia Nacional aprovou já uma proposta[192] que ainda não foi debatida em plenário.

No Reino Unido, todas as operações de vigilância praticadas no solo britânico carecem da autorização do Ministro do Interior. Contudo, o texto da lei não indica claramente se a intercepção não orientada de comunicações verificadas mediante a utilização de palavras-chaves está coberta pela noção de "intercepção" utilizada na "Regulation of Investigatory Powers Act 2000" (RIP) quando as comunicações interceptadas não são analisadas em solo britânico, mas transmitidas tal e qual para o exterior, sem avaliação. O controlo do respeito das disposições da RIP 2000 é efectuado *ex post* por "comissários", altos magistrados aposentados ou em funções, nomeados pelo Primeiro-Ministro. O comissário encarregado da intercepção ("Interception Commissioner") controla a concessão das autorizações de intercepção e fornece apoio às investigações de queixas relativas às intercepções. O "Intelligence Service Commissioner" controla as autorizações concedidas para as actividades dos serviços de informações e de segurança e fornece apoio às investigações de queixas respeitantes a estes serviços. O "Investigatory Powers Tribunal", que é presidido por um alto magistrado, investiga todas as queixas referentes às medidas de intercepção e às actividades dos serviços.

O controlo parlamentar é assegurado pela "Intelligence and Security Committee" (ISC)[193] que fiscaliza as actividades dos três serviços de informações civis (MI5, MI6 e GCHQ). É responsável, nomeadamente, pelo controlo das despesas e da gestão, bem como das actividades do serviço de segurança, do serviço de informações e do GCHQ. Esta comissão é composta por nove membros das duas câmaras do Parlamento e não pode contar com ministros no seu seio. Ao contrário das comissões de controlo de outros países, que são geralmente eleitas ou designadas pelo parlamento nacional ou pelo presidente do parlamento, esta comissão é nomeada pelo Primeiro-Ministro após consulta do líder da oposição.

Estes exemplos demonstram claramente que os níveis de protecção são muito diferentes. No que se refere ao controlo parlamentar, o relator gostaria de assinalar que a existência de comissões encarregadas de fiscalizar as actividades dos serviços de informações é muito importante: relativamente às comissões parlamentares normais, estas comissões têm a vantagem de beneficiarem da confiança dos serviços de informações, uma vez que os seus membros têm o dever de guardar sigilo e as suas reuniões são realizadas à porta fechada. Além disso, estas

---

[192] Ver "Proposition de loi tendant à la création de délégations parlementaires pour le renseignement", e o relatório conexo do deputado *Arthur Paecht*, Rapport fait au nom de la Commission de la défense nationale et des forces armées sur la proposition de loi (N° 1497) de M. Paul Quilès et plusieurs de ses collègues tendant à la création d'une délégation parlementaire pour les affaires de renseignement, enregistré`à la Présidence de L'Assemblée nationale le 23 novembre 1999.

[193] Intelligence services act 1994, Section 10

comissões dispõem de poderes especiais para o desempenho das suas funções, o que é indispensável para fiscalizar as actividades no domínio dos serviços secretos.

Felizmente, a maior parte dos Estados-Membros da UE criou comissões parlamentares de controlo para fiscalizar as actividades dos serviços de informações. Na Bélgica[194], na Dinamarca[195], na Alemanha[196], na Itália[197], nos Países Baixos[198] e em Portugal[199] existem comissões parlamentares que asseguram o controlo dos serviços de informações militares e civis. No Reino Unido[200], a comissão especial de controlo apenas se ocupa dos serviços de informações civis (manifestamente mais importantes) e o serviço de informações militares é controlado pela Comissão da Defesa. Na Áustria[201], os dois ramos do serviço de informações são controlados por duas comissões distintas, que, contudo, são organizadas na mesma maneira e beneficiam dos mesmos direitos. Nos Estados nórdicos da Finlândia[202] e da Suécia[203] o controlo parlamentar é assegurado por um *Ombudsman* independente e eleito pelo parlamento. Em França, na Grécia, na Irlanda, no Luxemburgo e em Espanha não existe uma comissão parlamentar especializada; nestes países, o controlo é assegurado pelas comissões no âmbito das actividades parlamentares gerais.

9.4. Análise da situação para os cidadãos europeus

Na Europa, a situação para os cidadãos europeus é pouco satisfatória. Os poderes dos serviços de informações em matéria de vigilância das telecomunicações apresentam diferenças consideráveis, e o mesmo se aplica aos poderes das comissões de controlo. Nem todos os Estados-membros que possuem serviços de informações criaram organismos parlamentares de

---

194 Comité permanent de contrôle des services de renseignements et de sécurité, Comité permanent R, Loi du 18 juillet 1991 /IV, organique du contrôle des services de police et de renseignements.

195 Udvalget vedrørende efterretningstjenesterne, Lov om etablering af et udvalg om forsvarets og politiets efterretningstjenester, lov 378 af 6/7/88.

196 Das parlamentarische Kontrollgremium (PKGr), Gesetz über die Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (PKGrG)vom 17. Juni 1999 BGBl I 1334 idgF.

197 Comitato parlamentare, L. 24 ottobre 1977, n. 801, Art. 11, Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato.

198 Tweede-Kamercommissie voor de Inlichtingen- en Veiligheidsdiensten, 17. Reglement van orde van de Tweede Kamer der Staten-General, Art. 22.

199 Conselho de Fiscalização dos Serviços de Informações (CFSI), Lei 30/84, de 5 de Setembro de 1984, com a redacção que lhe foi dada pela Lei 4/95, de 21 de Fevereiro de 1995, a Lei 15/96, de 30 de Abril de 1996 e a Lei 75-A/97, de 22 de Julho de 1997.

200 Intelligence and Security Committee (ISC), intelligence services act 1994, Section 10.

201 Ständiger Unterausschuss des Landesverteidigungsausschusses zur Überprüfung von nachrichtendienstlichen Maßnahmen zur Sicherung der militärischen Landesverteidigung und Ständiger Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit, Art. 52a B-VG, §§ 32b ff Geschäftsordnungsgesetz 1975.

202 Ombudsmann, gesetzliche Grundlage für die Kontrolle für die Polizei (SUPO): Poliisilaki 493/1995 §33 und Laki pakkokeinolain 5 a luvun muuttamisesta 366/1999 §15, für das Militär: Poliisilaki 493/1995 §33 und Laki poliisin tehtävien suorittamisesta puolustusvoimissa 1251/1995 §5.

203 Rikspolisstyrelsens ledning, Förordning (1989:773) med instruktion för Rikspolisstyrelsen (Verordnung (1989:773) über die nationale Polizeibehörde).

controlo independentes, dotados de poderes de controlo apropriados. Ainda estamos muito longe de um nível de protecção uniforme.

Do ponto de vista europeu, tal é tanto mais lamentável quanto a situação não afecta principalmente os cidadãos dos Estados cujo comportamento eleitoral pode influenciar o nível de protecção. O impacto adverso é sentido sobretudo pelos cidadãos de outros Estados, uma vez que os serviços de informações externos, por definição, desenvolvem as suas actividades no estrangeiro. O cidadão está relativamente indefeso face aos sistemas estrangeiros, pelo que a necessidade de protecção é ainda maior. Além disso, há que ter em mente que, em virtude da natureza específica dos serviços de informações, os cidadãos da UE podem ser afectados pelas actividades de diversos serviços de informações ao mesmo tempo. Neste contexto, seria desejável um nível de protecção uniforme e conforme com os princípios democráticos. Deveria igualmente ser considerada a questão de saber se, neste contexto, as disposições relativas à protecção de dados são exequíveis a nível da UE.

Além disso, a questão da protecção dos cidadãos europeus colocar-se-á em termos completamente novos quando, no âmbito de uma política de segurança comum, a cooperação entre os serviços de informações dos Estados-Membros se tornar uma realidade. As instituições europeias serão chamadas a adoptar disposições de protecção adequadas. Incumbirá ao Parlamento Europeu, defensor do princípio do Estado de direito, a tarefa de exigir os poderes de que necessita, enquanto órgão que dispõe de uma legitimidade democrática, para exercer um controlo apropriado. O Parlamento Europeu deverá igualmente tomar disposições para garantir o tratamento confidencial de dados sensíveis e de outros documentos secretos por uma comissão especializada cujos membros tenham o dever de guardar sigilo. Apenas quando estas condições foram preenchidas será realista reivindicar estes poderes de controlo com vista a assegurar uma cooperação eficaz entre os serviços de informações, cooperação essa indispensável para uma verdadeira política de segurança comum.

10. A protecção contra a espionagem económica

10.1. A economia como alvo da espionagem

Do ponto de vista da confidencialidade, existem nas empresas três tipos de informações. Por um lado, informações que gozam deliberadamente **da maior difusão possível**, entre as quais se incluem informações objectivas sobre os produtos da empresa (p. ex. características dos produtos, preços, etc.) e informações publicitárias que influenciam a imagem da empresa.

Em segundo lugar, existem informações que **não são protegidas nem difundidas activamente**, por nada terem a ver com a posição concorrencial da empresa. Tal sucede, por exemplo, com a data do passeio da empresa, a ementa da cantina ou a marca dos aparelhos de fax utilizados.

Por último, existem informações que são **protegidas do acesso por parte de terceiros**. Tais informações são protegidas da concorrência, mas também do Estado, quando uma empresa não pretende cumprir a legislação (impostos, regras de embargo, etc.). Encontram-se previstos diversos níveis de protecção, até ao segredo absoluto, p. ex. no que diz respeito aos resultados da investigação antes de serem patenteados, ou no caso da produção de armamento[204].

No caso em apreço, a espionagem tem a ver com a obtenção de informações mantidas secretas por uma empresa. Se o transgressor é uma empresa concorrente, fala-se de **espionagem de concorrência** (ou espionagem industrial). No caso de o transgressor ser um serviço de informações estatal, fala-se de **espionagem económica.**

10.1.1. Os objectivos da espionagem

Os dados estratégicos relevantes para a espionagem económica podem classificar-se por domínios ou por departamentos empresariais.

10.1.1.1. Domínios

Como é evidente, são de grande interesse informações provenientes dos seguintes domínios: biotecnologia, engenharia genética, tecnologia médica, tecnologia ambiental, grandes computadores, programas informáticos, optoelectrónica, tecnologia de imagem, de sensores e de sinais, armazenamento de dados, cerâmica técnica, ligas de alto rendimento e nanotecnologia. Esta lista não é exaustiva e encontra-se, aliás, em alteração permanente, de acordo com a evolução tecnológica. Nas áreas referidas, a espionagem consiste sobretudo na apropriação indevida de resultados da investigação ou de técnicas de produção especiais.

10.1.1.2. Departamentos empresariais

São logicamente alvo de espionagem os departamentos de investigação e desenvolvimento, de compras, de pessoal, de produção, de distribuição, de venda, de marketing, de linhas de produtos e financeiros. É frequentemente subestimada a importância e o valor dos dados em causa *(vide capítulo* 10, 10.1.4)

[204] Informationen für geheimschutzbetreute Unternehmen, Ministério Federal da Economia, 1997

10.1.2. *Espionagem da concorrência*

A posição estratégica de uma empresa no mercado depende da sua organização nos departamentos de investigação e desenvolvimento, processos de produção, linhas de produtos, de financiamento, de marketing, de vendas, de distribuição, de compras e de recursos humanos[205]. As informações sobre tais matérias são de grande interesse para todos os concorrentes, uma vez que fornecem elementos sobre projectos e pontos fracos, permitindo assim a adopção de contramedidas estratégicas.

Uma parte dessas informações está acessível ao público. Existem empresas de consultoria altamente especializadas que, dentro de toda a legalidade, elaboram análises de concorrência, entre as quais se encontram firmas de renome como p. ex. Roland & Berger, na Alemanha. Nos Estados Unidos, a "Competitive Intelligence" faz actualmente parte do instrumentário básico de gestão[206]. A partir de uma multiplicidade de informações individuais, é elaborado de modo profissional um quadro claro da situação.

A transição da legalidade para a espionagem ilegal da concorrência decorre da escolha dos instrumentos para obtenção de informações. Só a partir do momento em que os instrumentos utilizados são ilegais na respectiva ordem jurídica se entra no domínio da criminalidade; a elaboração de análises não é, em si mesma, punível. As informações especialmente interessantes para um concorrente são obviamente protegidas e apenas podem ser obtidas por meios ilegais. As técnicas então utilizadas em nada se distinguem dos métodos gerais de espionagem descritos no Capítulo 2.

Não existem indicações exactas sobre a amplitude da espionagem de concorrência. À semelhança da espionagem clássica, os números ocultos são extremamente elevados. Nenhuma das partes implicadas (transgressor e vítima) tem interesse em publicidade. Para as empresas atingidas, tal significa sempre uma perda de imagem, e os transgressores também não têm obviamente qualquer interesse na publicitação das suas actividades. Por tal motivo, só poucos casos são levados a tribunal.

No entanto, surgem repetidamente informações na imprensa sobre espionagem de concorrência. Para além disso, o relator debateu a matéria com alguns responsáveis pela segurança de grandes empresas alemãs[207] e com gestores de empresas norte-americanas e europeias. Em resumo, pode concluir-se que são constantemente detectados casos de espionagem de concorrência, embora os mesmos não determinem a actividade quotidiana.

10.2. Prejuízos causados pela espionagem económica

A existência de números ocultos elevados não permite quantificar com rigor a amplitude dos prejuízos causados pela espionagem de concorrência/económica. Acresce ainda o facto de uma parte dos números referidos ser inflacionada em obediência a diversos interesses. As empresas de segurança e os serviços de contra-espionagem têm obviamente interesse em situar os prejuízos no topo superior da escala possível. Em todo o caso, os números transmitem uma determinada ideia.

---

[205] *Michael E. Porter*, Competitive Strategy, Simon & Schuster (1998)

[206] *Roman Hummelt*, Wirtschaftsspionage auf dem Datenhighway, Hanser Verlag (1997)

[207] Pormenores e nomes protegidos.

Já em 1988, o Instituto Max Planck avaliava os prejuízos causados pela espionagem económica na Alemanha em pelo menos 8.000 milhões de DM[208]. O presidente da associação de empresas de consultoria de segurança na Alemanha, Klaus-Dieter Matschke, indica, invocando o parecer de peritos, o montante de 15.000 DM/ano. Hermann Lutz, presidente dos sindicatos de polícia europeus, avalia os prejuízos em 20 mil milhões de DM anuais. O FBI[209] refere, para o período de 1992/1993, um prejuízo de 1,7 mil milhões de dólares, sofrido pela economia norte-americana devido à espionagem económica e de concorrência. O ex-presidente da Comissão de Controlo dos Serviços Secretos da Câmara dos Representantes dos EUA fala de 100 mil milhões de dólares de prejuízos, devido a encomendas perdidas e a custos adicionais de investigação e desenvolvimento. Entre 1990 e 1996, tais práticas terão tido como consequência a perda de 6 milhões de postos de trabalho.[210]

A bem da verdade, não se revela necessário conhecer exactamente a ordem de grandeza do prejuízo. A obrigação que cabe ao Estado de, conjuntamente com as forças policiais e os serviços de contra-espionagem, agir contra a espionagem económica e da concorrência é independente do valor do prejuízo económico. Os dados relativos aos prejuízos totais são destituídos de utilidade para a tomada de decisões, a nível empresarial, relativamente à protecção de informações e à adopção, por parte da empresa, de medidas de contra-espionagem. Todas as empresas têm de calcular o prejuízo máximo que são passíveis de sofrer na sequência do furto de informações, avaliar a probabilidade de tal ocorrência e comparar os montantes assim calculados com os custos da segurança. O problema real consiste, não na ausência de dados concretos em matéria de prejuízos totais, mas sim no facto de, excepção feita às grandes empresas, todas as outras raramente procederem a cálculos de custos/benefícios, secundarizando, por conseguinte, a segurança.

10.3. Quem pratica a espionagem?

Segundo um estudo da sociedade de auditoria Ernest Young LLP[211], os principais mandantes de práticas de espionagem empresarial são concorrentes em 39% dos casos, clientes em 19%, fornecedores em 9% e serviços secretos em 7%. A espionagem é praticada por trabalhadores da própria empresa, por empresas privadas de espionagem, por piratas informáticos pagos e por profissionais dos serviços secretos.[212]

10.3.1. Trabalhadores da própria empresa (delitos de iniciados)

A bibliografia utilizada, os dados sobre a matéria referidos por peritos à comissão, bem como as trocas de pontos de vista entre o relator e responsáveis por serviços de segurança e de contra-espionagem, convergem no sentido de mostrar que o maior perigo de espionagem provém de trabalhadores desiludidos e insatisfeitos. Na qualidade de assalariados da empresa, dispõem de acesso directo a informações, deixam-se comprar e revelam segredos da empresa a quem lhes paga.

---

[208] IMPULSE,3/97,S.13 ff.

[209] *Louis J. Freeh*, Director FBI, Statement for the Record, Hearing on Economic Espionage, House Judiciary Committee, Subcommittee on Crime, Washington D.C., 9.5.1996

[210] *Robert Lyle*, Radio Liberty/Radio fre Europe, 10.Februar 1999

[211] Computerzeitung, 30.11.1995, S.2

[212] *Roman Hummelt*, Spionage auf dem Datenhighway, (1997), S.49ff

Existem também elevados riscos relacionados com a mudança de profissão. Actualmente não é necessário copiar montanhas de papel a fim de poder transportar informações importantes para fora da empresa. Tais informações podem ser armazenadas em disquete sem que ninguém se aperceba e fornecidas ao novo empregador, em caso de mudança de emprego.

10.3.2. Empresas de espionagem privadas

Aumenta constantemente o número de empresas especializadas na espionagem de dados. Em alguns casos, trabalham nelas antigos colaboradores de serviços de informações. As empresas em causa operam frequentemente na área da consultoria de segurança, como também da investigação, fornecendo informações por encomenda. De um modo geral, são utilizados métodos legais, existindo todavia empresas que recorrem a métodos ilegais.

10.3.3. Piratas informáticos

Os piratas informáticos são especialistas em computadores que conseguem obter, graças aos seus conhecimentos, acesso a redes informáticas a partir do exterior. Durante os primeiros anos, eram sobretudo maníacos de computadores que se divertiam a ultrapassar os dispositivos de segurança dos sistemas informáticos. Actualmente existem piratas informáticos que trabalham por encomenda, tanto junto de serviços como no mercado.

10.3.4. Serviços de informações

Após o termo da Guerra Fria, as tarefas dos serviços de informações reconheceram uma transformação. A criminalidade internacional organizada e a economia constituem novos domínios de actividade (para mais pormenores, *vide* Capítulo 10, 10.5).

10.4. Como se processa a espionagem?

De acordo com as informações de entidades responsáveis pela contra-espionagem e pela segurança de grandes empresas, a espionagem económica recorre a todos os métodos e instrumentos testados dos serviços de informações (*vide* Capítulo 2, 2.4). Todavia, as empresas dispõem de estruturas mais abertas do que as instituições militares e de informações ou serviços governamentais. Por tal motivo, a espionagem económica apresenta os seguintes riscos acrescidos:

- É mais fácil aliciar colaboradores, uma vez que as possibilidades oferecidas pela segurança das empresas não são comparáveis às dos serviços de contra-espionagem;
- A mobilidade do posto de trabalho leva a que sejam transportadas informações importantes no computador portátil. O roubo de tais aparelhos ou a cópia clandestina do disco duro após intrusão num quarto de hotel são, pois, técnicas habituais da espionagem industrial;
- A intrusão em redes informáticas é mais fácil do que quando se trata de organismos públicos, sensíveis à segurança, justamente porque as pequenas e médias empresas não se encontram sensibilizadas para os problemas de segurança e adoptam menores precauções;
- As escutas (*vide* Capítulo 3, 3.2) são, pelos mesmos motivos, mais fáceis.

A análise das informações colhidas mostra que a espionagem económica se efectua principalmente *in loco* ou num posto de trabalho móvel uma vez que as informações procuradas

não podem ser obtidas, com raras excepções (*vide infra* Capítulo 10, 10.6) através da escuta das redes de telecomunicações internacionais.

10.5. Espionagem económica praticada por Estados

10.5.1. Espionagem económica estratégica praticada por serviços de informações

Após o termo da Guerra Fria, foram libertadas capacidades dos serviços de informações, que, mais do que outrora, são actualmente utilizadas noutros domínios. Os EUA declaram abertamente que uma parte das suas actividades de informações implica também a economia, incluindo por exemplo o controlo da aplicação de sanções económicas, o controlo da aplicação das normas relativas a fornecimentos de armas e dos chamados bens de uso dual, a evolução dos mercados de matérias-primas e os acontecimentos nos mercados financeiros internacionais. Segundo o que o relator pôde apurar, os serviços norte-americanos não são os únicos a operar nesse domínio, e tal não constitui objecto de uma reprovação maciça.

10.5.2. Serviços de informações como agentes de espionagem da concorrência

São formuladas críticas nos casos em que se verifica uma utilização abusiva dos serviços de informações estatais para, através de espionagem, proporcionar vantagens na concorrência internacional às empresas que operam no respectivo território. Neste contexto, há que distinguir dois casos[213].

10.5.2.1. Estados de alta tecnologia

Os Estados industriais altamente desenvolvidos podem também beneficiar da espionagem industrial. Obtendo informações sobre o desenvolvimento numa determinada área, podem adoptar medidas próprias, no plano da economia externa ou da política de subsídios, que tornem a sua indústria mais concorrencial ou lhes permitam economizar subvenções. Outro aspecto importante pode consistir na obtenção de pormenores relativos a contratos de valor elevado (*vide infra* Capítulo 10, 10.6).

10.5.2.2. Estados menos desenvolvidos do ponto de vista técnico

Para alguns destes Estados, trata-se de obter conhecimentos técnicos, a fim de recuperar o atraso da sua indústria sem custos de desenvolvimento e sem despesas com licenças. Para além disso, trata-se de obter modelos de produtos e técnicas de produção, a fim de se manterem concorrenciais no mercado mundial, com cópias produzidas a custos (salários!) baixos. Está provado que essa tarefa foi atribuída aos serviços russos. A Lei Federal n° 5 da Federação Russa, relativa às informações sobre o estrangeiro, menciona expressamente a obtenção de informações económicas e técnico-científicas como missão dos serviços de informações.
Outros Estados (p. ex. Irão, Iraque, Síria, Líbia, Coreia do Norte, Índia e Paquistão) procuram obter informações para os seus programas nacionais de armamento, sobretudo no domínio nuclear, bem como das armas químicas e biológicas. Outra componente da actividade dos serviços desses Estados consiste na gestão de empresas de cobertura para a compra de bens de uso dual, sem levantar suspeitas.

[213] Comunicação privada de um serviço de contra-espionagem ao relator, fonte protegida

10.6. Será o ECHELON adequado à espionagem industrial?

O controlo estratégico das telecomunicações internacionais apenas permite obter informações úteis para a espionagem de concorrência de forma aleatória. De facto, as informações sensíveis encontram-se sobretudo nas próprias empresas, **de modo que a espionagem de concorrência consiste sobretudo em tentar, através de trabalhadores** ou de pessoas infiltradas, obter informações ou penetrar nas redes informáticas internas. Apenas nos casos em que são transmitidas para o exterior informações sensíveis, por cabo ou por satélite, é possível utilizar um sistema de controlo das telecomunicações para fins de espionagem de concorrência. Tal situação verifica-se sistematicamente nos três casos seguintes:

- Em empresas que operam em três regiões horárias, de modo que os resultados intermédios da Europa podem ser enviados para a América e, posteriormente, para a Ásia;

- Nos casos de videoconferências em empresas multinacionais, por cabo ou por satélite;

- Quando são negociados contratos importantes *in loco* (construção de instalações, de infra-estruturas de telecomunicações, criação de sistemas de transporte, etc.), devendo ser estabelecidas comunicações, a partir desse local, com a sede da empresa.

Quando, nos casos citados, as empresas não protegem as suas comunicações, a intercepção das mesmas fornece dados valiosos para fins de espionagem de concorrência.

10.7. Casos divulgados

Existem alguns casos de espionagem económica e de concorrência descritos na imprensa ou na bibliografia especializada. Foi estudada uma parte dessas fontes, fornecendo-se uma síntese dos resultados nos quadros seguintes. Referem-se brevemente os intervenientes, a data em que o caso ocorreu, os pormenores, o objectivo e as consequências do mesmo.
É flagrante que, por vezes, o mesmo caso é relatado de modos muito diferentes. Refira-se, a título de exemplo, o caso Enercon, no qual são descritos como "autores" a NSA, o Ministério da Economia dos EUA ou o concorrente que efectuou fotografias.

Caso	Quem	Quando	O quê	Como	Objectivo	Consequências	Fonte
Air France	DGSE	até 1994	Conversas entre homens de negócios em viagens	Foram descobertos microfones nas cabinas de 1ª classe da Air France – a companhia aérea apresentou desculpas públicas	Obtenção de informações	Não referidas	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ de Arno Schütze, 1/
Airbus	NSA	1994	Informações sobre negócio de aeronaves entre a Airbus e a companhia aérea saudita	Escuta de faxes e telefonemas entre as partes	Transmissão de informações às concorrentes norte-americanas Boeing e Mc-Donnell-Douglas	Americanos concluem a transacção no valor de 6 mil milhões de dólares	„Antennen gedreht“, Wirtschaftswoche Nr.46 / 9. de Novembro de 2000
Airbus	NSA	1994	Contrato de 6 mil milhões de dólares com a Arábia Saudita Revelação de suborno do consórcio europeu Airbus.	Escuta de faxes e telefonemas entre o consórcio europeu Airbus e a companhia aérea e o Governo sauditas sobre satélites de comunicações	Revelação de suborno	A McDonnel-Douglas, concorrente norte-americana da Airbus, conclui o negócio	Duncan Campbell em STOA 1999, Vol 2/5, com base em „Baltimore Sun, America's fortress of Spies“, by Scott Shane and Tom Bowman, 3.12.1995 e Washington Post, French Recent US Coups in New Espionnage, de William Drozdiak
BASF	Distribuidor	Não referido	Descrição do processo de produção de matéria-prima do creme para a pele da firma BASF (cosméticos)	Não referido	Não referido	Inexistentes, porque descoberto	„Nicht gerade zimperlich“, Wirtschaftswoche Nr.43 / 16. Outubro de 1992
Ministério da Economia DE	CIA	1997	Informações sobre produtos de alta tecnologia no Ministério da Economia	Intervenção do agente	Obtenção de informações	É descoberta a tentativa do agente e este é expulso	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ de Arno Schütze, 1/98
Ministério da Economia DE	CIA	1997	Antecedentes do processo Mykonos, Berlim, créditos Hermes relativos a exportações para o Irão, lista de empresas alemãs fornecedoras de produtos de alta tecnologia ao Irão	Agente da CIA descoberto quando o Embaixador dos EUA mantém conversações amigáveis com o director do serviço do Ministério da Economia competente para os países árabes (especialmente Irão)	Obtenção de informações	Não referidas O funcionário dirige-se a responsáveis da segurança alemã, os quais comunicam às autoridades norte-americanas que a operação da CIA é indesejada. O agente da CIA é seguidamente “retirado”.	„Wirtschaftsspionage. Die gewerbliche Wirtschaft im Visier fremder Nachrichtendienste“, Landesamt für Verfassungsschutz Baden-Württemberg, Estugarda, referente a 1998
Dasa	serviço de informações russo	1996 – 1999	Venda e entrega de documentos sobre a tecnologia de armamento, de uma empresa de Munique dedicada à tecnologia de defesa (segundo SZ / 30.05.2000: Rüstungskonzern Dasa in Ottobrunn)	2 alemães contratados	Obtenção de informações sobre mísseis dirigíveis, sistemas de armamento (defesa antitanque e antiaérea)	SZ / 30.05.2000: „(...) Traição sob o ponto de vista militar “não especialmente grave”. O mesmo se aplica aos prejuízos económicos, segundo determinou o tribunal.“	„Anmerkungen zur Sicherheitslage der deutschen Wirtschaft“, ASW; Bona, 2001 „Haftstrafe wegen Spionage für Russland“, SZ / 30. Maio de 2000

Embargo	BND	Cerca de	Nova exportação para a Líbia de tecnologia protegida por embargo (pela Siemens), entre outras	Escuta de telecomunicações	Revelação de transferência ilegal de armas e de tecnologia	Sem consequências especiais, os fornecimentos não são impedidos	"Maulwürfe in Nadelstreifen", Andreas Förster, p. 110

Caso	Quem	Quando	O quê	Como	Objectivo	Consequências	Fonte
Enercon	Perito em energia eólica de Oldenburg e trabalhadora de Kenetech	Não referido	Parque eólico da firma Enercon, de Aurich	Não referido	Não referido	Não referido	„Anmerkungen zur Sicherheitslage der deutschen Wirtschaft“, ASW; Bona, Abril de 2001
Enercon	NSA	Não referido	Aerogerador para produção de energia, desenvolvido pelo engenheiro frísio oriental Aloys Wobben	Não referido	Transmissão de referências técnicas de Wobbens a firma dos EUA	Firma dos EUA regista a patente do aerogerador de Wobben; (violação do direitos de patentes)	„Aktenkrieger“, SZ, 29. de Março de 2001
Enercon	Firma dos EUA Kenetech Windpower Corp	1994	Pormenores importantes de parque eólico de alta tecnologia (terminais e platinas)	Fotografias	Patenteado com êxito nos EUA	Enercon GmbH lsuspende projectos de penetração no mercado americano	„Sicherheit muss künftig zur Chefsache werden“, HB / 29 de Agosto de 1996
Enercon	Engenheiro W. de Oldenburgo e firma Kenetech dos EUA	Março 1994	Aerogerador tipo E-40 de Enercon	Engenheiro W. transmite conhecimentos, funcionária de Kenetech fotografa instalações e pormenores eléctricos	Kenetech: procede a investigações para proceder judicialmente, por violação de patente contra Enercon por aquisição ilegal de segredos da empresa; Segundo colaboradores da NSA, foram transmitidas à Kenetech informações detalhadas sobre a Enercon através do ECHELON.	Não referidas	„Klettern für die Konkurrenz“, SZ 13 de Outubro de 2000
Enercon	Kenetech Windpower	Antes de 1996	Dados para parque eólico de Enercon	Engenheiros da Kenetech-fotografam as instalações	Cópia das instalações pela Kenetech	É feita justiça à Enercon; é movido processo penal contra espiões; cálculo dos prejuízos: várias centenas de milhões de DM	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ de Arno Schütze, 1/98
Ministério do Comércio do Japão	CIA	1996	Negociações sobre quotas de importação de automóveis dos EUA para o mercado japonês	Pirataria informática no sistema de computadores do Ministério do Comércio do Japão	O intermediário americano Mickey Kantor deverá aceitar a oferta mais baixa	Kantor aceita a oferta mais baixa	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ de Arno Schütze, 1/98
Automóveis japoneses	Governo dos EUA	1995	Negociações sobre a importação de automóveis de luxo japoneses Informação sobre os níveis de emissões de automóveis japoneses	COMINT, sem outros pormenores	Obtenção de informações	Não referidas	Duncan Campbell em STOA 2/5 de 1999 com base no Financial Post, Kanada, 28.2.1998

Caso	Quem	Quando	O quê	Como	Objectivo	Consequências	Fonte
López	NSA	Não referido	Videoconferência de VW e López	Escuta a partir de Bad Aibling	Transmissão de informações à General Motors e Opel	Através de uma medida de escuta, o Ministério Público teria obtido "indicações muito precisas" para investigação	Capitão Erich Schmidt-Eenboom, do exército alemão, citado in „Wenn Freunde spionieren" www.zdf.msnbc.de/news/54637.asp?cp1=1
López	López e três colaboradores	1992 - 1993	Documentos e dados dos departamentos de investigação, planeamento, produção e compras (documentos para fábrica na Espanha, informações relativas aos custos de diversas séries, estudos de projectos, estratégias de aquisição e de poupança)	Recolha de material	Utilização dos documentos da General-Motors pela VW	Acordo extrajudicial. Em 1996, López demite-se da VW-. Aquele paga 100 milhões de dólares à GM/Opel (pretensos honorários de advogados) e adquire durante 7 anos peças sobressalentes no valor global de 1000 milhões de dólares.	„Wirtschaftsspionage. Die gewerbliche Wirtschaft im Visier fremder Nachrichtendienste", Landesamt für Verfassungsschutz Baden-Württemberg, Estugarda, referente a 1998
López	NSA	1993	Videoconferência entre José Ignacio López e Ferdinand Piëch, presidente da VW	Gravação da videoconferência e entrega da mesma à General Motors (GM)	Protecção dos segredos da empresa norte-americana GM, que López pretendia revelar à VW (listas de preços, projectos secretos sobre a nova fábrica de automóveis e novo modelo de carro pequeno)	López é denunciado, procedimento penal supenso em 1998 contra pagamento de sanções pecuniárias Sem consequências em relação à NSA	„Antennen gedreht", Wirtschaftswoche Nr.46 / 9 de Novembro de 2000 „Abgehört", Berliner Zeitung, 22 de Janeiro de 1996 „Die Affäre López ist beendet", Wirtschaftsspiegel, 28 de Julho de 1998 „Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?" de Arno Schütze, 1/98
Los Alamos	Israel	1988	Dois colaboradores do programa de investigação nuclear de Israel penetram no computador central do laboratório de armas nucleares de Los Alamos	Pirataria informática	Obtenção de informações sobre novo detonador para armans nucleares dos EUA	Sem consequências especiais, dado que os piratas informáticos fogem para Israel, onde um deles é detido transitoriamente. Não é referida oficialmente qualquer ligação com os serviços secretos de Israel.	"Maulwürfe in Nadelstreifen", Andreas Förster, p. 137
Contrabando	BND	Anos 70	contrabando de computadores para a RDA	Não referido	Revelação de transferência de tecnologia para o Bloco Leste	Sem consequências especiais, os fornecimentos não são impedidos	"Maulwürfe in Nadelstreifen", Andreas Förster, p. 113

Caso	Quem	Quando	O quê	Como	Objectivo	Consequências	Fonte
TGV	DGSE	1993	Cálculo de custos da Siemens Contrato para fornecimento de comboios de alta velocidade à Coreia do Sul	Não referido	Oferta a preços mais baixos	O fabricante de ICE perde o contrato a favor da Alcatel-Alsthom	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ de Arno Schütze, 1/98
TGV	Desconhecido	1993	Cálculo de custos da AEG e Siemens sobre contrato público com a Coreia do Sul para fornecimento de comboios de alta velocidade	Siemens queixa-se de escuta das ligações telefónicas e por fax na sua filial em Seoul	Vantagem negocial para a concorrente britânico-francesa GEC Alsthom	Contratantes decidem-se pela GEC Alsthom, embora a oferta alemã fosse melhor	„Abgehört“, Berliner Zeitung, 22 de Janeiro de1996
Thomson-Alcatel contra. Raytheon	CIA/ NSA	1994	atribuição pelo Brasil de um contrato à Thomson-Alcatel francesa no montante de milhares de mihões de dólares (1,4) para vigilância por satélite do Amazonas	Escuta das comunicações do vencedor do concurso (Thomson-Alcatel, FR)	Revelação de corrupção (pagamento de subornos)	Clinton queixa-se junto do Governo brasileiro; a instâncias do Governo dos EUA, nova atribuição do contrato à firma americana “Raytheon”	"Maulwürfe in Nadelstreifen", Andreas Förster, p. 91
Thomson-Alcatel contra Raytheon	O Ministério da Economia dos EUA “ter-se-á esforçado“	1994	Negociações sobre o projecto de vigilância por radar da floresta tropical brasileira, no montante de milhares de milhões	Não referido	Obtenção do contrato	As empresas francesas Thomson CSF e Alcatel perdem o contrato a favor da firma americana Raytheon	„Antennen gedreht“, Wirtschaftswoche Nr.46 / 9 de Novembro de 2000
Thomson-Alcatel contra Raytheon	NSA Ministério do Comércio		Negociações sobre projecto no montante de milhares de milhões de dólares (1,4) para vigilância do Amazonas (SIVA) Revelação de suborno do júri de selecção brasileiro. Observação de Campbell: Rayethon equipa a estação de escuta de Sugar Grove	Escuta da negociação entre a Thomson-CSF e o Brasil e transmissão dos resultados Raytheon Corp.	Revelação de corrupção Obtenção do contrato	Raythen obtém o contrato	Duncan Campbell, em STOA 1999, Vol 2/5 com base no New York Times, How Washington Inc makes a Sale, de David Sanger, 19.2.1995 e http://www:rayethon:com/sivam/contract:html
Thyssen	BP	1990	Contrato no valor de milhões para extracção de gás natural e petróleo no Mar do Norte	Escuta de faxes do vencedor do concurso (Thyssen)	Revelação de corrupção	BP processa Thyssen para obter indemnização	"Maulwürfe in Nadelstreifen", Andreas Förster, p. 92
VW	Desconhecido	„Anos transactos“	Não referido	p. ex. câmara de infravermelhos escondida num monte de terra, que transmite imagens via rádio	Obtenção de informações sobre novos desenvolvimentos	V W anuncia avultada perda de lucros	„Sicherheit muss künftig zur Chefsache werden“, HB / 29. de Agosto de 1996
VW	Desconhecido	1996	Circuito de testes da VW em Ehra-Lessien	Câmara oculta	Informações sobre novos modelos da VW	Não referidas	„Auf Schritt und Tritt“ Wirtschaftswoche Nr. 25, 11 de Junho de 1998

10.8. Protecção em relação à espionagem económica

10.8.1. Protecção jurídica

Na ordem jurídica de todos os Estados industriais são impostas sanções penais ao roubo de segredos de empresas. Como em todos os outros casos de direito penal, é variável o nível de protecção nacional assegurado. Todavia, como regra geral, a pena fica claramente aquém da prevista para espionagem no âmbito da segurança militar. Em muitos casos, apenas é proibida a espionagem de concorrência dirigida contra empresas nacionais, mas não contra empresas do estrangeiro. Tal acontece nos Estados Unidos da América.

As leis relevantes limitam-se a proibir, no fundamental, a actividade de espionagem de empresas industriais contra outras empresas industriais, sendo duvidoso que limitem igualmente a actividade de serviços de informações estatais, uma vez que estes se encontram autorizados a praticar o roubo de informações com base na legislação que os institui.

Um caso-limite seria aquele em que os serviços de informações pusessem à disposição de empresas individuais informações obtidas através de espionagem. Em circunstâncias normais, tal prática já não seria coberta pela legislação que confere competências especiais aos serviços de informações. No interior da UE, tal constituiria nomeadamente uma violação do Tratado CE.

Independentemente desse facto, seria muito difícil a uma empresa obter, na prática, protecção jurídica mediante recurso aos tribunais. As escutas não deixam vestígios, nem conduzem a provas utilizáveis em juízo.

10.8.2. Outros obstáculos à espionagem económica

O facto de os serviços de informações desenvolverem igualmente actividades no sector da economia, no sentido de obterem informações estratégicas gerais, é entretanto aceite entre os Estados. Todavia, esse "acordo de cavalheiros" é alvo de violação flagrante no caso da espionagem de concorrência a favor da indústria nacional. Se um Estado for acusado com provas, enfrenta problemas políticos graves. O mesmo se aplica também, ou sobretudo, a uma potência mundial como os EUA, cuja pretensão de liderança política global ficaria prejudicada de forma gritante. As potências médias poder-se-iam dar ao luxo de ver demonstrada a sua culpabilidade, mas não uma potência mundial.

Para além dos problemas políticos, coloca-se igualmente a questão prática de saber a que empresa individual deverão ser fornecidos os resultados da espionagem de concorrência. No domínio da construção aeronáutica, a resposta é simples porque apenas existem dois operadores a nível global. Em todos os outros casos, quando existem vários operadores que, para além do mais, não são públicos, é extremamente difícil privilegiar um deles. No que diz respeito à transmissão a empresas individuais de informações pormenorizadas sobre as ofertas dos concorrentes, no âmbito de concursos públicos internacionais seria ainda pensável que as informações obtidas por espionagem fossem transmitidas a todos os concorrentes do próprio país. Tal é especialmente verdadeiro quando existe uma estrutura de apoio acessível a todos os concorrentes nacionais, como é o caso do chamado *Advocacy Center*, nos EUA. No caso de apropriação ilícita de tecnologia, que deveria desembocar num registo de patente, já não seria obviamente possível uma igualdade de tratamento das empresas.

Tal constituiria um problema grave, sobretudo no sistema político norte-americano. Para o financiamento das suas campanhas eleitorais, os políticos norte-americanos dependem decisivamente de donativos da indústria nos seus círculos eleitorais. Se se tornasse manifesto um único caso de favorecimento de empresa individuais por serviços de informações, tal provocaria violentas reacções no sistema político. Conforme declarou, numa troca de pontos de vista com representantes da comissão, o ex-Director da CIA, Woolsey : "In this case the hill (i.e o Congresso dos EUA) would go mad!". Lá ter razão, tem!

10.9. Os EUA e a economia após o termo da guerra fria

O Governo norte-americano tem vindo, desde 1990, a equiparar de modo crescente a segurança económica e a segurança nacional. O relatório anual da Casa Branca "National Security Strategy"[214] salienta reiteradamente que **"a segurança económica constitui parte integrante, não só dos interesses nacionais, mas também da segurança nacional".**

Várias foram as causas deste processo, causas essas decorrentes da confluência de três factores:

- o interesse dos serviços de informações numa missão que sobrevivesse à guerra fria;
- o mero reconhecimento do Ministério norte-americano dos Negócios Estrangeiros de que, uma vez terminada a guerra fria, o papel de liderança dos EUA a nível mundial terá, no futuro, de fundamentar-se, não só na força militar, mas também na solidez económica;
- o interesse político do Presidente Clinton no reforço da economia americana e na criação de postos de trabalho.

Esta conjugação de interesses da Administração norte-americana revestiu-se de consequências de ordem prática.

Assim sendo, o FBI concentrou, desde 1992, as suas actividades de contra-espionagem na espionagem económica, tendo implementado, em 1994, um "Economic Counterintelligence Program". Segundo declarações proferidas pelo Director do FBI, Freeh, perante o Parlamento, trata-se de um programa **defensivo** que visa obviar a que a competitividade da economia norte-americana seja enfraquecida pelo furto de informações.

Tal implica, pelo menos na perspectiva americana, que o Governo recorra à CIA e, subsequentemente, à NSA, visando a defesa contra distorções da concorrência por suborno. O então Director da CIA James Woolsey declarou-o expressamente no decurso de uma conferência de imprensa pelo mesmo dada, em 7 de Março de 2000, a pedido do Ministério dos Negócios Estrangeiros norte-americano.[215]

Assim sendo, o Ministério do Comércio norte-americano coordenou as suas actividades de promoção da exportação de tal modo que uma empresa norte-americana apenas tem um interlocutor quando pretende exportar. Neste contexto, a coordenação de todas as possibilidades do Governo visando um efeito concentrado processa-se, não só de modo passivo, mas também activo (Cf Capítulo 10, 10.9.4).

[214] Estratégia de segurança nacional

[215] State Department Foreign Press Center Briefing, Subject: Intelligence Gathering and Democracies: The Issue of Economic and Industrial Espionage, Washington DC, 7.3.2000

10.9.1. Repto para o Governo norte-americano: espionagem económica contra empresas norte-americanas

As operações desenvolvidas por serviços de informações contra a economia americana não são invulgares nem inéditas. Quer os EUA, quer outros importantes Estados industrializados constituiram, ao longo de décadas, alvo da espionagem económica. Todavia, a aquisição de informações científicas e tecnológicas representou, durante a guerra fria, um suplemento da espionagem clássica. Após o termo da guerra fria, a espionagem económica estabeleceu-se como objectivo próprio.[216]

O Director do FBI, Louis J. Freeh, declarou circunstanciadamente, em 1996, perante o Congresso norte-americano que a economia dos EUA constituia alvo de espionagem económica por parte dos serviços de informações de outros Estados. Afirmou, *inter alia,* o seguinte: "Assim sendo, cidadãos, empresas e indústrias americanos, bem como o próprio Governo dos EUA, constituem um alvo de Governos estrangeiros que recorrem a toda uma panóplia de medidas tendentes ao furto ou à obtenção ilegal de tecnologias específicas, dados e informações, por forma a adquirir vantagens concorrenciais para as respectivas indústrias" nacionais.[217] Segundo o Director do FBI, também o furto de informações por parte de americanos acusa um incremento similar. As suas declarações perante o Parlamento americano serão, seguidamente, resumidos. O relator lamenta que o Governo norte-americano não tenha autorizado a uma delegação da comissão a realização de um diálogo com o FBI sobre estas questões. Tal teria viabilizado uma actualização das informações. Assim, o relator pressupõe que, no entender do Governo dos EUA, a audição que teve lugar perante a "House of Representatives" em 1996 reflecte a situação actual no tocante à ameaça de espionagem económica que impende sobre a economia americana, reportando-se, por conseguinte, a essa fonte.

10.9.1.1. Os intervenientes

Aquando da referida audição, o FBI procedia a investigações sobre as actividades de pessoas ou organizações de 23 países por espionagem económica contra os EUA. Alguns opositores ideológicos ou militares dos EUA prosseguem simplesmente as actividades que desenvolviam no período da guerra fria[218]. Em contrapartida, outros governos praticam a espionagem económica e tecnológica, embora sejam, desde há muito, aliados militares e políticos dos EUA, contexto em que, frequentemente, tiram partido do acesso facilitado a informações americanas. Alguns desenvolveram uma infraestrutura própria de processamento de informações sobre alta tecnologia e de utilização das mesmas no plano concorrencial com empresas norte-americanas. Não são nomeados países concretos, ainda que determinadas insinuações permitam inferir tratar-se da Rússia, de Israel e da França[219].

---

[216] Statement for the Record of *Louis J. Freeh*, Director FBI, Hearing on Economic Espionage, House Judiciary Committee, Subcommittee on Crime, Washington DC, 9.5.1996

[217] "Consequently foreign governments, through a variety of means, actively target U.S. persons, firms, industries and the U.S. government itself, to steal or wrongfully obtain critical technologies, data and information in order to provide their own industrial sectors with a competitive advantage."

[218] "The end of the Cold War has not resulted in a peace dividend regarding economic espionage", *Freeh*, Statement for the Record of *Louis J. Freeh*, Director FBI, Hearing on Economic Espionage, House Judiciary Committee, Subcommittee on Crime, Washington DC, 9.5.1996

[219] Interpretação, pelo relator, das declarações crípticas de *Louis J. Freeh* perante a comissão

10.9.1.2. Objectivos da espionagem económica

Os objectivos da espionagem económica enunciados pelo FBI não se distinguem das declarações constantes do Capítulo 10, 10.1.1.. Não obstante, a alta tecnologia e a indústria de defesa são indicadas como objectivos prioritários. Interessante é constatar que as informações relativas a candidaturas, contratos, clientes e informações estratégicas nestes domínios são consideradas como objectivos da espionagem económica cuja consecução requer uma estratégia **agressiva**[220]**.**

10.9.1.3. Métodos

No quadro do "Economic Counterintelligence Program", o FBI constatou a existência de uma vasta gama de métodos de espionagem. Regra geral, observa-se uma conjugação de métodos, sendo rara a utilização de um único. Segundo o FBI, a melhor fonte é a constituída por uma pessoa numa empresa ou numa organização, o que senão aplica apenas à realidade americana (*vide* Capítulo 10, 10.3. e 4). No âmbito da audição, o FBI relata a intervenção de pessoas para fins de espionagem, não referindo, surpreendentemente, o recurso a métodos electrónicos.

10.9.2. A atitude oficial do Governo dos EUA sobre a espionagem económica activa

O ex-Director da CIA, Woolsey, descreveu, no quadro de uma conferência de imprensa[221] e de um encontro com membros da comissão em Washington, a actividade de escuta dos serviços secretos dos EUA, que, seguidamente, será reproduzida em síntese:

1. Os EUA exercem vigilância sobre as telecomunicações internacionais, a fim de obter informações gerais sobre desenvolvimentos económicos, sobre fornecimentos de bens de uso dual e sobre o cumprimento de embargos.

2. Os EUA exercem vigilância dirigida à comunicação entre empresas individuais no âmbito de concursos para a adjudicação de contratos, a fim de impedir distorções do mercado através de suborno em prejuízo de empresas americanas. Todavia, Woolsey não apresentou quaisquer exemplos concretos, embora tenha sido instado a fazê-lo.

Segundo afirmaram, o suborno é proibido por lei às empresas americanas e os auditores económicos são obrigados a comunicar casos detectados de pagamento de subornos. No caso de se verificar a existência de suborno em contratos públicos graças à vigilância das telecomunicações, o Embaixador americano interviria junto do governo do respectivo país. As empresas americanas participantes no concurso não seriam, todavia, directamente informadas. Woolsey excluiu categoricamente a hipótese de se tratar de pura espionagem da concorrência.

As declarações feitas pelo Director em exercício da CIA, George J. Tenet, no decurso de uma audição realizada perante a comissão do controlo dos serviços secretos da "House of Representatives" em 12 de Abril de 2000, apresentam o mesmo teor:[222] "Não constitui política nem *praxis* dos EUA praticar espionagem, a fim de obter vantagens desleais para empresas americanas." Durante a mesma audição, Tenet acrescentou que, no caso de informações sobre

[220] Nestes domínios, a intercepção de comunicações constitui um método promissor!

[221] *James Woolsey*, Remarks at the Foreign Press Center, Transskript, 7.3.2000, http://cryptome.org/echelon-cia.htm

[222] „It is not the policy nor the practice of the U.S. to engage in espionage that would provide an unfair advantage to U.S. Companies“.

corrupção, tal seria transmitido a outras autoridades governamentais, por forma a que estas pudessem ajudar as empresas norte-americanas[223]. Em resposta à pergunta formulada pelo Deputado Gibbons, Tenet anuiu em que não existe qualquer proibição legal da espionagem da concorrência, referindo, porém, não a considerar necessária, porquanto os serviços não levam a efeito tais actividades.

O Presidente da comissão de controlo dos serviços secretos na "House of Representatives", Porter Goss, procedeu a uma apresentação análoga das actividades de intercepção no quadro de um encontro com o mesmo efectuado em Washington.

10.9.3. Situação jurídica em caso de corrupção de agentes públicos[224]

O suborno tendente à obtenção de contratos não constitui um problema europeu, mas sim um problema de alcance mundial. De acordo com o "Bribe Payers Index (BPI), publicado em 1999, pela "Transparency International", em que se procedia à classificação dos 19 principais países de exportação segundo a sua tendência para a corrupção activa, a Alemanha e os EUA partilham o 9º lugar. No referente à Suécia, à Áustria, aos Países Baixos, ao Reino Unido e à Bélgica, foi constatada uma *praxis* menor de suborno, sendo o respectivo nível apenas mais elevado em Espanha, França e Itália.[225]

A justificação americana para a prática da espionagem económica assenta na referência a práticas de corrupção de empresas europeias. Tal é questionável, não só pelo facto de atitudes incorrectas isoladas não poderem constituir uma justificação para acções de espionagem de alcance mundial, mas também e sobretudo pelo facto de a "lei do mais forte" apenas poder vingar num vazio jurídico.

Na Europa, procede-se legalmente contra a corrupção com veemência análoga à dos EUA. A existência de interesses idênticos conduziu, em 1997, à adopção da Convenção da OCDE sobre a luta contra a corrupção de agentes públicos estrangeiros nas transacções comerciais internacionais[226]. Este diploma obriga os Estados signatários a aplicarem sanções a actos de corrupção cometidos por agentes públicos estrangeiros e contém, a par da tipificação do crime, também disposições relativas a sanções, competência jurisdicional e aplicação.

A Convenção, que entrou em vigor em 15.2.1999, foi transposta e ratificada por todos os Estados-Membros da UE, excepção feita à Irlanda. Os EUA procederam à transposição da

---

[223] „As I indicated also in my testimony, there are instances where we learn, that foreign companies or their governments bribe, lie, cheat or steal their way to disenfranchise American companies. When we generate this information, we take it to other appropriate agencies, make them aware of it. They use that information through other means and channels to see if they can assist an American company. But we play defense, we never play offense, and we never will play offense."

[224] *Albin Eser, Michael Überhofer, Barbara Huber* (Eds), Korruptionsbekämpfung durch Strafrecht. Ein rechtsvergleichendes Gutachten zu den Bestechungsdelikten im Auftrag des Bayerischen Staatsministeriums der Justiz, edition iuscrim (1997)

[225] O grau oscila entre 10 (baixa taxa de suborno) e 0 (alta taxa de suborno): Suécia (8,3), Austrália (8,1), Canadá (8,1), Áustria (7,8), Suíça (7,7), Países Baixos (7,4), Reino Unido (7,2) Bélgica (6,8), Alemanha (6, 2), EUA (6,2), Singapura (5,7), Espanha (5,3), França (5,2), Japão (5,1), Malásia (3,9), Itália (3,7), Taiwan (3,5), Coreia do Sul (3,4), China (3,1).

http://www.transparency.org/documents/cpi/index.html#bpi

[226] Convention on Combating Bribery of Foreign Public Officials in International Business Transactions

http://www.oecd.org/daf/nocorruption/20nov1e.htm

Convenção adaptando em conformidade a lei "Foreign Corrupt Practices Act" (FCPA) de 1977, que prescreve a obrigatoriedade de registo contabilístico para as empresas e proíbe a corrupção de agentes públicos estrangeiros, por meio da lei "International Anti-Bribery and Fair Competition Act", promulgada em 1998.[227] Nem nos EUA, nem nos Estados-Membros da UE, são dedutíveis, a título de despesa das empresas, "luvas" pagas a agentes públicos estrangeiros.[228]

Enquanto que a Directiva da OCDE apenas tem como alvo a luta contra a corrupção de agentes públicos estrangeiros, foram adoptados, no quadro do Conselho da Europa, em 1999, duas Convenções de maior alcance, as quais, contudo, ainda não entraram em vigor. A Convenção de direito penal[229] contra a corrupção abrange igualmente a corrupção no sector privado. Foi a mesma assinada por todos os Estados-Membros da UE, excepção feita à Espanha, e também pelos EUA, mas, até à data, apenas foi ratificada pela Dinamarca.

A Convenção de direito civil contra a corrupção[230] prevê regulamentação em matéria de responsabilidade civil e de ressarcimento por perdas e danos, designadamente a nulidade de contratos e cláusulas contratuais que obriguem ao pagamento de "luvas". Esta última Convenção foi assinada por todos os Estados-Membros da UE, excluindo os Países Baixos, Portugal e a Espanha. Os EUA não a assinaram.

Também no contexto da UE, foram adoptados dois diplomas jurídicos que têm por objecto a luta contra a corrupção: a Convenção relativa à prevenção e à luta contra a corrupção dos funcionários públicos e a acção comum sobre a corrupção no sector privado.

A Convenção contra a corrupção em que estejam implicados funcionários das Comunidades Europeias ou dos Estados-Membros da União Europeia[231] tem por objectivo assegurar, a nível da UE, a punibilidade da corrupção passiva e activa de funcionários públicos. Os Estados-Membros comprometem-se a sancionar a corrupção activa ou passiva de um funcionário público, quer se trate de um funcionário que seja cidadão nacional, quer de um funcionário de um outro Estado-Membro ou de um funcionário da UE.

A acção comum relativa à corrupção no sector privado[232] assegura que a corrupção passiva e activa de empresas é punida por lei. Neste contexto, as sanções penais aplicam-se, não só a pessoas singulares, mas também a pessoas colectivas. O âmbito de aplicação da acção comum é, todavia, menor do que o da Convenção relativa à luta contra a corrupção de funcionários públicos, porquanto apenas obriga os Estados-Membros a sancionarem factos que, pelo menos, em parte, tenham sido cometidos no seu território. O alargamento da aplicabilidade de sanções penais a actos cometidos, no estrangeiro, por cidadãos nacionais ou em benefício de pessoas

---

[227] OFFICE OF THE CHIEF COUNSEL FOR INTERNATIONAL COMMERCE, Legal Aspects of International Trade and Investment, http://www.ita.doc.gov/legal/

[228] http://www.oecd.org/daf/nocorruption/annex3.htm

[229] Criminal Law Convention on Corruption, http://conventions.coe.int/treaty/EN/WhatYouWant.asp?NT=173&CM=8&DF=21/06/01

[230] Civil Law Convention on Corruption ETS no.: 174, http://conventions.coe.int/treaty/EN/WhatYouWant.asp?NT=174&CM=8&DF=21/06/01

[231] Acto do Conselho de 25 de Junho de 1997, que estabelece, com base na alínea c), do artigo K, ponto 3 do Tratado da União Europeia, a Convenção contra a corrupção em que estejam implicados funcionários das Comunidades Europeias ou dos Estados-Membros da União Europeia. JO C 195 de 25.6.1997, p. 2.

[232] Acção comum de 22 de Dezembro de 1998 adoptada pelo Conselho com base no artigo K.3 do Tratado da União Europeia, relativa à corrupção no sector privado (98/742/JI), JO L 358 de 31.12.1998, p. 2

colectivas nacionais, é confiada ao livre arbítrio dos Estados-Membros. A Alemanha e a Áustria instituiram sanções penais para delitos de corrupção cometidos no estrangeiro desde que os mesmos sejam puníveis no local em que foram perpetrados.

10.9.4. O papel do "Advocacy Center" na promoção das exportações dos EUA

Mercê do decreto "Executive Order 12870“, o Presidente Clinton instituiu, em 1993, o denominado "Trade Promotion Coordinating Committee (TPCC)[233], que tem por missão coordenar o desenvolvimento da política de promoção comercial do Governo norte-americano, bem como definir uma estratégia para esse efeito. Nos termos do referido "Executive Order", o TPCC é igualmente integrado por um representante do "National Security Council“ (NSC)[234]. O NSC formula a política de segurança nacional dos Estados Unidos, quer no respeitante a questões de política interna e externa, bem como militar, quer no respeitante a questões que se prendem com os serviços de informações. As atribuições do NSC variam consoante as prioridades estipuladas pelo Presidente. Em 21 de Janeiro de 1993, o Presidente Clinton procedeu ao alargamento do NSC, que passou a incluir a PDD2, atribuindo simultaneamente uma maior importância a questões de ordem económica na formulação da política de segurança. O NSC é constituído, *inter alia,* pelo Presidente, pelo Vice-presidente, pelo Ministro dos Negócios Estrangeiros e pelo Ministro da Defesa. O Director da CIA é membro consultivo do referido órgão.

10.9.4.1. A missão do Advocacy Center

O "Advocacy Center", que funciona junto do Ministério do Comércio dos EUA, constitui a peça central da estratégia nacional de exportações posta em prática pelo Presidente Clinton e prosseguida pelo Presidente Bush. Constitui o mesmo a *interface* TPCC/economia americana. O Centro, fundado em 1993, tem ajudado, segundo as suas próprias declarações, centenas de empresas americanas a vencerem concursos públicos no estrangeiro.

O "Advocacy Center" presta assistência às empresas norte-americanas:
- organizando os recursos do Governo norte-americano – desde os vários peritos em matéria financeira, regulamentar, nacional e sectorial, passando pela rede mundial de funcionários comerciais, até à Casa Branca;
- pugnando por condições equitativas de concorrência e pela promoção da concorrência aberta no domínio dos concursos internacionais, desde os projectos de infraestruturas no valor de muitos milhares de milhões de dólares até ao contrato estratégico para uma pequena empresa;
- concluindo acordos, em nome de companhias norte-americanas, desde o arranque de projectos até à sua conclusão, mediante apoio activo;
- apoiando o emprego nos EUA e promovendo as exportações dos EUA através de êxitos alcançados por companhias norte-americanas que vencem concursos de adjudicação de projectos e contratos ultramarinos;
- apoiando empresas norte-americanas cujas negociações se encontram em fase de estagnação em virtude da inacção de um determinado governo estrangeiro ou de burocracia;

[233] Arquivos da Casa Branca, http://govinfo.library.unt.edu/npr/library/direct/orders/tradepromotion.html

[234] Homepage do National Security Council (NSC), http://www.whitehouse.gov/nsc

10.9.4.2. O modo de funcionamento do Centro[235]

Apenas o Director uma pequena equipa de 12 pessoas (dados relativos a 6.2.2001) trabalha no próprio Centro. Os domínios de actividade dos directores de projecto são os seguintes: a Rússia e os novos Estados independentes; a África, a Ásia Oriental e o Pacífico; o Próximo Oriente e o Norte de África; a Ásia Meridional, o Bangladesh, a Índia, o Paquistão e o Sri Lanka; a Europa e a Turquia; a China, Hong-Kong e Taiwan; o Canadá, as Caraíbas e a América Latina; a nível mundial - aeronáutica, indústria automóvel e de defesa, bem como telecomunicações, tecnologia da informação e indústria informática.

O Centro funciona, em relação às empresas, como pólo central no que diz respeito às diversas entidades da Administração dos EUA responsáveis pela promoção das exportações. Desenvolve a sua actividade sem discriminar empresas, mas limita-se a apoiar, de acordo com regras claras, projectos de interesse nacional para os EUA. Assim, pelo menos 50% do valor dos produtos fornecidos deverá ser proveniente dos EUA.

10.9.4.3. Participação da CIA nas actividades do TPCC

Duncan Campbell apresentou aos Membros da comissão alguns documentos que deixaram de ser confidenciais, documentos esses que demonstram uma participação da CIA nas actividades do "Advocacy Centers". Contêm os mesmos actas do "Trade Promotion Co-ordinating Committee" relativas a uma reunião do grupo de trabalho "Indonésia", de Julho e Agosto de 1994[236]. Nesse grupo, que tem por missão definir uma estratégia comercial para a Indonésia, participam, de acordo com os documentos em questão, vários colaboradores da CIA, cujo nome é referido nas actas em causa.

Por outro lado, as actas permitem concluir que um dos colaboradores da CIA define, como objectivo do grupo, a identificação dos principais concorrentes, a qual servirá de informação de base[237].

10.9.4.4. Questões em aberto relacionadas com o Centro

O Governo americano não autorizou o encontro previsto e confirmado pelo Centro entre membros da comissão e o Centro. Por tal motivo, não puderam ser debatidas duas questões que suscitam dúvidas, o que o relator o lamenta:

a) A comissão dispõe de documentos (*vide* capítulo 10, 10.9.4.3) que comprovam uma participação da CIA nas actividades do TPCC;

b) O "Advocacy Center" refere, no âmbito do folheto informativo da sua autoria (atrás citado), que reúne os recursos de 19 "agências governamentais dos EUA". Todavia, noutra parte do folheto apenas são referidas nominalmente 18 agências. Coloca-se a questão de saber por que motivo não é referido publicamente o nome da décima nona agência.

---

[235] Homepage des Advocacy Centers, http://www.ita.doc.gov/td/advocacy/

[236] TPCC Working Group Meeting, Agenda, 18.7.1994, TPCC Indonesia Advocacy-Finance Working Group, Distribution List, Acta da reunião de 17.8.1994, em carta do "U.S. & Foreign Commercial Service" de 25.8.1994

[237] ibidem: "Bob Beamer suggested that any primary competitors known to the group for these projects should be included as background information", Bob Beamer … dos representantes da CIA

O relator considera que a anulação do encontro que havia sido agendado com o "Advocacy Center" se deve ao facto de aí terem lugar actividades sobre as quais o Governo americano não pretende pronunciar-se.

10.10. A segurança das redes informáticas

10.10.1. A importância do presente capítulo

Tal como já exposto no capítulo 10, 10.10.4, a violação de redes informáticas ou o furto de dados contidos em computadores portáteis ("laptops") representa actualmente o segundo melhor método de espionagem económica, a par da intervenção de espiões. As explanações constantes do presente capítulo não se encontram directamente correlacionadas com um sistema de intercepção de comunicações internacionais organizado a nível mundial. Todavia, na perspectiva dos objectivos que se propõe esta comissão, não é possível prescindir, no contexto do capítulo sobre a espionagem económica, de uma breve explanação de um dos seus instrumentos mais poderosos. Tal reveste-se certamente de utilidade para fins de definição da importância de um sistema de intercepção de comunicações internacionais no contexto da espionagem económica.

10.10.2. O risco da utilização das modernas tecnologias da informação na economia

O moderno processamento de dados por via electrónica impôs-se há muito no sector económico. Os dados são, na sua totalidade, compactamente armazenados em suportes de memória. Os dados memorizados em computador tornaram-se, entretanto, num dos principais factores do "know-how" empresarial. Esta mutação da sociedade industrial para a sociedade da informação permite o acesso a novas oportunidades, mas comporta igualmente riscos consideráveis no respeitante à segurança[238].

10.10.2.1. O risco em progressão

O risco crescente a que se assiste pode descrever-se sucintamente do seguinte modo[239]:
É cada vez maior o número de empresas em rede, sendo crescente o número de informações susceptíveis de ser pura e simplesmente copiadas em caso de violação da rede. Simultaneamente, são descentralizadas outras partes sensíveis das informações, sendo, por conseguinte, pouco propícias a uma gestão central em matéria de segurança. A mobilidade dos titulares de cargos decisórios, que transportam consigo - nos seus computadores portáteis - informações sensíveis, gera riscos suplementares. A externalização de serviços conduz à transferência de actividades de manutenção também no sector das tecnologias da informação, transferência essa que, numa perspectiva de segurança, deveria preferencialmente processar-se de outro modo. A importância da segurança das empresas no quadro da hierarquia empresarial induz, em conjugação com a falta de conhecimentos dos órgãos decisórios em matéria de segurança, a tomada de decisões incorrectas.

10.10.2.2. Alguns dos riscos específicos

Compressão da informação em suportes de dados compactos

Os dados confidenciais das empresas figuram, hoje em dia, num espaço físico diminuto, em suportes de dados comprimidos, o que permite, por exemplo, subtrair a uma empresa a totalidade de planos para um novo projecto num disco rígido amovível com as dimensões de um maço de

[238] Computerspionage, Dokumentation Nr. 44, Bundesministerium für Wirtschaft, Juli 1998

[239] *Roman Hummelt,* Wirtschaftsspionage auf dem Datenhighway, Hanser Verlag, München 1997

cigarros ou apagá-los electronicamente mediante o acesso ilegítimo a uma rede informática sem deixar quaisquer vestígios e num curto espaço de tempo.

Descentralização de informações confidenciais

Na época dos "mainframes" (sistemas centrais interactivos), o controlo do acesso a informações confidenciais era de fácil organização, uma vez que apenas existia uma unidade a gerir. Hoje em dia, são colocadas na rede à disposição do utilizador, no seu local de trabalho, consideráveis capacidades informáticas. Tal constitui obviamente uma vantagem notória para o utilizador, representando, porém, uma catástrofe em termos de segurança.

Simplificação da reproductibilidade de informações

Na época dos projectos desenhados à mão e das máquinas de escrever mecânicas era extremamente difícil reproduzir documentos sem incorrer no risco de que tal viesse a ser descoberto. Hoje em dia, na era electrónica, tal é fácil. As informações digitalizadas podem ser reproduzidas em grande número, de modo simples, com rapidez e sem deixar quaisquer vestígios. Assim, a obtenção do material desejado pode, frequentemente, processar-se mediante uma única intervenção, o que reduz consideravelmente o risco de detecção.

Mobilidade de titulares de cargos decisórios

Os responsáveis superiores das empresas transportam, nos seus "laptops", sem que de tal se encontrem suficientemente cientes, informações sobre a empresa dotadas de importância estratégica. A possibilidade de proceder rapidamente a uma cópia do disco rígido aquando de um "controlo aduaneiro" ou por ocasião de uma busca no respectivo quarto de hotel propicia aos serviços de informações possibilidades consideráveis. Pode igualmente acontecer que a agenda seja pura e simplesmente objecto de furto. Em virtude da descentralização, os conteúdos dos discos rígidos dos "laptops" dos responsáveis de uma empresa só dificilmente podem ser abrangidos por um sistema central de segurança.

Transferência da manutenção para prestadores de serviços externos

A filosofia da externalização ("outsourcing") pode induzir, em termos de gestão empresarial, uma diminuição de custos. No domínios das tecnologias da informação e da manutenção de instalações telefónicas, tal permite a técnicos externos à empresa o acesso a quase todas as informações. Os riscos associados a esse facto não podem ser suficientemente assinalados.

Insuficiências na gestão das redes

A par de lacunas na segurança do próprio "software", as quais são reiteradamente detectadas pelos piratas informáticos, o maior perigo procede dos administradores das redes que não têm a devida consciência dos riscos existentes. Na sua versão de base, o Windows NT encontra-se configurado de tal modo que revela praticamente todas as informações sobre a rede necessárias ao sucesso de um "ataque" à mesma[240]. Mantendo-se essa configuração e não sendo alteradas as "standard passwords", o acesso não autorizado à rede torna-se fácil. Um erro consiste no facto de serem notórias as diligências em prol da segurança do "firewall", sendo, porém, fraca a protecção da rede contra a sabotagem interna[241].

[240] *George Kurtz, Stuart McClure, Joel Scambray,* Hacking exposed, Osborne/McGraw-Hill (2000), 94

[241] *Martin Kuppinger*, Internet- und Intranetsicherheit, Microsoft Press Deutschland (1998), 60

10.10.3. Frequência dos ataques contra as redes

O número de violações das redes informáticas na Internet regista um aumento anual [242]. À "Computer Emergency Response Team" (CERT), uma organização fundada em 1988 nos EUA com o objectivo de garantir a segurança na Internet, foram notificados, em 1989, 132 incidentes de segurança. Em 1994, elevavam-se já a 2241 e, em 1996, ascenderam a 2573, sendo muito elevado o número de casos não noticiados. Esta tese é corroborada por uma simulação em larga escala levada a efeito pelo Ministério Norte-Americano da Defesa nos seus próprios computadores. Aquando dessa operação, tentou-se sistematicamente a infiltração a partir do exterior em 8932 servidores e "mainframes". Os resultados do teste foram positivos em 7860 sistemas; apenas em 390 casos foi detectado o acto de violação e apenas 19 casos foram notificados. Procede-se a uma distinção entre "ataques" e incidentes de segurança. Um "ataque" constitui uma tentativa isolada de aceder de modo ilegítimo a um sistema. O incidente de segurança consiste num conjunto de "ataques" conjuntos. Estudos de longo prazo efectuados pelo Pentágono e por universidades americanas, cujos resultados foram estimados tendo em conta toda a Internet, permitem presumir a existência de 20000 incidentes de segurança e de 2 milhões de "ataques" na Internet por ano.

10.10.4. Agentes e métodos

Os serviços de informações estrangeiros que atacam os sistemas da tecnologia de informações visam obter, tão imperceptivelmente quanto possível, as informações nos mesmos contidas. Em princípio, é possível distinguir entre três grupos de agentes, que actuam segundo três *modi operandi* diferentes.

Agentes internos com direito de acesso geral

Um espião infiltrado ou contratado que consiga ocupar o cargo de gestor de sistemas ou de administrador de segurança num centro de dados informáticos apenas necessita, para a sua actividade de espionagem, de exercer, de modo extensivo, as competências que oficialmente lhe são cometidas para se apropriar da quase totalidade do "know-how" do seu empregador. O mesmo se aplica a um engenheiro que exerça um cargo de chefia e a quem assista o direito de acesso ilimitado a todas as bases de dados tecnológicas da empresa.

A eficácia de um tal espião é máxima. Todavia, caso surjam suspeitas, encontra-se o mesmo exposto a um elevado risco de ser descoberto, uma vez que as investigações se concentram de imediato no pequeno círculo de pessoas que têm autorização de acesso geral às informações. Por outro lado, o facto de um espião usufruir da autorização de acesso geral não é previsível nem influenciável, sendo uma mera questão de sorte.

Agentes internos com direito de acesso localizado

Um espião operante no interior de uma empresa usufrui de vantagens claras relativamente a um pirata informático cuja acção de ataque se processe a partir do exterior: tem apenas de superar a segurança da rede, não sendo, adicionalmente, confrontado com um "firewall". A partir de um determinado posto de trabalho é possível espionar a arquitectura da rede, desde que se disponha de conhecimentos adequados, sendo possível obter importantes informações mediante o recurso a técnicas igualmente utilizadas no quadro da pirataria informática praticada a partir do exterior, bem como mercê de outras técnicas susceptíveis de utilização a nível interno[243]. Acresce que o

[242] *Othmar Kyas,* Sicherheit im Internet, International Thomson Publishing (1998), 23

[243] *Anonymus*, Hacker's guide, Markt &Technik-Verlag (1999)

espião pode comunicar, de modo insuspeito, com outros membros da empresa, sendo a designada "social engineering" propícia à obtenção de "passwords".

A eficácia de um espião deste tipo pode ser elevada, não sendo, porém, tão previsível como a do referido no primeiro caso. O risco de descoberta é menor, designadamente em redes cujo administrador vote uma menor atenção aos riscos de um "ataque" interno. A infiltração de um espião com formação técnica específica para aceder ilicitamente a redes informáticas revela-se muito mais simples (estagiários, investigadores convidados, etc.).

10.10.5. Prática da pirataria informática a partir do exterior

A infiltração de piratas informáticos nas redes a partir do exterior constitui um facto conhecido e bem documentado. Entretanto, também os serviços de informações formam especialistas para esse efeito. A eficácia de uma tal operação não é previsível, dependendo, em larga medida, da qualidade de organização dos mecanismos de defesa e do facto de a rede do departamento de investigação se encontrar ou não fisicamente ligada à Internet. O risco em que incorre o espião profissional é nulo, mesmo que o "ataque", enquanto tal, seja descoberto, porquanto não tem de se encontrar presente *in situ*.

10.11. A subavaliação dos riscos

10.11.1. A consciência dos riscos no sector económico

A consciência do risco que representa a espionagem económica não se tem revelado, até à data, muito acentuada neste sector. Tal, traduz-se, nomeadamente no facto de os responsáveis pela segurança integrarem, frequentemente, os quadros médios da gestão, não sendo membros da direcção da empresa. Porém, a segurança custa dinheiro, e a verdade é que, regra geral, os membros da direcção apenas se debruçam sobre as questões de segurança quando é demasiado tarde.

As grandes empresas dispõem, no entanto, dos seus próprios departamentos de segurança, ocupando pessoal com formação específica também no domínio das tecnologias da informação. As pequenas e médias empresas, em contrapartida, só muito raramente dispõem de especialistas de segurança, contentando-se normalmente com um equipamento informático que funcione eficazmente. Acontece que também estas empresas podem constituir alvo da espionagem económica, porquanto são, em parte, altamente inovadoras. Além disso, as pequenas e médias empresas subcontratadas constituem, em virtude da sua integração em todo o processo de produção, bases de operações adequadas a "ataques" contra grandes empresas.

10.11.2. A consciência dos riscos no sector da investigação

Os investigadores interessam-se, regra geral, apenas pelo seu domínio de especialidade. Assim sendo, são, por vezes, facilmente vítimas dos serviços de informações. O relator constatou com alguma surpresa que também entre os institutos de investigação aplicada a comunicação se processa, de modo não criptado, via correio electrónico e rede científica. Tal é pura loucura.

10.11.3. A consciência dos risco nas Instituições Europeias

10.11.3.1. Banco Central Europeu

As informações sobre a preparação de decisões do Banco Central Europeu poderiam revestir-se de grande importância para os serviços de informações. Que, além disso, também os mercados teriam grande interesse nessas informações, afigura-se óbvio. No quadro de uma reunião à porta fechada, a comissão ouviu, representantes do Banco Central Europeu sobre os dispositivos de segurança por aquele adoptados visando a protecção das informações. Foi dado ao relator concluir que existe no Banco Central Europeu a consciência do risco e que se vela pela segurança, no quadro das possibilidades existentes. Não obstante, dispõe o mesmo de informações[244] segundo as quais a consciência de risco em alguns bancos centrais nacionais não é particularmente acentuada.

10.11.3.2. Conselho da União Europeia

Antes da nomeação do Alto Representante para a Política Externa e de Segurança, o Conselho havia concentrado, fundamentalmente, os seus esforços em matéria de confidencialidade nas diligências tendentes a ocultar ao público e ao Parlamento Europeu os trâmites do processo decisório e a atitude dos Governos dos Estados-Membros. Jamais teria o mesmo resistido a uma operação de espionagem de envergadura profissional[245]. Assim, o controlo das instalações técnicas das cabines de interpretação é alegadamente confiado a uma firma israelita. O Conselho adoptou agora medidas de segurança[246] que correspondem às normas-padrão em vigor na NATO.

10.11.3.3. O Parlamento Europeu

Até à data, o Parlamento Europeu jamais trabalhou com documentos classificados, razão pela qual, em matéria de protecção do segredo, não tem experiência nem uma cultura de segurança. A necessidade apenas se fará sentir quando o Parlamento tiver acesso a documentos secretos. Caso contrário, não é próprio de uma assembleia democrática, a quem cumpre a máxima transparência possível, a prática de uma política geral de secretismo. Não obstante, deveria ser possível encriptar, pelo menos a bem da protecção de informadores e peticionários, o correio electrónico entre os vários gabinetes dos deputados, em caso de necessidade. Até à data, tal não é possível.

[244] Comunicação particular, fonte protegida

[245] Comunicação de Membros do COREPER e de funcionários do Conselho; fontes protegidas

[246] Decisão do Conselho, de 19 de Março de 2001, que aprova as regras de segurança do Conselho, JO L 101 de 11.4.2001, p. 1 e seguintes

10.11.3.4. Comissão Europeia

Na Comissão Europeia existem Direcções-Gerais, nas quais, em virtude da natureza das informações aí tratadas, não existe qualquer necessidade de confidencialidade ou de protecção. Pelo contrário, em todos os domínios correlacionados com a legislação deveria imperar absoluta transparência. O Parlamento Europeu deverá zelar por que nesses domínios não seja, desnecessariamente, ainda mais dissimulado, mercê de normas de confidencialidade despropositadas, o exercício de influência nas propostas legislativas por parte das empresas interessadas do que já é hoje.

Existem, todavia, também sectores na Comissão em que são manuseadas informações sensíveis. A par de EURATOM, trata-se sobretudo dos domínios das relações externas, do comércio externo e da concorrência. Com base nas informações que a comissão obteve das Direcções-Gerais visadas, no quadro de uma reunião à porta fechada, e sobretudo com base nas demais informações em posse do relator, subsistem sérias dúvidas quanto à existência de uma consciência de risco no respeitante à espionagem e a uma articulação profissional com as questões de segurança no seio da Comissão Europeia. É obviamente impróprio expor as lacunas de segurança no quadro de um relatório de acesso público. O relator reputa, todavia, imperativo que o Parlamento Europeu se debruce, a breve trecho, sobre esta questão de um modo adequado.

É possível, já hoje, constatar que os sistemas de encriptação mercê dos quais a Comissão comunica com parte dos seus gabinetes externos são obsoletos. Tal não significa que o nível de segurança seja mau. Os aparelhos actualmente utilizados já não são, contudo, produzidos e apenas cerca de metade dos gabinetes externos dispõe de possibilidades de encriptação. A introdução de um novo sistema que opere com base em correio electrónico encriptado afigura-se imperativa.

11. Auto protecção através da criptografia

11.1. Objectivo e funcionamento da encriptação

11.1.1. Objectivo da encriptação

Sempre que se transmite uma mensagem corremos o risco de esta cair nas mãos de alguém não autorizado. Neste caso, para impedir que elementos exteriores tomem conhecimento do seu conteúdo, é imperativo tornar a mensagem ilegível ou inaudível, isto é, encriptada. Por isso, nos domínios militar e diplomático desde sempre foram utilizadas técnicas de encriptação[247].

Nos últimos 20 anos a importância da encriptação aumentou, dado que é cada vez maior a proporção de comunicações transmitidas para o estrangeiro e, neste contexto, o próprio Estado já não pode proteger a confidencialidade da correspondência e das comunicações à distância. Além disso, a ampliação das capacidades técnicas do próprio Estado para escutar/registar legalmente as comunicações provocou uma maior necessidade de protecção por parte de cidadãos preocupados. Finalmente, o interesse crescente dos criminosos pelo acesso ilegal à informação e pela sua falsificação desencadeou a adopção de medidas de protecção (por exemplo, no sector bancário).

Com a invenção das comunicações eléctricas e electrónicas (telégrafo, telefone, rádio, teleimpressora, fax e Internet), a transmissão de mensagens foi fortemente simplificada e tornou-se incomparavelmente mais rápida. Isto tem a desvantagem de não existir qualquer protecção **técnica** contra a escuta/registo e qualquer pessoa com um aparelho adequado pode interceptar as comunicações se tiver acesso ao meio de transmissão dessas comunicações. Se for efectuada em condições profissionais, a escuta deixa poucos ou nenhuns rastos. Desta forma, a encriptação ganhou uma nova importância. Foi o sector bancário que – com o advento das transferências electrónicas de dinheiro – primeiro começou a proteger regularmente as comunicações relativas a essas transferências por meio da encriptação. Com a crescente internacionalização da economia, esse sector também começou - pelo menos parcialmente - a usar a criptografia para proteger as comunicações. Com a ampla introdução das comunicações via Internet, que são totalmente desprotegidas, cresceu também a necessidade dos particulares de protegerem as suas comunicações contra escutas.

No contexto deste relatório também se coloca a questão de saber se existem métodos de encriptação das comunicações baratos, juridicamente autorizados, suficientemente seguros e de utilização simples que permitam a auto-protecção contra escutas.

11.1.2. Funcionamento da encriptação

O princípio da encriptação consiste em transformar um texto original num texto secreto de tal forma que este não faça nenhum sentido ou tenha um sentido diferente. Porém, o destinatário poderá retransformá-lo no original. Através da encriptação, uma sequência lógica de letras é transformada, por exemplo, numa sequência sem sentido que ninguém do exterior compreenderá.

[247] Há provas de que isto já era feito na Antiguidade, por exemplo, com a utilização dos *Scytale* (cilindros) pelos espartanos no século V.

Isto é feito segundo um determinado método (algoritmo de encriptação) que assenta na troca de letras (transposição) e/ou na substituição de letras (substituição). **O método de encriptação** (algoritmo) actualmente não é mantido em segredo. Pelo contrário: recentemente houve um concurso público a nível mundial para a criação de uma nova norma global de encriptação para utilização na economia. O mesmo se aplica à realização de um determinado algoritmo de encriptação que funcionará como *hardware* em aparelhos (por exemplo, num criptofax).

O **verdadeiro segredo** é a chamada **chave.** A melhor forma de descrever este processo é recorrer a um exemplo de um domínio correlacionado. O funcionamento dos trincos das portas é normalmente do conhecimento público, tanto mais que é objecto de uma patente. A protecção individual de uma porta resulta do facto de poderem existir muitas chaves diferentes para um determinado tipo de trinco. É exactamente assim que funciona a encriptação de informações: com um **método de encriptação do conhecimento público** (algoritmo) é possível manter a confidencialidade de **muitas** mensagens, graças a chaves individuais diferentes que os detentores mantêm em segredo.

Para esclarecer os conceitos anteriormente utilizados, apresentamos como exemplo a chamada "encriptação de César". O chefe militar romano César encriptava as suas mensagens segundo um método simples, no qual cada letra era substituída pela terceira letra seguinte do alfabeto – isto é o A pelo D, o B pelo E, etc. Assim, a palavra **ECHELON** transformava-se na palavra **HFKHORQ.** Neste caso, o **algoritmo de encriptação** consiste na **troca de letras** dentro do alfabeto e a **chave** concreta é a indicação de trocar cada letra pela **terceira letra seguinte do alfabeto!** Tanto a encriptação como a desencriptação ocorrem da mesma forma: através da deslocação de 3 letras. Trata-se, por isso, de um processo simétrico. Actualmente um processo deste tipo não protege nada nem sequer por um segundo!

Numa boa encriptação, o método pode ser completamente do conhecimento público e, apesar disso, a encriptação ser considerada como segura. Para tal, é necessário que a variedade de chaves seja tão grande que não seja possível, num tempo adequado, provar todas as chaves possíveis (o chamado **ataque à força bruta**), mesmo com a utilização de computadores. Por outro lado, a variedade de chaves, por si só, não garante a segurança criptológica se o método de encriptação contiver um texto secreto que inclua pontos de referência para uma descodificação (por exemplo, a acumulação de determinadas letras)[248]. Nestes aspectos, a encriptação de César não é uma forma de encriptação segura. Através da simples substituição é possível – devido à diferente frequência das letras numa língua – decifrar rapidamente o processo, tanto mais que há apenas 25 possibilidades de troca, logo 25 chaves, porque o alfabeto só tem 26 letras. Assim, o adversário pode, simplesmente por tentativas, obter rapidamente a chave adequada e decifrar o texto.

Seguidamente tentaremos esclarecer como deve ser um sistema seguro.

11.2. A segurança dos sistemas de encriptação

11.2.1. Aspectos gerais do conceito de segurança da encriptação

Quando se exige a um sistema de encriptação que seja "seguro", pode-se aludir com isto a dois processos diferentes. Por um lado, pode-se exigir que o sistema seja absolutamente seguro, que a

[248] *Otto Leiberich*, „Vom diplomatischen Code zur Falltürfunktion - Hundert Jahre Kryptographie in Deutschland", Spektrum der Wissenschaft, Junho de 1999, pp. 26 e seguintes.

descodificação da mensagem seja impossível sem ter conhecimento da chave e que esta impossibilidade seja comprovável em termos matemáticos. Por outro lado, também nos podemos contentar que o código - segundo o estado actual da técnica - seja inquebrável e que, desta forma, a segurança seja garantida por um prazo que ultrapasse largamente o prazo "crítico" no qual uma mensagem pode ser mantida confidencial.

11.2.2.Segurança absoluta: o *one-time pad*

Até agora, o único processo absolutamente seguro é o *one-time pad* (sistema "one-time"). Este sistema foi desenvolvido em finais da Primeira Guerra Mundial[249], mas posteriormente também foi utilizado na teleimpressora de crise entre Moscovo e Washington. O conceito baseia-se numa chave que consiste numa sequência de letras completamente aleatória, sequência que nunca se repete. O emissor e o receptor encriptam a mensagem com base nesta sequência de letras e destroem a chave imediatamente após a sua primeira utilização. Como a chave não possui qualquer ordem interior, é impossível para um criptoanalista quebrar o código. Isto pode mesmo ser provado matematicamente[250].

A desvantagem deste processo consiste em que não é fácil gerar grandes quantidades de chaves aleatórias deste tipo[251] e a distribuição segura da chave é difícil e nada prática. Por isso, este método não é utilizado no tráfego comercial geral.

11.2.3. Segurança relativa segundo o estado actual da técnica

11.2.3.1. Utilização de máquinas para a encriptação e desencriptação

Ainda antes da invenção do *one-time pad* já tinham sido desenvolvidos processos criptográficos que disponibilizavam uma grande quantidade de chaves e geravam textos cifrados contendo a menor quantidade possível de regularidades no texto - que, por isso, quase não forneciam pontos de referência para uma criptanálise. Para que estes métodos pudessem ter uma aplicação prática suficientemente rápida, foram criadas máquinas de encriptação e desencriptação. A mais espectacular deste tipo foi certamente a ENIGMA[252], que foi utilizada pela Alemanha na Segunda Guerra Mundial. O exército de peritos em desencriptação sediado em Bletchley Park (Inglaterra) conseguiu quebrar a encriptação da ENIGMA graças a máquinas especiais, as chamadas "bombas". Tanto a ENIGMA como as "bombas" eram aparelhos mecânicos.

11.2.3.2. Utilização do computador na criptologia

A invenção do computador foi revolucionária para a ciência da criptologia porque a sua capacidade de desempenho permitiu a utilização de sistemas cada vez mais complexos. Apesar de o computador em nada ter alterado os princípios básicos da encriptação, mesmo assim aconteceram algumas inovações. Em primeiro lugar, o grau da complexidade possível dos

---

[249] Foi criado pelo major *Joseph Mauborgne*, director da Secção de Investigação Criptográfica do exército americano. *Simon Singh*, Geheime Botschaften, Carl Hanser Verlag (1999), p. 151.

[250] *Simon Singh*, Geheime Botschaften, Carl Hanser Verlag (1999), pp. 151 e seguintes.

[251] *Reinhardt Wobst,* Abenteuer Kryptologie[2], Adison-Wesley (1998), p. 60.

[252] A Enigma foi inventada por Arthur Scherbius e patenteada em 1928. De certa forma ela assemelhava-se a uma máquina de escrever, pois possuia um teclado no qual era introduzido o texto original. Graças a um quadro de interruptores e cilindros rotativos, o texto era encriptado segundo determinadas instruções e posteriormente desencriptado com a mesma máquina e com a ajuda de livros de código.

sistemas de encriptação multiplicou-se por N, já que deixou de existir a limitação do que era mecanicamente exequível; em segundo lugar, a velocidade do processo de encriptação aumentou drasticamente.

A informação é processada pelos computadores de forma digital, por meio de números binários. Isto significa que a informação é expressa numa sequência de dois sinais, nomeadamente 0 e 1. O 1 corresponde, no sentido físico, a uma tensão eléctrica ou a uma magnetização ("ligado"), o 0 à interrupção da tensão ou da magnetização ("desligado"). Neste contexto, acabou por se impor a normalização segundo o sistema ASCII[253], no qual cada letra é representada por uma combinação de sete algarismos 0 e 1[254]. Assim, um texto assume o aspecto de uma sequência de 0 e 1, isto é, em vez de letras são encriptados números.

Neste contexto, podem ser utilizadas tanto as formas de transposição (troca) como as de permuta (substituição). A substituição pode ocorrer, por exemplo, através da adição de uma chave sob a forma de uma qualquer sequência de números. Segundo as regras da matemática binária, a soma de números iguais é 0 (logo 0+0 = 0 e 1+1=0) e a soma de dois números diferentes é 1 (0+1=1). A nova sequência de números encriptada gerada por adição é, por isso, uma sequência binária que pode ser reprocessada digitalmente ou tornada novamente legível retirando a chave acrescentada.

Com o recurso aos computadores é possível – com a utilização de fortes algoritmos de encriptação – gerar textos cifrados que praticamente não oferecem nenhum ponto de referência para uma criptanálise. Nesse caso, uma tentativa de desencriptação só pode ser efectuada experimentando várias chaves possíveis. Quanto maior for a chave, tanto maiores as hipóteses de este processo fracassar - mesmo com a utilização de computadores de elevado desempenho - devido ao tempo para tal necessário. Assim, existem processos de encriptação praticáveis que, segundo o estado actual da técnica, podem ser considerados seguros.

11.2.4. Normalização e limitação premeditada da segurança

Devido à propagação dos computadores nos anos 70, a normalização dos sistemas de encriptação tornou-se cada vez mais urgente, pois só assim as empresas poderiam comunicar de forma segura com os seus parceiros comerciais sem terem de recorrer a um equipamento desproporcionado. Os primeiros esforços neste sentido foram efectuados nos EUA.

Uma encriptação forte também pode ser utilizada para fins ilícitos ou por potenciais adversários militares. Também pode dificultar, ou mesmo impossibilitar, a espionagem electrónica. Por isso, a NSA insistiu na escolha de uma norma de encriptação suficientemente segura para o sector económico mas que permitisse a desencriptação pela própria NSA, devido ao seu equipamento técnico específico. Por esse motivo, a dimensão da chave foi limitada a 56 bits. Isto reduz o número de chaves possíveis a 100 000 000 000 000 000[255]. De facto, em 23 de Novembro de 1976 a chamada *cifra de Lucifer* de Horst Feistel, na sua **versão de 56 bits,** foi adoptada oficialmente sob a designação de *Data Encryption Standard* (DES) e durante um quarto de

[253] American Standard Code for Information Interchange.

[254] A = 1000001, B= 1000010, C= 1000011, D= 1000100, E = 1000101, etc.

[255] Este número, representado em termos binários, consiste em 56 algarismos 0 e 1. *Vide* a este propósito Singh, Geheime Botschaften, Carl Hanser Verlag (1999), p. 303.

século constituiu a norma de encriptação oficial norte-americana[256]. Esta norma também foi adoptada na Europa e no Japão, especialmente no sector bancário. O algoritmo da DES – ao contrário do que afirmaram diversos meios de comunicação – ainda não foi quebrado até agora; porém, entretanto já foi criado equipamento suficientemente forte para experimentar várias chaves ("ataque à força bruta"). Pelo contrário, a *Triple-DES* - que é uma chave de 112 bits - continua a ser considerada como segura. O sucessor da DES, a AES (*Advanced Encryption Standard*), é um processo europeu[257] que foi desenvolvido sob a designação *Rijndael* em Lovaina (Bélgica). **É uma norma rápida e considerada segura porque não tem nenhuma limitação da dimensão da chave.** Tal deve-se à alteração da política de criptografia norte-americana.

A normalização significa, para as empresas, uma simplificação considerável da encriptação. Porém, mantém-se o problema da distribuição das chaves.

11.3. O problema da distribuição/transmissão segura das chaves

11.3.1.A encriptação assimétrica: o processo da chave-pública

Enquanto um sistema trabalhar com uma chave que serve tanto para encriptar como para desencriptar (encriptação simétrica) será muito difícil utilizar essa chave com **muitos** parceiros de comunicação. Na verdade, a chave deve ser transmitida **antecipadamente** a cada parceiro de comunicação novo de forma a que elementos terceiros não tomem conhecimento da mesma. Para o sector económico, isto é dificilmente praticável; para os particulares, só é possível em casos específicos.

A encriptação assimétrica oferece uma solução para este problema: não é utilizada a mesma chave para a encriptação e a desencriptação. A mensagem é encriptada com uma chave que pode ser do conhecimento de todos, a chamada **chave pública.** Porém, o processo funciona como uma rua de sentido único, numa só direcção, e já não é possível retransformar o texto cifrado no texto original apenas com a chave pública. Por isso, quem quiser receber uma mensagem encriptada pode enviar a sua chave pública ao seu parceiro de comunicação, também por um meio não seguro, para a encriptação da mensagem. Para desencriptar a mensagem então recebida será utilizada uma outra chave, a **chave privada**, que é mantida em segredo e nunca é enviada[258]. Para compreender este processo, a comparação mais esclarecedora é a de um cadeado: qualquer pessoa pode fechar um cadeado destes e assim trancar de forma segura um baú; porém, só quem tiver a chave certa poderá voltar a abri-lo[259]. A chave pública e a chave privada estão correlacionadas mas não é possível decifrar a chave privada a partir da chave pública.

Ron Rivest, Adi Shamir e Leonard Adleman inventaram um sistema de encriptação assimétrico que foi designado por processo RSA, a partir dos seus nomes. Numa função unidireccional (a chamada função-alçapão) é utilizado como componente da chave pública o resultado da multiplicação de dois números primos muito grandes. O texto original é encriptado assim. A desencriptação só pode ser feita por quem conhecer o valor dos dois números primos utilizados. Porém, não existe nenhum processo matemático que permita inverter a multiplicação de dois

[256] *Simon Singh*, Geheime Botschaften, Carl Hanser Verlag (1999), pp. 302 e seguintes.

[257] Foi criado por dois criptógrafos belgas na Universidade Católica de Lovaina, *Joan Daemen* e *Vincent Rijmen*.

[258] A ideia da encriptação assimétrica sob a forma de processo de chave pública é da autoria de *Whitfield Diffie* e *Martin Hellmann*.

[259] *Simon Singh*, Geheime Botschaften, Carl Hanser Verlag (1999), p. 327.

números primos, de forma a calcular os números primos iniciais a partir do resultado da multiplicação. Até agora, isto só é possível através de tentativas sistemáticas. Por isso, segundo o estado actual da técnica, este processo é considerado seguro desde que sejam escolhidos números primos suficientemente altos. O único risco consiste em que um dia um matemático brilhante descubra um modo rápido de decomposição dos factores. Porém, até agora – e apesar de grandes esforços – ninguém conseguiu tal coisa[260]. Aliás, foi reiteradamente afirmado que o problema é insolúvel mas até agora ninguém deu provas exactas de tal facto[261].

Não obstante, a encriptação por chave pública – em comparação com o processo simétrico (por exemplo, DES) – exige do computador uma capacidade de processamento muito maior ou a utilização de processadores rápidos e de grande capacidade.

11.3.2. A encriptação por chave pública para os particulares

Para generalizar o acesso à encriptação por chave pública, Phil Zimmerman teve a ideia de associar o processo de chave pública – que exige bastante do computador – a um processo simétrico mais rápido. A mensagem em si deveria ser encriptada por um processo simétrico – o processo IDEA, desenvolvido em Zurique – mas a chave de encriptação simétrica, pelo contrário, seria transmitida simultaneamente após o processo de chave pública. Zimmermann criou um programa muito fácil de utilizar - chamado *Pretty Good Privacy* – que, ao carregar numa tecla (ou clicando com o rato), cria a chave necessária e efectua a encriptação. O programa foi colocado na Internet onde qualquer um o pode descarregar. O PGP acabou por ser comprado pela firma norte-americana NAI mas continua a ser disponibilizado gratuitamente aos particulares[262]. No caso das versões anteriores, o código-fonte foi publicado, pelo que se pode partir do princípio que não foi incluído no programa qualquer função-alçapão. Infelizmente, o código-fonte da versão mais recente - PGP 7, que se distingue por um *interface* gráfico manifestamente fácil de utilizar – já não foi publicado.
Não obstante, existe ainda uma outra aplicação prática da norma *Open PGP*: o *GnuPG*. Este programa oferece os mesmos métodos de encriptação do PGP e também é compatível com este último. Neste caso trata-se de um programa gratuito, o seu código-fonte é conhecido e qualquer um pode utilizá-lo e transmiti-lo. O Ministério da Economia e Tecnologia da R.F.A. promoveu a portabilidade do *GnuPG* para Windows e o desenvolvimento de um *interface* gráfico mas, infelizmente, este trabalho ainda não foi completamente amadurecido. Não obstante, segundo as informações de que dispõe o relator, este trabalho prossegue.

Além disso, existem ainda outras normas concorrentes do *OpenPGP*, como a norma S/MIME, que é apoiada por muitos programas de e-mail. Porém, neste caso, o relator não dispõe de quaisquer informações sobre as possibilidades de aplicação gratuita.

11.3.3. Processos futuros

Aspectos completamente novos relativamente à transmissão segura de chaves poderão resultar futuramente da criptografia quântica. Esta assegura que um acto de escuta durante a transmissão de uma chave seria detectado. Se forem enviados fotões polarizados, a sua polarização não pode ser detectada sem ser alterada. Desta forma, quem escutar a transmissão de dados pode ser facilmente detectado. Então só seria utilizada uma chave que não pudesse ser escutada. Nas

[260] *Johannes Buchmann*, "Faktorisierung großer Zahlen", Spektrum der Wissenschaft 2 1999, pp. 6 e seguintes.

[261] *Simon Singh*, Geheime Botschaften, Carl Hanser Verlag (1999), pp. 335 e seguintes.

[262] Informações sobre este programa encontram-se no endereço www.pgpi.com.

tentativas já efectuadas foi conseguida uma transmissão por 48 km de fibra de vidro e uma transmissão aérea de 500 m[263].

11.4. Segurança dos produtos de encriptação

No debate sobre a verdadeira segurança dos processos de encriptação, surge constantemente a crítica de que os produtos norte-americanos possuem funções-alçapão. Por exemplo, o programa *Excel* causou grandes títulos na imprensa, tendo-se afirmado que na sua versão europeia metade da chave é inserida abertamente no cabeçalho do documento. A Microsoft também mereceu a atenção da imprensa quando um *hacker* alegadamente encontrou uma "chave NSA" no programa, o que a Microsoft naturalmente desmentiu vigorosamente. Como a Microsoft não tornou público o código-fonte do programa, qualquer opinião a este respeito é especulação. Em qualquer caso, no que respeita às versões anteriores do PGP e *GnuPG*, a existência de uma tal função-alçapão pode ser excluída com grande certeza, dado que o respectivo código-fonte está no domínio público.

11.5. A encriptação em conflito com os interesses do Estado

11.5.1. Tentativas de limitação da encriptação

Vários Estados proíbem a utilização de *software* de encriptação ou de aparelhos de criptografia e fazem depender a abertura de excepções à sua autorização. Neste contexto, não se trata apenas de ditaduras como, por exemplo, a China, o Irão ou o Iraque. Também alguns Estados democráticos elaboraram leis visando limitar a utilização ou venda de programas ou aparelhos de encriptação. Na verdade, a comunicação deveria ser protegida contra a possibilidade de leitura por particulares não autorizados mas o Estado deveria, tal como dantes, manter a possibilidade de, em determinados casos, proceder legitimamente a escutas. A perda da superioridade técnica das autoridades deveria ser compensada por proibições estabelecidas por lei. Assim, até à pouco tempo a França proibiu a utilização da criptografia em geral e fez depender a sua utilização de uma autorização individual. Na Alemanha também houve, há alguns anos, um debate sobre as limitações da encriptação e a obrigação de depositar a chave. Os EUA, em vez disso, limitaram a dimensão da chave no passado.

11.5.2. Importância da encriptação segura para o comércio electrónico

Entretanto, estas tentativas devem ter fracassado definitivamente. Ao interesse do Estado em ter acesso à desencriptação e, consequentemente, ao texto original opõe-se nomeadamente, não só o direito à preservação da esfera privada, mas também interesses económicos muito fortes. Porque o comércio electrónico e as transferências bancárias electrónicas dependem de uma comunicação segura na Internet. Se ela não puder ser garantida, estas técnicas estão condenadas ao fracasso porque então a confiança dos clientes deixaria de existir. Esta correlação explica a mudança das políticas norte-americana ou francesa relativamente à criptografia.

Neste contexto, devemos notar que o comércio electrónico necessita de processos de encriptação seguros numa perspectiva dupla: não só para encriptar a mensagem mas também para comprovar sem a menor dúvida a identidade do parceiro comercial. A assinatura electrónica pode funcionar nomeadamente através da inversão da utilização do processo de chave pública: a chave privada é utilizada para a encriptação e a chave pública para a desencriptação. Esta forma de encriptação

[263] Sobre a criptografia quântica, *Reinhardt Wobst*, Abenteuer Kryptographie[2], Adison-Wesley (1998), pp. 234 e seguintes.

confirma a autenticidade da assinatura. Qualquer um pode convencer outra pessoa da sua autenticidade através da utilização da chave pública mas não pode imitar a própria assinatura. Esta função também foi incorporada no PGP de uma forma bastante fácil de utilizar.

11.5.3.Problemas para as pessoas que viajam em negócios

Em muitos países, é proibido às pessoas que viajam em negócios utilizar programas de encriptação nos computadores portáteis que os acompanham. Isto impede qualquer tipo de protecção das comunicações com a sua própria empresa, bem como a segurança dos dados transportados contra possíveis ataques.

11.6. Questões práticas da encriptação

Para responder à questão sobre quem e em que circunstâncias deverá ter acesso à encriptação, convém distinguir entre particulares e empresas. No que respeita aos particulares, devemos afirmar abertamente que a encriptação de comunicações telefónicas e por fax através da utilização de criptotelefones ou criptofax não é verdadeiramente exequível. Isto porque, por um lado, os custos de aquisição destes aparelhos são relativamente elevados mas também porque a sua utilização implica que o parceiro de comunicação deve dispor dos mesmos aparelhos, o que só acontece em casos muito raros.

Pelo contrário, os e-mail podem e devem ser protegidos por encriptação contra todos. À afirmação frequentemente reiterada de que uma pessoa não tem segredos e por isso não precisa de encriptação devemos contrapor que as mensagens por escrito normalmente também não são enviadas em cartões postais. Um e-mail não encriptado não é mais do que uma carta sem envelope. A encriptação de e-mails é segura e relativamente fácil e na Internet já se encontram programas de utilização fácil - como, por exemplo, o PGP/GnuPG – que até são disponibilizados gratuitamente aos particulares. Porém, lamentavelmente continua a faltar a sua necessária divulgação. Neste contexto, seria desejável que o sector público desse o bom exemplo e procedesse à encriptação normalizada, de forma a desmistificar a encriptação. No que diz respeito às empresas, deveria providenciar-se rigorosamente para que as informações sensíveis sejam transmitidas só através de meios de transmissão seguros. Isto parece evidente – e para as grandes empresas é - mas justamente as pequenas e médias empresas transmitem informações internas via e-mail frequentemente sem a encriptação, porque ainda não foram suficientemente sensibilizadas para o problema. Neste contexto, devemos esperar que as associações industriais e as câmaras de comércio se empenhem muito mais na sensibilização. Na verdade, a encriptação dos e-mails é só mais um aspecto de segurança entre muitos e, principalmente, não servirá de nada se as informações já forem acessíveis a outros ainda antes de serem encriptadas. Isto significa que é imperativo tornar seguro o local de trabalho no seu conjunto, para que seja garantida a segurança dos espaços utilizados, e examinar o acesso físico aos escritórios e computadores. Porém, também é imperativo impedir o acesso não autorizado às informações através da rede, por meio da instalação das correspondentes *firewalls*. Neste contexto, a ligação entre a Intranet e a Internet coloca riscos específicos. Se quisermos levar a sério a segurança, então também deveríamos usar apenas sistemas operativos cujo código-fonte seja do domínio público e testado, pois só assim podemos saber com segurança o que acontece aos dados. Assim, para as empresas existe uma imensidão de tarefas a efectuar no domínio da segurança. Já existem no mercado inúmeras firmas que dão consultadoria em matéria de segurança e se encarregam da sua execução concreta a preços acessíveis e a oferta aumenta constantemente para corresponder à procura. Além disto, devemos esperar que as associações industriais e as câmaras de comércio se

ocupem deste problema, a fim de sensibilizar particularmente as pequenas empresas para a problemática da segurança e apoiá-las na concepção e execução de um conceito de protecção abrangente.

12. Relações externas da UE e recolha de dados por parte dos serviços de informações

12.1. Introdução

A adopção do Tratado de Maastricht, em 1991, foi portadora da criação da Política Externa e de Segurança Comum (PESC) na sua forma mais elementar, novo instrumento político da União Europeia. Seis anos mais tarde, o Tratado de Amesterdão veio consolidar a estrutura da PESC, criando a possibilidade de iniciativas de defesa comum no interior da União Europeia, sem prejuízo das alianças existentes. Com base no Tratado de Amesterdão e tendo em conta a experiência colhida no Kosovo, o Conselho Europeu de Helsínquia, de Dezembro de 1999, lançou a iniciativa de segurança e de defesa europeia. Esta iniciativa visa a criação, até ao segundo semestre de 2003, de uma força multinacional composta por 50.000 a 60.000 soldados. A existência de uma tal força militar multinacional tornará inevitável a instituição de uma capacidade autónoma em matéria de informações. A simples integração da existente a nível da UEO seria insuficiente para o efeito. Afigura-se inevitável um reforço da cooperação entre os serviços de informações dos Estados-Membros mais ambicioso do que as actuais formas de cooperação.

Não obstante, o desenvolvimento da PESC não constitui o único elemento que conduz ao reforço da cooperação entre os serviços de informações da União. Com efeito, os progressos da integração económica registados na União europeia tornarão, por seu turno, necessária uma cooperação mais intensa no domínio da recolha de dados pelos serviços de informações. Uma política económica comum requer uma percepção comum da realidade económica no exterior da União Europeia. Uma posição comum nas negociações comerciais conduzidas a nível da OMC ou com países terceiros necessita de uma protecção comum da posição negocial. As grandes empresas europeias necessitam de uma protecção comum contra a espionagem económica procedente do exterior da UE.

Importa, enfim, salientar que o desenvolvimento do segundo pilar e das actividades da União no domínio da justiça e dos assuntos internos deverá igualmente conduzir a um reforço da cooperação entre os serviços de informações. A luta contra o terrorismo, contra o tráfico ilícito de armas, contra o tráfico de seres humanos e contra o branqueamento de capitais não pode processar-se sem uma cooperação intensa entre os serviços de informações.

12.2. Possibilidades de cooperação no interior da UE

12.2.1. A actual cooperação[264]

Embora constitua, desde há muito, tradição o facto de os serviços de informações apenas confiarem nas informações que eles próprios recolhem e de nutrirem mesmo desconfiança relativamente aos seus homólogos no território da União Europeia, a cooperação entre estes serviços acusa um aumento progressivo. São frequentes os contactos existentes no quadro da NATO, da UEO e da União Europeia. Embora os serviços de informações da NATO continuem

[264] *Charles Grant,* Intimate relations. Can Britain play a leading role in European defence - and keep its special links to US intelligence? 4.2000, Centre for European Reform

largamente dependentes do contributo dos Estados Unidos, que dispõem de instrumentos bastante mais aperfeiçoados, a criação do centro de satélites da UEO em Torrejon (Espanha) e de uma secção de informações a nível do Quartel-General da UEO contribuíram para tornar a actuação da Europa mais autónoma neste domínio.

12.2.2. Vantagens de uma política comum europeia no domínio da informação

Em complemento dos desenvolvimentos já em curso, cumpre assinalar as vantagens objectivas de que se revestiria uma política comum em matéria de serviços de informações.

Essas vantagens são as seguintes:

12.2.2.1. Vantagens de ordem prática

Em primeiro lugar, as informações secretas e não-secretas disponíveis são demasiado numerosas para poderem ser recolhidas, examinadas e avaliadas por um único organismo ou para constituírem objecto de acordos bilaterais na Europa Ocidental. As actividades dos serviços de informações englobam a defesa, as políticas económicas nacionais e internacionais de países terceiros, a luta contra o crime organizado e o tráfico de estupefacientes. Mesmo se existisse apenas a nível elementar, nomeadamente, para efeitos de recolha de informações de acesso geral (OSINT), a cooperação propiciaria resultados que assumem grande importância para as políticas da União.

12.2.2.2. Vantagens de ordem financeira

No passado recente, os orçamentos destinados à recolha de dados pelos serviços de informações foram sujeitos a reduções, o que, nalguns casos, continua a observar-se. Simultaneamente, a necessidade de informações aumentou, o mesmo tendo acontecido, por conseguinte, aos respectivos serviços. Assim sendo, esses orçamentos não só tornam essa cooperação possível, como também, a longo prazo, vantajosa em termos financeiros. Em particular no caso do estabelecimento e da manutenção de infra-estruturas técnicas, as operações conjuntas revestem-se de importância quando os recursos financeiros são escassos, mas também se revelam significativas em matéria de avaliação da informação recolhida. O reforço da cooperação incrementará a eficácia da recolha de dados pelos serviços de informações.

12.2.2.3. Vantagens de ordem política

Em princípio, as informações recolhidas são utilizadas para propiciar aos governos a possibilidade de tomarem melhor e mais bem fundada a tomada de decisões. Uma maior integração política e económica da União implica que as informações sejam acessíveis a nível europeu e que assentem em mais do que uma fonte.

12.2.3. Conclusões

Estas vantagens objectivas ilustram a importância crescente da cooperação no interior da União Europeia. No passado, os estados-nação asseguravam, cada um de *per se*, a sua segurança externa, a ordem pública interna, a prosperidade nacional e identidade cultural. Hoje em dia, a União Europeia assume, pouco a pouco, um papel que é, pelo menos, complementar do papel do

Estado-Nação. É impossível que os serviços de informações sejam o último e único domínio a não ser abrangido pelo processo da integração europeia.

12.3. Cooperação além União Europeia

Desde a Segunda Guerra Mundial, a cooperação no domínio da recolha de informações tem-se processado, não primordialmente a nível europeu, mas sobretudo a nível transatlântico. Foi já mencionado o estabelecimento de relações particularmente estreitas em matéria de recolha de informações entre o Reino Unido e os Estados Unidos. Também no domínio das informações militares e no âmbito da NATO, e para lá deste, os Estados Unidos foram e continuam a ser o parceiro dominante. Consequentemente, a principal questão consiste em saber se o reforço da cooperação europeia no domínio da recolha de informações poderá perturbar gravemente as relações com os Estados Unidos ou se comportará eventualmente o reforço dessas mesmas relações. Como evoluirão as relações entre a UE e os EUA sob a nova Administração Bush? Como evoluirão as particulares relações existentes entre os Estados Unidos e o Reino Unido neste contexto?

Há quem sustente não existir necessariamente qualquer contradição entre as relações especiais Estados Unidos/Reino Unido e a evolução das PESC. Outros entendem que o problema da recolha de informações pode representar a questão que obrigará o Reino Unido a decidir se o seu destino é europeu ou transatlântico. Os estreitos elos existentes entre o Reino Unido e os Estados Unidos (e as outras partes do acordo UK/USA) poderiam tornar mais difícil a partilha de informações entre os outros Estados da União, dado o Reino Unido poder mostrar-se menos propenso a partilhar informações no interior da Europa e os seus parceiros da UE poderem manifestar-se menos confiantes relativamente ao Reino Unido. Do mesmo modo, se os Estados Unidos considerarem que o Reino Unido desenvolveu elos especiais com os seus parceiros da UE e que tal constitui parte integrante de um acordo europeu específico, poderiam hesitar em partilhar informações com o Reino Unido. O reforço da cooperação neste domínio pode, pois, constituir um importante teste das ambições europeias do Reino Unido, bem como da capacidade de integração da própria União.

Nas circunstâncias actuais, afigura-se, todavia, pouco verosímil que mesmo progressos extremamente rápidos na cooperação entre os parceiros europeus permitam, a curto e, mesmo, a longo prazo, substituir o avanço tecnológico dos Estados Unidos. A União Europeia não estará habilitada a criar uma rede avançada de satélites SIGINT, de satélites de obtenção de imagens e de estações terrestres. A União Europeia não estará habilitada a criar, a curto prazo, uma rede de informática altamente sofisticada que lhe permita proceder à selecção e avaliação do material recolhido. A União Europeia não estará disposta a mobilizar os recursos orçamentais necessários para implementar uma verdadeira alternativa às actividades dos Estados Unidos neste domínio. Do ponto de vista tecnológico e financeiro, seria, por conseguinte, do interesse da União manter relações estreitas com os Estados Unidos no domínio da recolha de informações. Todavia, também do ponto de vista político, será importante manter e, eventualmente, reforçar as relações com os Estados Unidos, sobretudo no tocante à luta comum contra o crime organizado, o terrorismo, o tráfico de estupefacientes e de armas e o branqueamento de capitais. A promoção de operações conjuntas por parte dos serviços de informações revela-se necessária como instrumento de apoio de a uma luta comum. Acções comuns em matéria de manutenção da paz, como as observadas na ex-Jugoslávia, requerem um maior contributo europeu em todas as áreas de acção.

Por outro lado, uma maior consciência europeia deveria ser coadjuvada por uma maior responsabilidade europeia. A União Europeia deveria tornar-se um parceiro com maior igualdade de direitos, não só no plano económico, mas também no domínio da defesa e, por conseguinte, no domínio da recolha de informações. Assim sendo, uma capacidade mais autónoma da Europa em matéria de serviços de informações não deveria ser considerada como um elemento passível de enfraquecer as relações transatlânticas. Deveria, pelo contrário, permitir reforçar as relações em causa, fazendo da União um parceiro com maior igualdade de direitos e mais competente. Concomitantemente, cumpre à União Europeia envidar esforços autónomos no sentido de proteger a sua economia e a sua indústria contra ameaças ilegais e indesejáveis, como sejam a espionagem económica, a cibercriminalidade e os atentados terroristas. Por outro lado, a existência de um consenso transatlântico revela-se necessária no domínio da espionagem industrial. A União Europeia e os Estados Unidos deveriam acordar em normas relativas ao que é autorizado nesta matéria e ao que é proibido no domínio em causa. No intuito de reforçar a cooperação transatlântica, deveria ser lançada, a nível da OMC, uma iniciativa comum. Tratar-se-ia de utilizar os mecanismos da referida organização para proteger um desenvolvimento económico leal a nível mundial.

12.4. Observações finais

O desenvolvimento de uma capacidade comum da União Europeia em matéria de informações deve ser considerado como necessário e inevitável, salvaguardando, simultaneamente, a indispensável protecção da vida privada dos cidadãos europeus. A cooperação com países terceiros, e em particular com os Estados Unidos, deverá ser mantida e, se possível, reforçada. Tal não significa necessariamente que as actividades europeias SIGINT devam automaticamente ser integradas num sistema ECHELON da UE independente ou que a União deva tornar-se de pleno direito parceiro do Acordo UKUSA. Não obstante, o exercício de uma responsabilidade verdadeiramente europeia no domínio da recolha de informações por parte dos respectivos serviços deverá ser seriamente encarada. Uma capacidade europeia integrada neste domínio requer, em simultâneo, um sistema de controlo político, na Europa, das actividades dos organismos respectivos. Há que tomar decisões sobre os meios a que deverá recorrer para analisar as informações e adoptar as decisões políticas decorrentes da análise. A ausência de um tal sistema de controlo político e, por conseguinte, da consciência e responsabilidade políticas no respeitante ao processo de recolha de informações seria prejudicial ao processo de integração europeia.

13. Conclusões e recomendações

13.1. Conclusões

Da existência de um sistema mundial de intercepção das comunicações privadas e económicas (sistema ECHELON)

A existência de um sistema de escuta das comunicações que opera a nível mundial com a participação dos Estados Unidos da América, do Reino Unido, do Canadá, da Austrália e da Nova Zelândia, no quadro do acordo UKUSA, deixou já de constituir objecto de dúvidas. Com base nos indícios disponíveis, bem como em inúmeras declarações coincidentes oriundas de círculos muito diferenciados, incluindo fontes americanas, pode presumir-se que, pelo menos durante algum tempo, tenha sido dado ao sistema ou a partes do mesmo o nome de código "ECHELON". Importante afigura-se o facto de o mesmo ser utilizado para fins de escuta das comunicações privadas e económicas, mas não militares.

A análise demonstrou que as possibilidades técnicas deste sistema não são provavelmente tão vastas como presumido por alguns meios de comunicação social. Independentemente desse facto, afigura-se preocupante que numerosos responsáveis comunitários, que foram ouvidos sobre esta matéria, designadamente membros da Comissão, tenham declarado não terem qualquer conhecimento do sistema.

Dos limites do sistema de intercepção

O sistema de vigilância baseia-se sobretudo na escuta global de comunicações por satélite. Ora, em regiões com elevada densidade de comunicações, apenas uma exígua parte das comunicações se efectua por satélite. Tal significa que a maioria das comunicações não podem ser interceptadas por estações terrestres, mas unicamente mediante a intercepção de cabos ou escuta via rádio. As averiguações indicaram, porém, que os países UKUSA apenas têm acesso a uma parte ainda muito restrita das comunicações por cabo ou por rádio e que, por carência de pessoal, apenas podem avaliar uma parte ainda mais restrita da comunicação. Por extremamente vastos que possam ser os meios e as capacidades disponíveis para fins de intercepção de comunicações, o número extremamente elevado destas últimas torna impossível, na prática, um controlo rigoroso e absoluto de todas as comunicações.

Da eventual existência de outros sistemas de intercepção

Uma vez que a intercepção de comunicações constitui um meio de espionagem tradicional dos serviços secretos, um tal sistema poderia ser explorado por outros países desde que disponham dos meios financeiros e das condições geográficas necessárias. Em virtude dos seus territórios ultramarinos, a França estaria geográfica e tecnicamente habilitada, enquanto único Estado-Membro da UE, a operar, por si só, um sistema de intercepção mundial. São muito os indícios existentes de que também a Rússia opera um tal sistema.

Da compatibilidade com o direito da UE

No atinente à questão da compatibilidade de um sistema do tipo ECHELON com o direito da UE, impõe-se estabelecer a seguinte diferenciação: se o sistema for apenas utilizado para fins de informação, não se observa qualquer contradição com o direito da UE, na medida em que as actividades ao serviço da segurança do Estado não são abrangidas pelo Tratado CE, sendo-lhes

aplicável o título V do Tratado UE (PESC), que não contém ainda qualquer disposição nesta matéria, pelo que não se observa qualquer colisão. Se, pelo contrário, o sistema é objecto de utilização abusiva para espionar a concorrência, é o mesmo contrário à obrigação de lealdade que vincula os Estados-Membros e à concepção de um mercado comum em que a concorrência é livre. Se um Estado-Membro nele participa, viola, assim a legislação da União.

Na sua reunião de 30 de Março de 2000, o Conselho declarou não poder aceitar a instituição ou a existência de um sistema de intercepção que não respeite a ordem jurídica dos Estados-Membros e que constitua uma violação dos princípios fundamentais do respeito pela dignidade humana.

Da compatibilidade com o direito fundamental ao respeito da vida privada e familiar (Artigo 8º da Convenção dos Direitos do Homem)

Todas as operações de intercepção de comunicações constituem uma grave ingerência na vida privada da pessoa humana. O artigo 8º da Convenção dos Direitos do Homem, que protege a vida privada, apenas permite uma tal ingerência quando esteja em causa garantir a segurança nacional, desde que a mesma se encontre prevista em disposições do direito nacional, disposições essas que sejam de acesso geral e estabeleçam em que circunstâncias e condições os poderes públicos a ela podem recorrer. Tais ingerências devem ser proporcionadas, razão pela qual se impõe ponderar os interesses em jogo. Não é suficiente que a intervenção seja meramente oportuna ou desejável.

Um sistema de informações que, aleatória e sistematicamente, interceptasse todas e quaisquer comunicações, infringiria o princípio da proporcionalidade e seria, por conseguinte, contrário à Convenção dos Direitos do Homem. Observar-se-ia igualmente uma violação da Convenção se as disposições por força das quais a vigilância das comunicações tem lugar fossem desprovidas de base jurídica, caso esta não fosse acessível a todos ou se se encontrasse formulada de molde a que qualquer indivíduo não pudesse prever as suas consequências. Dado que as disposições com base nas quais os serviços de informações norte-americanos operam no estrangeiro são, em grande parte, secretas, o respeito do princípio da proporcionalidade afigura-se, no mínimo, questionável. Observa-se manifestamente uma violação dos princípios de acesso ao direito e de previsibilidade dos seus efeitos. Embora os EUA não sejam partes contratantes na Convenção relativa aos Direitos do Homem, os Estados-Membros devem proceder à sua observância. Não podem, com efeito, subtrair-se às obrigações que a mesma lhes impõe autorizando os serviços de informações de outros países submetidos a disposições menos rigorosas a operarem no seu território. Caso contrário, o princípio da legalidade e as suas duas componentes (acesso e previsibilidade) seria privado dos seus efeitos e a jurisprudência do Tribunal dos Direitos do Homem seria destituída de conteúdo.

A conformidade com os direitos fundamentais de uma actividade legalmente legitimada de serviços de informações exige, além disso, a existência de suficientes mecanismos de controlo, a fim de equilibrar os riscos inerentes à acção secreta levada a efeito por uma parte do aparelho administrativo. Atendendo a que o Tribunal Europeu dos Direitos do Homem salientou expressamente a importância de um sistema de controlo eficaz no domínio das actividades dos serviços de informações, afigura-se preocupante que alguns Estados-Membros não disponham de órgãos parlamentares de controlo dos serviços secretos.

Da protecção dos cidadãos da UE contra os serviços de informações: será aquela suficiente?

Dado que a protecção dos cidadãos da UE depende da situação jurídica observada nos Estados-Membros, sendo consideráveis as diferenças registadas e verificando-se, em alguns casos, a ausência de órgãos de controlo parlamentares, dificilmente pode ser considerada suficiente a protecção observada. Todavia, mesmo onde existem tais órgãos de controlo, grande é a tentação de votar uma maior atenção às actividades internas dos serviços de informações do que às actividades externas, uma vez que, regra geral, os cidadãos nacionais apenas são visados no primeiro caso.

Em caso de cooperação entre serviços de informações no âmbito da PESC e as autoridades de segurança no quadro da CJAI, as instituições são convidadas a promoverem a criação de disposições de protecção suficientes para os cidadãos europeus.

Da espionagem económica

Constitui parte integrante das atribuições dos serviços de informações estrangeiros o interesse por dados económicos, como sejam e desenvolvimento de sectores, a evolução dos mercados das matérias-primas, a observância de embargos, o respeito das disposições relativas ao aprovisionamento de bens de utilização dual, etc.. Essa a razão pela qual as empresas que desenvolvem actividades nesses domínios são, frequentemente, vigiadas. Os serviços de informações dos EUA não procedem, porém, apenas à produção de informações de carácter económico geral. Sob a alegação de combate a tentativas de suborno, interceptam igualmente as comunicações das empresas no quadro da adjudicação de contratos. Sendo particularmente circunstanciada, esta intercepção comporta o risco de as informações serem utilizadas para a espionagem da concorrência em vez de servirem o objectivo de luta contra a corrupção, ainda que os EUA e o Reino Unido declarem que tal não praticam. Neste contexto, cumpre referir que o papel do "Advocacy Center" do Ministério Norte-Americano do Comércio continua a não ser inteiramente claro, tendo o mesmo cancelado um encontro que havia sido agendado no intuito de esclarecer essa situação. Há também que salientar que, no quadro da OCDE, foi adoptada, em 1997, uma Convenção relativa à luta contra a corrupção de agentes públicos, a qual prevê que a corrupção seja passível de punição a nível internacional. Assim, também sob este aspecto, a corrupção não pode justificar, em casos isolados, a intercepção de comunicação.

Em todo o caso, cumpre afirmar claramente que é intolerável que os serviços de informações se deixem instrumentalizar para efeitos de espionagem da concorrência, espionando empresas estrangeiras para lograr vantagens concorrenciais para empresas nacionais. Embora se afirme com frequência que o sistema de intercepção mundial examinado no quadro do presente documento é utilizado para esse efeito, não existem provas factuais que o atestem.

Com efeito, os dados sensíveis encontram-se fundamentalmente, no interior das empresas, pelo que a espionagem consiste, sobretudo, na tentativa de obter informações através dos próprios funcionários ou de pessoas infiltradas e, com frequência crescente, penetrando nas respectivas redes informáticas. Apenas nos casos em que dados sensíveis são encaminhados para o exterior via cabo ou via rádio (satélite) é possível utilizar um sistema de vigilância das comunicações para fins de espionagem da concorrência. Tal aplica-se sistematicamente aos três casos seguintes:

- a empresas que operam em três fusos horários, de tal modo que os resultados intercalares podem ser enviados da Europa para a América e, seguidamente, para a Ásia;
- a videoconferências de empresas multinacionais realizadas via satélite ou por cabo;

- a negociações de contratos importantes *in loco* (construção de infra-estruturas ou de infra-estruturas de telecomunicações, construção de sistemas de transporte, etc.) em que são necessários contactos com a central da empresa em causa. No caso das pequenas e médias empresas, a consciência do risco e da necessidade de segurança é, lamentavelmente, com frequência, insuficiente, não sendo muitas vezes reconhecidos os riscos de espionagem económica e de intercepção das comunicações. Uma vez que, nas Instituições europeias (à excepção do Banco Central Europeu, da Direcção-Geral "Relações Externas" do Conselho, bem como da Direcção-Geral "Relações Externas" da Comissão), a sensibilização para as questões de segurança nem sempre é manifesta, observa-se uma necessidade de actuação imediata.

Das possibilidades de autoprotecção

As empresas devem proteger todo o seu ambiente de trabalho, bem como todos os meios de comunicação que sirvam para transmitir informações sensíveis. São em número suficiente os sistemas de encriptação seguros existentes a preços módicos no mercado europeu. Também as pessoas singulares devem ser incentivadas à encriptação do respectivo correio electrónico, uma vez que um correio não criptado equivale a uma carta sem envelope. Na Internet, encontram-se sistemas relativamente conviviais, postos à disposição de todas as pessoas, por vezes mesmo gratuitamente.

Da cooperação entre os serviços de informações existentes na UE

Em Dezembro de 1999, o Conselho Europeu de Helsínquia decidiu promover o desenvolvimento de estruturas militares europeias mais eficazes, por forma a dar cumprimento a toda a panóplia de missões estabelecidas em Petersberg no contexto da PESC. A bem da consecução deste objectivo, a UE deveria estar habilitada, o mais tardar em 2003, a destacar rapidamente forças militares compostas por 50.000 a 60.000 pessoas dotadas de autonomia e das capacidades necessárias em matéria de comando de tropas e de reconhecimento estratégico, bem como das devidas capacidades em matéria de serviço de informações. As primeiras medidas tendentes à constituição de tais capacidades em matéria de serviço de informações foram já empreendidas no quadro da UEO, bem como do comité permanente de política e de segurança.

A cooperação entre os serviços de informações da UE afigura-se imprescindível, uma vez que, por um lado, uma política de segurança comum que excluísse os serviços secretos seria absurda e, por outro, tal comportaria inúmeras vantagens de ordem profissional, financeira e política, sendo, além disso, conforme à ideia de uma parceria assente na igualdade de direitos com os Estados Unidos e susceptível de reunir todos os Estados-Membros no seio de um sistema instituído na plena observância da Convenção dos Direitos do Homem. O controlo correspondente por parte do Parlamento Europeu deverá, obviamente, nesse caso encontrar-se assegurado.

O Parlamento Europeu propõe-se dar aplicação ao Regulamento (CE) nº 1049/2001 relativo ao acesso do público aos documentos do Parlamento Europeu, do Conselho e da Comissão e adaptar o seu Regimento em conformidade no que respeita ao acesso a documentos sensíveis.

13.2. Recomendações

Relativamente à conclusão e à alteração de acordos internacionais sobre a protecção dos cidadãos e empresas

1. O Secretário-Geral do Conselho da Europa é instado a apresentar ao Comité de Ministros uma proposta sobre a adaptação, aos métodos de comunicação modernos e às

possibilidades de intercepção, do disposto no artigo 8º da CEDH referente à protecção da vida privada, no âmbito de um protocolo adicional ou juntamente com as disposições relativas à protecção dos dados aquando da revisão da Convenção respectiva, na condição de que tal não se traduza, nem numa redução do nível de protecção assegurado pelo Tribunal, nem numa redução da flexibilidade necessária à adaptação a ulteriores desenvolvimentos.

2. Os Estados-Membros da União Europeia são exortados a criar uma plataforma europeia, constituída por representantes dos órgãos nacionais responsáveis pelo controlo da observância dos direitos fundamentais e civis por parte dos Estados-Membros, bem como pela verificação da consentaneidade das disposições legais nacionais relativas aos serviços de informações com o enunciado da Convenção Europeia dos Direitos do Homem e a Carta dos Direitos Fundamentais da UE. A esse organismo incumbirá examinar as disposições legislativas relativas à garantia de confidencialidade da correspondência e das telecomunicações. Além disso, deverá o mesmo apresentar aos Estados-Membros uma recomendação relativa à elaboração de um código de conduta que garanta a todos os cidadãos europeus que se encontrem no território dos Estados-Membros a protecção da vida privada, tal como se encontra definida no artigo 7º da Carta dos Direitos Fundamentais da UE, e que, além disso, assegure que a actividade dos serviços de informações se processe em consentaneidade com os direitos fundamentais e, dessa forma, corresponda às condições referidas no capítulo 8 do presente relatório, em particular no seu ponto 8.3.4, em conformidade com o disposto no artigo 8º da CEDH.

3. Os Estados-Membros do Conselho da Europa são instados a adoptar um protocolo adicional que possibilite a adesão das Comunidades Europeias à CEDH ou a reflectir sobre outras medidas que excluam conflitos na jurisprudência entre o Tribunal de Estrasburgo e o do Luxemburgo.

4. Os Estados-Membros são instados a adoptar, aquando da próxima Conferência Intergovernamental, a Carta Europeia dos Direitos Fundamentais enquanto instrumento jurídico de observância obrigatória e passível de ser invocado em juízo, por forma a incrementar o nível de protecção dos direitos fundamentais, designadamente no respeitante à protecção da vida privada. Os órgãos da UE são instados a aplicar, na respectiva esfera de competências e de actividades, os direitos fundamentais constantes da Carta.

5. A União Europeia e os EUA são exortados a adoptar uma convenção nos termos da qual ambas as Partes aplicarão reciprocamente as normas relativas à protecção da vida privada e da confidencialidade da comunicação empresarial que se aplicam aos seus próprios cidadãos e empresas.

6. Exorta os Estados-Membros a concluirem um acordo com países terceiros na perspectiva do reforço da protecção da vida privada dos cidadãos da UE, nos termos do qual todas as partes contratantes se comprometam a que, em caso de intercepção praticada por uma das partes no território de uma outra, a primeira informará a segunda sobre as medidas previstas.

7. O Secretário-Geral da ONU é exortado a incumbir a comissão responsável de apresentar propostas tendentes a adaptar o artigo 17º do Pacto Internacional sobre os Direitos Civis e Políticos, que garante a protecção da vida privada, ao progresso técnico.

8. Os EUA são exortados a assinar o protocolo adicional ao Pacto Internacional sobre os Direitos Civis e Políticos, a fim de tornar admissíveis, em caso de violação, as queixas apresentadas por particulares à comissão dos direitos humanos, prevista no referido diploma; exorta as ONG norte-americanas pertinentes, em particular a ACLU (American Civil Liberties Union) e a EPIC (Electronic Privacy Information Center) a exercerem pressões nesse sentido junto do governo norte-americano.

9. O Conselho e os Estados-Membros são expressamente instados a instituir um sistema de vigilância e controlo democráticos das capacidades autónomas europeias dos serviços de informações, bem como de outras actividades correlacionadas a nível europeu. Cumpre cometer ao Parlamento Europeu, no quadro desse sistema de vigilância e controlo, uma importante função.

Relativamente às disposições legislativas nacionais de protecção dos cidadãos e empresas

10. Todos os Estados-Membros são expressamente instados a examinar a sua própria legislação em matéria de actividade dos serviços de informações à luz da respectiva consentaneidade com os direitos fundamentais, tal como consagrados na Convenção Europeia dos Direitos do Homem, bem como na jurisprudência do Tribunal Europeu dos Direitos do Homem e, eventualmente, a adaptá-la em conformidade. São os mesmos exortados a reconhecer a todos os cidadãos europeus as mesmas garantias legais em matéria de protecção da vida privada e de confidencialidade da correspondência. Caso as respectivas legislações prevejam discriminações no respeitante às competências de vigilância dos serviços secretos, cumpre eliminá-las.

11. Os Estados-Membros são instados a diligenciar no sentido de um nível de protecção comum face à actividade dos serviços de informações e a elaborar para esse efeito um código de conduta que se norteie pelo nível de protecção nacional mais elevado, uma vez que os cidadãos afectados pela actividade de um serviço de informações estrangeiro são, em geral, cidadãos de outros Estados e, por conseguinte, também de outros Estados-Membros. Deverá ser igualmente negociado com os EUA um código de conduta equivalente.

12. Os Estados-Membros são instados a reunir os seus dispositivos de intercepção, por forma a reforçarem a eficácia da PESD nos domínios de actividade dos serviços de informações, do combate ao terrorismo, da proliferação de armas nucleares e do tráfico internacional de estupefacientes, na observância das disposições relativas à protecção da vida privada dos cidadãos e à confidencialidade da comunicação empresarial, sob o controlo do Parlamento Europeu, do Conselho e da Comissão.

Relativamente a medidas legais específicas de combate à espionagem económica

13. Os Estados-Membros são exortados a examinar em que medida a espionagem económica e o suborno para fins de obtenção de contratos poderiam ser combatidos mediante disposições do direito europeu e internacional e, em especial, se seria possível adoptar uma regulamentação no âmbito da OMC que tivesse em conta o impacto de uma tal actividade em termos de distorção da concorrência, determinando, por exemplo, a nulidade de tais

contratos. Os EUA, o Canadá, a Austrália e a Nova Zelândia são instados a participar esta iniciativa.

14. Os Estados-Membros são instados a comprometer-se, de modo vinculativo, a não praticar espionagem económica directamente ou escudando-se atrás de uma potência estrangeira operante no seu território, nem a autorizar tal prática a uma potência estrangeira a partir do seu território, por forma a actuar, desse modo, em consonância com o espírito e a letra do Tratado CE.

15. Os Estados-Membros e o Governo dos Estados Unidos são instados a entabular um diálogo aberto entre os EUA e a União Europeia sobre espionagem económica.

16. As autoridades do Reino Unido são exortadas a esclarecer o seu papel na aliança UK/USA face à existência de um sistema de tipo "ECHELON" e à respectiva utilização para fins de espionagem económica.

17. Os Estados-Membros são instados a garantir que os seus serviços de informações não sejam abusivamente utilizados para fins de obtenção de informações de concorrência, porquanto tal seria contrário à obrigação de lealdade que incumbe aos Estados-Membros e à concepção de um mercado comum assente na livre concorrência.

Relativamente a medidas de aplicação da lei e respectivo controlo

18. Os Estados-Membros são convidados a garantir um controlo judicial e parlamentar adequado dos seus serviços secretos. Caso os Parlamentos nacionais não disponham de qualquer órgão parlamentar próprio de controlo dos serviços de informações, são os mesmos instados a proceder à respectiva criação.

19. As comissões nacionais de controlo dos serviços secretos são instadas, no exercício dos poderes de controlo que lhe foram conferidos, a atribuír grande importância à protecção da vida privada, independentemente de estar em causa o controlo de cidadãos nacionais ou de cidadãos de outros Estados-Membros da UE ou de países terceiros.

20. Os serviços de informações dos Estados-Membros são instados a só aceitarem dados provenientes de outros serviços de informações quando os mesmos tenham sido investigados em condições previstas no próprio direito nacional, uma vez que os Estados-Membros não podem eximir-se aos compromissos assumidos no âmbito da CEDH recorrendo a outros serviços de informações.

21. Apela à Alemanha e ao Reino Unido para que, no futuro, subordinem a autorização da intercepção de comunicações, no seu território, pelos serviços de informações dos EUA, à observância do disposto na CEDH, ou seja, para que estabeleçam que tais actividades deverão ser conformes ao princípio da proporcionalidade, que a sua base jurídica deverá ser acessível a todos, devendo os seus efeitos para o indivíduo ser previsíveis, e instituam as devidas medidas de controlo, uma vez que lhes cabe assegurar que as operações desenvolvidas pelos serviços de informações no seu território sejam consentâneas com o respeito dos direitos do Homem, independentemente de as operações em causa serem autorizadas ou meramente toleradas.

Relativamente a medidas de incremento da autoprotecção de cidadãos e empresas

22. A Comissão e os Estados-Membros são instados a informar os seus cidadãos e empresas sobre a possibilidade de intercepção, em determinadas circunstâncias, das respectivas informações transmitidas a nível internacional. Essa informação deverá ser acompanhada de assistência prático em matéria de definição e aplicação de medidas de protecção gerais, incluindo a segurança das tecnologias da informação.

23. A Comissão, o Conselho e os Estados-Membros são instados à definição e aplicação de uma política eficaz e activa em matéria de segurança da sociedade da informação. Nesse contexto, cumpre votar particular atenção a uma maior sensibilização de todos os utilizadores de modernos sistemas de comunicação para a necessidade e as possibilidades de protecção de informações confidenciais. Impõe-se instituir uma rede de organismos, coordenada à escala europeia, que seja susceptível de garantir assistência prática aquando do planeamento e da aplicação de estratégias de protecção global.

24. A Comissão e os Estados-Membros são instados a elaborar medidas adequadas para a promoção, o desenvolvimento e a produção de tecnologias e software de encriptação europeus e a apoiar todos os projectos que visem o desenvolvimento de criptosoftware de fácil utilização, com código-fonte aberto.

25. A Comissão e os Estados-Membros são instados a promover projectos de software, com código-fonte aberto ("open-source software"), pois só assim se poderá garantir que não sejam integrados quaisquer "backdoors" aos programas. A Comissão é convidada a estabelecer um padrão para a segurança de "software" destinado ao intercâmbio de informações por via electrónica, segundo o qual "software" cujo código-fonte não seja aberto, seja classificado como sendo "menos fiável".

26. As instituições europeias e as administrações públicas dos Estados-Membros são convidadas a praticar sistematicamente a encriptação de correio electrónico, a fim de, a longo prazo, tornar a encriptação regra habitual.

Relativamente a medidas de reforço da segurança nas Instituições

27. As Instituições comunitárias e as administrações públicas dos Estados-Membros são instadas a providenciar no sentido de que o seu pessoal tenha formação adequada e de que, no quadro de estágios e cursos de formação específicos, se familiarize com as novas técnicas de encriptação.

28. A Comissão é incumbida de encomendar um estudo em matéria de segurança que ilustre o que deve ser protegido, bem como um plano de protecção.

29. A Comissão é instada a proceder a uma actualização do seu sistema de encriptação, por forma a adaptá-lo ao progresso técnico, dado ser imperativa uma modernização do mesmo, solicitando-se à autoridade orçamental (Conselho, conjuntamente com o Parlamento) a disponibilização dos recursos para o efeito necessários.

30. Solicita-se à comissão competente a elaboração de um relatório de iniciativa sobre a segurança e a protecção da confidencialidade nas Instituições europeias.

31. A Comissão é convidada a garantir a protecção dos dados por si processados e a intensificar a protecção de documentos que não são de acesso público.

32. A Comissão e os Estados-Membros são instados a investir, no âmbito do 6º Programa-Quadro de Investigação, em novas tecnologias de encriptação e na investigação no domínio da segurança contra tentativas de desencriptação.

Relativamente a outras medidas

33. As empresas são exortadas a cooperar de forma mais estreita com as instituições de contra-espionagem, notificando em particular os ataques provenientes do exterior para fins de espionagem económica, de modo a aumentar a eficácia destas instituições;

34. A Comissão é convidada a apresentar uma proposta de instituição - em estreita colaboração com a indústria e os Estados-Membros - de uma rede coordenada europeia de serviços de consultoria para questões relacionadas com a segurança das informações das empresas - designadamente nos Estados-Membros em que ainda não existam tais centros -, a qual, para além do aumento da sensibilização para o problema, tenha também como missão proporcionar ajuda prática;

35. A Comissão é instada a prestar atenção particular à situação dos países candidatos no respeitante a questões de segurança. Caso, em virtude da carência de independência tecnológica, os países em causa não possam assumir as medidas de protecção necessárias, deveriam ser apoiados nesse domínio.

36. O Parlamento Europeu é convidado a organizar um congresso supra-europeu de protecção da vida privada face à vigilância das telecomunicações, a fim de criar uma plataforma destinada às ONG da Europa, dos EUA e de outros Estados, na qual se possam discutir aspectos transfronteiriços e internacionais e coordenar domínios de actividades e procedimentos.

PARLAMENTO EUROPEU

1999 *2004*

Documento de sessão

FINAL
A5-0264/2001
PAR2

11 de Julho de 2001

RELATÓRIO

sobre a existência de um sistema global de intercepção de comunicações privadas e económicas (sistema de intercepção ECHELON) (2001/2098 (INI))

Parte 2: Opiniões minoritárias
Anexos

Comissão Temporária sobre o Sistema de Intercepção Echelon

Relator: Gerhard Schmid

ÍNDICE

Página

OPINIÃO MINORITÁRIA de Giuseppe di Lello, Pernille Frahm e Alain Krivine 4

OPINIÃO MINORITÁRIA de Patricia McKenna e Ilka Schröder.....5

OPINIÃO MINORITÁRIA de Jean-Charles Marchiani 6

OPINIÃO MINORITÁRIA de Maurizio Turco.....7

Anexo I.: Lista dos peritos que prestaram informações perante a comissão.....8

Anexo II.: Bibliografia 158

Anexo III.: Intercepção de comunicações para fins de acção penal: definições e comentários 17

1. Nota preliminar 17

2. Distinção entre a intercepção de comunicações para fins de acção penal e a intercepção de comunicações por parte dos serviços de informações 17

3. Actividades desenvolvidas na UE em matéria de intercepção de comunicações para fins de acção penal 18

3.1. Observações gerais 18

3.2. Limitação da competência da UE a regulamentações técnicas 18

3.3. Iniciativas e actos jurídicos no domínio da intercepção de telecomunicações.....19

4. Actividades de carácter transnacional no domínio da intercepção de telecomunicações: definições e comentários 21

Anexo IV.: 23

OPINIÃO MINORITÁRIA de Giuseppe di Lello,

Pernille Frahm e Alain Krivine

O relatório da Comissão afirma a existência do sistema de intercepção Echelon gerido por diferentes Estados, entre os quais o Reino Unido, Estado-Membro da União Europeia, com a colaboração da Alemanha.

Um tal sistema de intercepção indiferenciada de comunicações, de dados e de documentos viola o direito fundamental ao respeito da vida privada, consagrado no artigo 8º da Convenção Europeia dos Direitos Humanos e no artigo 6º do Tratado da União Europeia.

Este sistema viola, por conseguinte, de um modo flagrante, as liberdades dos cidadãos europeus, a lógica do mercado livre e a segurança da União; qualquer que seja a nossa apreciação ou oposição a essas lógicas e a estes Tratados, as violações em causa são inaceitáveis.

Assim sendo, dever-se-ia, no quadro das conclusões do relatório, ter solicitado ao Reino Unido que se dissociasse do sistema Echelon e a Alemanha que encerrasse a base de intercepção situada no seu território. É de lamentar que a União Europeia se preocupe mais intensamente com a espionagem industrial do que com as escutas individuais.

OPINIÃO MINORITÁRIA de Patricia McKenna e Ilka Schröder

Constitui um aspecto importante do presente relatório o facto de no mesmo ser assinalada a existência do sistema Echelon. Todavia, são escassas as ilações políticas daí extraídas. O facto de o Parlamento Europeu criticar a prática de intercepção "Echelon", participando simultaneamente em planos tendentes ao estabelecimento de um serviço secreto europeu, afigura-se uma atitude hipócrita.

Não existe, a nível mundial, nenhum mecanismo de controlo público eficaz dos serviços secretos e das suas práticas antidemocráticas. É inerente aos serviços secretos a impossibilidade de serem controlados. Assim sendo, impõe-se abuli-los. O presente relatório contribui para legitimar um serviço secreto europeu, o qual violará direitos fundamentais – tal como o sistema "Echelon" o faz.

Maioritariamente, o Parlamento concentra-se na indústria cujos interesses em matéria de lucro se encontram alegadamente ameaçados pela espionagem industrial. Não obstante, a questão de importância vital reside no facto de ninguém poder já comunicar a longa distância num clima de confidencialidade. A espionagem política constitui uma ameaça muito maior do que a espionagem económica.

O presente relatório subestima sistematicamente estes perigos do sistema Echelon, sendo omisso relativamente ao projecto de intercepção ENFOPOL na UE. Viver ou não sob controlo permanente representa uma decisão fundamental para toda e qualquer sociedade. Aprovando o presente relatório, o Parlamento Europeu demonstra não ser sua preocupação proteger os direitos humanos e as liberdades dos cidadãos.

OPINIÃO MINORITÁRIA de Jean-Charles Marchiani

Foi sem surpresa que o Grupo UEN registou os resultados da votação do relatório do Deputado Schmid, o qual, inicialmente, era suposto visar o sistema de espionagem anglo-saxão "Echelon".

A maioria deste Parlamento havia, desde o início, indicado claramente as suas intenções, preferindo esta comissão *ad hoc* à instauração de uma verdadeira comissão de inquérito. Não tinha a mesma, pois, nada mais a temer da realização de trabalhos em que a eficácia do relator em proceder sistematicamente a manobras de diversão de nenhum modo se encontrava ameaçada por um grupo de descontentes motivados por razões de ordem diversa.

A nossa mensagem é límpida: os esforços do Deputado Schmid não conseguiram ocultar a prova da existência do sistema "ECHELON", nem a da implicação activa ou passiva de vários Estados-Membros no mesmo.

Assim sendo, observa-se uma grave violação aos princípios dos Tratados, a qual deveria ter dado lugar à aplicação de sanções ou, pelo menos, de medidas susceptíveis de evitar a subordinação de solidariedade intra-europeia aos imperativos da solidariedade anglo-saxã.

O compacto relatório da autoria do Deputado Schmid é rico em informações, mas falha o seu objectivo.

Cumpre-nos, por conseguinte, dele nos distanciar, rejeitando um funcionamento que permite, simultaneamente, a este Parlamento adoptar sanções "preventivas" contra um governo democraticamente eleito e de tal se abster em circunstâncias desta natureza… .

OPINIÃO MINORITÁRIA de Maurizio Turco

A. Enquanto se torna patente a presença provável de um sistema anglo-americano de "intercepções sistemáticas e generalizadas filtradas com motores de pesquisa", omite-se que essa capacidade tecnológica é certamente utilizada pela Alemanha e pela Holanda – e, provavelmente, pela França. Consequentemente – uma vez que os serviços secretos interceptam, em nome da segurança nacional, comunicações provenientes do estrangeiro sem autorização -, alguns países membros interceptam actividades de instituições, cidadãos e empresas de outros Estados-Membros.

B. O reforço da criptação, ainda que favoreça a protecção da vida privada, comporta, por outro lado, o reforço dos meios de decifração técnicos legais e dada a existência de um elo indissolúvel entre o desenvolvimento de sistemas criptográficos, criptoanalíticos e técnicas de intercepção.

C. As soluções devem, por conseguinte, ser identificadas na esfera política:

- mediante o controlo jurisdicional e parlamentar das actividades de intercepção e a vigilância dos serviços de polícia, segurança e espionagem;
- impedindo a multiplicação das autoridades de controlo que operam com normas diversas de protecção de dados e na ausência de um verdadeiro controlo democrático e jurisdicional;
- regulamentando – no sentido das normas mais rigorosas e retomando a jurisprudência do Tribunal Europeu dos Direitos do Homem – a protecção da vida privada dos cidadãos europeus contra ingerências preventivas por autoridades estatais eliminando as discriminações existentes na União entre cidadãos de diversos Estados-Membros.

Anexo I.: Lista dos peritos que prestaram informações perante a comissão

1. Deputados dos parlamentos nacionais

Arthur PAECHT, Assembleia Nacional, França
Armand De DECKER, Presidente do Senado belga
Anne-Marie LIZIN, Senado belga
Hans VAN HEVELE, Secretariado do Senado belga
Guilherme SILVA, Assembleia da República, Portugal
Ludwig STIEGLER, Bundestag, Alemanha
Dieter ANTONI, Parlamento austríaco
Desmond O´MALLEY, Parlamento irlandês

2. Representantes dos Serviços Secretos

Ernst UHRLAU, Coordenador dos Serviços Secretos no Gabinete do Chanceler Federal, Alemanha
Harald WOLL, Landesamt für Verfassungsschutz", Baden-Württemberg, Alemanha

3. Peritos em matéria de telecomunicações, de segurança das redes e de segurança informática

José Manuel MENDES ESTEVES SERRA VERA, Director Técnico, Banco Espírito Santo, Portugal
Clive FEATHER, Chefe do Departamento de Desenvolvimento de „Software", Demond Internet Ltd, Reino Unido
Jacques VINCENT-CARREFOUR, ex-chefe do Departamento de Segurança das Redes, France Telecom
Bruno PELLERO, Consultor especializado na intercepção de telecomunicações, Itália
Erhard MÖLLER, Lutz BERNSTEIN, Bernd SCHINKEN, Politécnico de Aachen, Alemanha

4. Autores e Jornalistas especialistas de ECHELON

Duncan CAMPBELL, Reino Unido
Bo ELKJAER, Dinamarca
Kenan SEEBERG, Dinamarca
James BAMFORD, Washington D.C.
Nicky HAGER, Nova Zelândia

5. Peritos no domínio da encriptação

Reinhard WOBST, Unix Software, Alemanha
Bernd ROELLGEN, Ciphers GmbH, Alemanha
Peter BAHR, Ciphers GmbH, Alemanha
Johan KEMPENAERS, KBC Bank, Bélgica
Leo VERHOEVEN, KBC Bank, Bélgica

Bart PRENEEL, Professor de Criptologia, Universidade Católica de Lovaina, Bélgica
Danny de TEMMERMAN, Comissão Europeia
Desmond PERKINS, Comissão Europeia

6. Peritos em matéria de espionagem económica e questões conexas

Sorbas VON COESTER, Director de Salamandre (firma de consultoria), França
Christian HARBULOT, Ecole de guerre économique, França
Thierry LA FRAGETTE, Circé, França
Ralf NEMEYER, Articon-Integralis, Alemanha

7. Direitos do Homem e protecção da vida privada

Dimitri YERNAULT, Universidade Livre de Bruxelas
Simon DAVIES, Privacy International, Reino Unido
Jérôme THOREL, Privacy International, França
Yaman AKDENIZ, Cyber Rights and Cyber Liberties, Leeds UK
David NATAF, Alexandre COSTE, Millet-Sala-Nataf (escritório de advogados), Paris
Rüdiger DOSSOW, Conselho da Europa, Estrasburgo

8. Representantes de Instituições Europeias

Comissão Europeia
Comissário Christopher PATTEN (Relações Externas)
Comissário António VITORINO (Justiça e Assuntos Internos)
Comissário Erki LIKKANEN (Política Empresarial e Sociedade da Informação)
Lodewijk BRIET, Direcção-Geral „Relações Externas“
Jacques DE BAENST, Chefe de Protocolo e da Segurança
Françoise DE BAIL, Direcção-Geral „Comércio“
Susan BINNS, Direcção-Geral „Mercado Interno“

Conselho da União Europeia
Brian CROWE, Director-Geral „Relações Externas“
Roland GENSON, Delegação Permanente do Luxemburgo, responsável pelo pelouro da „Justiça e Assuntos Internos“
Hervé MASUREL, Representante da Presidência francesa em exercício
Embaixador Gunnar LUND, Representante da Presidência sueca em exercício

Banco Central Europeu
Christoph BOERSCH, Wolfgang SCHUSTER, Dominique DUBOIS, Banco Central Europeu

9. Interlocutores no quadro das deslocações efectuadas

Deslocação do presidente e do relator a Paris, 18-19 de Janeiro de 2001
Jean-Claude MALLET, Secretary General of SGDN
Bertrand DUMONT, Géneral de corps aérien, Secrétaire général adjoint, SGDN
Claude-France ARNOULD, Directeur des affaires internationales et stratégiques, SGDN
Henri SERRES, Directeur chargé de la sécurité des systèmes d´information, SGDN
Stéphane VERCLYTTE, Conseiller pour les affaires juridiques et européennes, SGDN

Philippe DULUC, Conseillier pour les affaires scientifiques et techniques, SGDN
Gérard ARAUD, Directeur des Affaires Stratégiques, Ministère des Affaires etrangères
Olivier MOREAU, Directeur de la Securité, Ministère des Affaires etrangères
Eric PERRAUDAU, Conseillier, Ministère de la Defense
Jean-Pierre MILLET, Advogado

Deslocação do presidente e do relator a Londres, 24-26 de Janeiro de 2001
Tom KING, Chairman of the Intelligence & Security Committee, House of Commons
Alistair CORBETT, Head of the Secretariat of the ISC, House of Commons
Donald ANDERSON, Chairman of the Foreign Affairs Committee, House of Commons
Bruce GEORGE, Chairman of the Defence Committee, House of Commons
Jack STRAW, Secretary of State at the Home Office
Michael GILLESPIE, Security Service Coordinator
Charles GRANT, Director, Centre for European Reform
Casper BOWDEN, Director of FIPR

Deslocação da Mesa da comissão, dos coordenadores e do relator a Washington D.C., 6-12 de Maio de 2001
H.E. Günter BURGHARDT, Head of the Commission Delegation in Washington D.C.
James WOOLSEY, former Director CIA
Jeffrey RICHELSON, Director, National Security Archive, George Washington University
Marc ROTENBERG, Electronic Information Privacy Centre
Wayne MADSEN, Electronic Information Privacy Centre
David SOBEL, Electronic Information Privacy Centre
Barry STEINHARDT, Associate Director, American Civil Liberties Union
Porter J. GOSS, chairman House Permanent Select Committee on Intelligence
Nancy PELOSI, vice-chair House Permanent Select Committee on Intelligence
Robert DAVIS, Deputy Counsel for the office of Intelligence Policy Review, US Department of Justice.

Anexo II.: Bibliografia

BIBLIOGRAFIA CITADA

Advocacy Center, Homepage, http://www.ita.doc.gov/td/advocacy/

Andrew, Christopher, The growth of the Australian Intelligence Community and the Anglo-American Connection, 223-224 in *E. Hayden, H. Peake and S. Halpern* eds, In the Name of Inteligence. Essays in honor of *Washington Pforzheimer* (Washington NIBC Press 1995), 95-109

Andrew, Christopher, The making of the Anglo-American SIGINT Alliance, in: *Hayden B. Peake, Halpern, Samuel*. (Eds.): In the Name of Intelligence. Essays in Honor of Walter Pforzheimer, NIBC Press (1995), 95 -109

Andronov, Major *A.*, Zarubezhnoye voyennoye obozreniye, Nr.12, 1993, 37-43

Anonymus, Hacker's guide, Markt &Technik-Verlag (1999)

Bamford, James, Body of Secrets. Anatomy of the Ultra-Secret National Security Agency. From the Cold War through the Dawn of a new Century, Doubleday Books (2001)

Bamford, James, The Puzzle Palace. Inside the National Security Agency, America's most secret intelligence organization, Penguin Books (1983)

Benett, Gordon, Conflict Studies and Research Center, The Federal Agency of Government Communications and Information, August 2000, http://www.csrc.ac.uk/pdfs/c105.pdf

Berliner Zeitung, Abgehört, 22.1.1996

Bode, Britta, Heinacher, Peter, Sicherheit muß künftig zur Chefsache erklärt werdenn Handelsblatt, 29.8.1996

Brady, Martin, Direktor der DSD, Brief vom 16.3.1999 an Ross Coulthart, Sunday Program Channel 9; http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp; http://sunday.ninemsn.com/01_cover_stories/article_335.asp

Bronskill, Jim, Canada a key snooper in huge spy network, Ottawa Citizen, 24.10.2000, http://www.ottawacitizen.com/national/990522/2630510.html

Buchmann, Johannes, Faktorisierung großer Zahlen, Spektrum der Wissenschaft 2, 1999

Bundesministerium für Wirtschaft und Technologie der Bundesrepublik Deutschland, Computerspionage, Dokumentation Nr. 44, Juli 1998

Bundesministerium für Wirtschaft und Technologie der Bundesrepublik Deutschland, Informationen für geheimschutzbetreute Unternehmen (1997)

Bundesverfassungsgericht der Bundesrepublik Deutschland, BVerfG-Urteil, 1 BvR 2226/94 vom 14.7.1999 (zu Art. 10 GG, Gesetz zu Artikel 10 Grundgesetz)

Campbell, Duncan, A tecnologia de ponta em matéria de espionagem e comunicações (COMINT) de processamento automatizado para fins de espionagem de sistemas, de operadores de rede pública ou alugada de banda larga multilingues interceptados e a respectiva aplicabilidade na procura e selecção de COMINT, incluindo reconhecimento de voz, Vol. 2/5, in: STOA (Ed), o desenvolvimento de tecnologias de vigilância e risco de utilização abusiva de informações económicas (Outubro de 1999), PE 168.184

Campbell, Duncan, Inside Echelon, Heise Online, 24.7.2000, http://www.heise.de/tp/deutsch/special/ech/6928/1.html

Comité permanent de contrôle des service de renseignement, Rapport d'énquête sur la manière dont les services belges de renseignement reagissent face à l'éventualité d'un système americain "echelon" d'interception des communications téléphoniques et fax en Belgique, http://www.droit.fundp.ac.be/textes/echelonfr.pdf

Commission on the Roles and Capabilities of the US Intelligence Community, Preparing for the 21st Century: An Appraisal of U.S. Intelligence, (1996) http://www.gpo.gov/int/report.html

Deutscher Bundestag, Sekretariat des PKGr, Die Parlamentarische Kontrolle der Nachrichtendienste in Deutschland (2000)

Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet (Neuseeland), "Securing our Nation's Safety", Dezember 2000, http://www.dpmc.govt.nz/dess/securingoursafety/index.html

Dodel, Hans, Satellitenkommunikation, Hüthig Verlag (1999),

Elkjaer, Bo & Seeberg, Kenan, Echelon was my baby, Ekstra Bladet, 17.1.1999

Eser, Albin, Überhofer Michael, Huber Barbara (Eds), Korruptionsbekämpfung durch Strafrecht. Ein rechtsvergleichendes Gutachten zu den Bestechungsdelikten im Auftrag des Bayerischen Staatsministeriums der Justiz, edition iuscrim (1997)

Federation of American Scientists (FAS), Homepage, http://www.fas.org/

Fink, Manfred, Lauschziel Wirtschaft - Abhörgefahren und -techniken, Vorbeugung und Abwehr, Richard Boorberg Verlag, Stuttgart (1996)

Förster, Andreas, Maulwürfe in Nadelstreifen, Henschel Verlag (1997)

Frattini, Franco, Il ruolo dei servizi di informazione e sicurezza nel caso 'Echelon'. Relazione del comitato parlamentare per i servizi di informatione e sicurezza e per il segreto di stato. Approvata nella seduta del 29 novembre 2000, Trasmessa alle Presidenze il 19 dicembre 2000.

Freeh, Louis J, Statement for the Record, Hearing on Economic Espionage, House Judiciary Committee, Subcommittee on Crime, Washington DC, 9.5.1996

Freyer, Ulrich, Nachrichten-Übertragungstechnik, Hanser Verlag (2000)

Frowein, Jochen Abr., Peukert, Wolfgang, Europäische Menschenrechtskonvention[2], N. P. Engel Verlag (1996)

Frost, Mike in Fernsehinterview von NBC "60 Minutes" vom 27.2.2000, http://cryptome.org/echelon-60min.htm

Frost, Mike in Interview des australischen Senders Channel 9 vom 23.3.1999 http://www.geocities.com/CapitolHill/Senate/8789/sunday1.htm

Grant, Charles, Intimate relations. Can Britain play a leading role in European defence - and keep its special links to US intelligence? 4.2000, Centre for European Reform

Guisnel, Jean, L'espionnage n'est plus un secret, The Tocqueville Connection, 10.7.1998

Hager, Nicky, Secret Power. New Zealands´s Role in the international Spy Network, Craig Potton Publishing (1996)

Hager, Nicky, Exposing the global surveillance system, http://www.ncoic.com/echelon1.htm

Hoffmann, Wolfgang, Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V. (ASW), Aktuelle Anmerkungen zur Sicherheitslage der deutschen Wirtschaft, April 2001

Hummelt, Roman, Wirtschaftsspionage auf dem Datenhighway, Strategische Risiken und Spionageabwehr, Hanser Verlag (1997)

Intelligence and Security Committee (UK), Annual Report 1999-2000

Jacobs, Frnacis G, White, Robin C.A., The European Convention on Human Rights[2], Clarendon Press (1996)

Jauvert, Vincent, Espionnage - comment la France écoute le monde, Le Nouvel Observateur, 5.4.2001, Nr. 1900, S. 14 ff.

Kreye, Andrian, Aktenkrieger, Süddeutsche Zeitung, 29.3.2001

Kuppinger, Martin, Internet- und Intranetsicherheit, Microsoft Press Deutschland (1998), 60

Kurtz, George, McClure, Stuar, Scambray, Joel, Hacking exposed, Osborne/McGraw-Hill (2000)

Kyas, Othmar, Sicherheit im Internet, International Thomson Publishing (1998), 23

Landesamt für Verfassungsschutz Baden Württemberg, Wirtschaftsspionage, Die gewerbliche Wirtschaft im Visier fremder Nachrichtendienste, 10/1998

Legal Standards for the Intelligence Community in Conducting Electronic Surveillance, Bericht an den amerikanischen Congress Ende Februar 2000, http://www.fas.org/irp/nsa/standards.html

Leiberich, Otto, Vom diplomatischen Code zur Falltürfunktion - Hundert Jahre Kryptographie in Deutschland, Spektrum der Wissenschaft, Juni 1999

Lyle Robert, Radio Liberty/Radio fre Europe, 10.Februar 1999

National Security Councils (NSC), Homepage, http://www.whitehouse.gov/nsc

Madsen, Wayne in Fernsehinterview von NBC "60 Minutes" vom 27.2.2000, http://cryptome.org/echelon-60min.htm

Paecht, Arthur, Rapport d'information déposé en application de l'article 145 du règlement par la commission de la défense nationale et des forces armées, sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale, N° 2623 Assemblée nationale, enregisté à la Présidence de l'Assemblée nationale le 11 octobre 2000.

Paecht, Arthur, Rapport fait au nom de la Commission de la défense nationale et des forces armées sur la proposition de loi (N° 1497) de M. Paul Quilès et plusieurs de ses collègues tendant à la création d'une délégation parlementaire pour les affaires de renseignement, enregistré à la Présidence de l'assemblée nationale le 23. novembre 1999

Porter, Michael E., Competitive Strategy, Simon & Schuster (1998)

Richelson, Jeffrey T., Desperately seeking Signals, The Bulletin of the Atomic Scientists Vol. 56, No. 2/2000, pp. 47-51, http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html

Richelson, Jeffrey T., The U.S. Intelligence Community[4], Westview Press, 1999

Richelson, Jeffrey T., The National Security Agency Declassified, National Security Archive Electronic Breefing Book no. 24, George Washington University http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html

Richelson, Jeffrey T., Ball, Desmond, The Ties That Bind, Boston Unwin Hyman (1985)

Richter, Nicolas, Klettern für die Konkurrenz, Süddeutsche Zeitung, 13.9.2000

Rötzer, Florian, Die NSA geht wegen Echelon an die Öffentlichkeit, Heise Online, 26.02.2000, http://www.heise.de/bin/tp/issue/download.cgi?artikelnr=6633&rub_ordner=special

Schmidt-Eenboom, Erich, Streng Geheim, Museumsstiftung Post und Telekommunikation Heidelberg, (1999)

Schütze, Arno, Wirtschaftsspionage: Was macht eigentlich die Konkurrenz? P.M. Magazin, Die Moderne Welt des Wissens (1998)

Shane Scott, Bowman Tom, America's Fortress of Spies, Baltimore Sun, 3.12.1995

Simon Singh, Geheime Botschaften, Carl Hanser Verlag (1999)

Smith, Bradley F., The Ultra-Magic Deals and the Most Secret Special Relationship 1940-1946, Presidio (1993)

Sorti, Francesco, Dossier esclusivo. Caso Echelon. Parla Luigi Ramponi. Anche I politici sapevano, Il Mondo, 17.4.1998

State Department Foreign Press Center Briefing, Subject: Intelligence Gathering and Democracies: The Issue of Economic and Industrial Espionage, Washington DC, 7.3.2000

Süddeutsche Zeitung, Haftstrafe wegen Spionage für Russland, 30.5.2000

TPCC, Broschüre über das Advocacy Center, Oktober 1996

Thaller, Georg Erwin, Satelliten im Erdorbit. Nachrichten, Fernsehen und Telefonate aus dem Weltall, Franzis Verlag, München (1999)

Weißes Haus, Archive, http://govinfo.library.unt.edu/npr/library/direct/orders/tradepromotion.html

Wessely, Wolfgang, Das Fernmeldgeheimnis - ein unbekannts Grundrecht?, ÖJZ 1999, 491 ff

Wirtschaftswoche "Antennen gedreht", Nr. 46/9, November 1999

Wirtschaftswoche "Nicht gerade zimperlich", Nr. 43/16, Oktober 1992

Wobst, Reinhard, Abenteuer Kryptologie, Adison-Wesley (1998)

Woolsey, James, Why America Spies on its Allies, The Wall Street Journal Europe, 22.3.2000

Woolsey, *James,* Remarks at the Foreign Press Center, Transskript, 7.3.2000, http://cryptome.org/echelon-cia.htm

Wright, Steve, An appraisal of technologies for political control, STOA interim study (1998) PE 166.499/INT.ST.

Yernault, Dimitri, "Echelon" et l'Europe. La protection de la vie privée face à l'espionnage des communications, Journal des tribunaux, Droit Européen 2000, S. 187 ff.

BIBLIOGRAFIA COMPLEMENTAR

Air Intelligence Agency (AIA), Homepage, http://www.aia.af.mil

America´s Military Community, Homepage, http://www.military.com

Barr, Bob, Barr moves to expose "project ECHELON", 9.11.1999, http://www.house.gov/barr/p_110999.html

Bundesnachrichtendienst, Die Nachrichtendienste der Bundesrepublik Deutschland, 2000, http://www.bundesnachrichtendienst.de/diensteb.htm

Bundesamt für Verfassungsschutz, Spionage gefährdet die Sicherheit und die Interessen unseres Landes, 2001, http://www.verfassungsschutz.de/arbeitsfelder/spion/page.html

Campbell, Duncan, Somebody´s listening, They´ve got it taped, 12.8.1988, New Statesman, http://jya.com/echelon-dc.htm

Central Intelligence Agency (CIA), Homepage http://www.odci.gov/index.html

Commander Submarine Force, U.S. Atlantic Fleet - Surveillance and Intelligence, http://www.sublant.navy.mil/roles.htm#survintel

Collingwood, John, Carnivore Diagnostic Tool, 16.8.2000, FBI-Press-Room http://www.fbi.gov/

Ecole de Guerre Economique, Homepage, http://www.ege.eslsca.fr/

Federal Bureau of Investigation (FBI), Homepage, http://www.fbi.gov

Frankfurter Allgemeine Zeitung, Niederländische Wirtschaftsspionage, 19.4.2000

Frankfurter Allgemeine Zeitung, Wirtschaftsspionage, 3.2.2001

Freeh, J. Louis, Wirtschaftsspionage, 28.2.1996, Ansprache vor dem Senat, http://www.fbi.gov

General Dynamics, Seawolf Class, http://www.gdeb.com/programs/seawolf/

Göbel, Jürgen, Kommunikationstechnik, Grundlagen und Anwendungen, Hüthig (1999)

Goss, J. Porter, Additional views of chairman Porter J. Goss, 2000, http://www.aclu.org/echelonwatch/goss.htm

Gralla, Preston, So funktioniert das Internet: ein virtueller Streifzug durch das Internet, Markt und Technik (1999)

Hager, Nicky, Wie ich Echelon erforscht habe, 11.04.2000, http://www.heise.de/tp/deutsch/special/ech/6728/1.html

Hayden, Michael, Statement for the record of House Permanent Select Committee on intelligence, 12.04.2000 http://www.nsa.gov/releases/DIR_HPSCI_12APR.HTML

Innenministerium Brandenburg, Abwehr von Wirtschaftsspionage, 1999

Kerr, M. Donald, Congressional Statement on Carnivore Diagnostic Tool, 6.9.2000, http://www.fbi.gov

Kerr, M. Donald, Congressional Statement on Internet and data Interception Capabilities Developed by FBI, 24.7.2000, http://www.fbi.gov

Mass, Christian, Satelliten Signale anzapfen und auswerten, Satellitenspionage für Einsteiger, Franzis Verlag, Funkschau Telekom, Poing 1998

Mathiesen, Thomas, On Globalisation of Control: Towards an Integrated Surveillance System in Europe, Statewatch Publication, 11.1999

Matschke, Klaus Dieter, Geheimdienste im Auftrag des Wettbewerbs, 5.9.1998, Seku Media Verlag Ingelheim

National Security Agency (NSA), Homepage, http://www.nsa.gov/

Preneel, Bart, Relative Security of Cryptographic, 18.11.1998, Presentation on Conference on Problems of Global Security

Schönleber, Claus, Verschlüsselungsverfahren für PC-Daten, Franzis Verlag, Poing 1995

Secretary of State for the Home Department, Interception of communication in the UK, Juni 1999

Sénat et Chambre des représentants de Belgique, 14.2.2000, Rapport d´activités 1999 du Comité permanent de contrôle des services de renseignements et de sécurité

Tenet, George, Statement by Director of Central Intelligence before the House Permanent Select Committee on Intelligence, 12.4.2000, http://sun00781.dn.net/irp/congress/2000_hr/tenet.html

The United States Navy, Homepage, http://www.navy.mil

The US Army Intelligence and Security Command (INSCOM), Homepage http://www.vulcan.belvoir.army.mil

The White House, Defending America's Cyberspace, National Plan for Information systems protection Version 1.0, 2000, The White House 2000

Ulfkotte, Udo, Marktplatz der Diebe, Wie die Wirtschaftsspionage deutsche Unternehmen ausplündert und ruiniert. Bertelsmann Verlag, München (1999)

V. Bülow, Andreas, Im Namen des Staates. CIA, BND und die kriminellen Machenschaften der Geheimdienste. Piper Verlag, München (1998)

Verfassungsschutz Brandenburg, Abwehr von Wirtschaftsspionage - eine Aufgabe des Verfassungsschutzes, 1999, http://www.brandenburg.de/land/mi/vschutz/wispion.htm

Wall, Stephen, Ständiger Vertreter des Vereinigten Königreichs bei der Europäischen Union, Brief an Kommissar Liikanen zu GCHQ, 21.3.2000

Wojahn, Jörg, Die globalen High-Tech-Schnüffler, 1.9.2000, Der Standard

Anexo III.: Intercepção de comunicações para fins de acção penal: definições e comentários

1. Nota preliminar

No âmbito das actividades desenvolvidas em comissão, a tónica do debate sobre a admissibilidade, os efeitos e riscos dos sistemas de intercepção de informações a nível mundial incidiu reiteradamente nas medidas e actividades desenvolvidas na UE, as quais, embora se prendam com a questão da intercepção das comunicações, se integram, porém, no domínio da cooperação judicial em matéria penal.

Assim sendo, o relator não abordou essas medidas na parte principal do relatório, porquanto se impõe dissociar a questão da legitimidade da intercepção de comunicações para fins de acção penal da questão da intercepção de comunicações para objectivos dos serviços de informações. Embora, em ambos os casos, se trate de ingerências na vida privada cuja justificação por parte de quem as pratica assenta em razões de segurança *lato sensu*, os respectivos *modi operandi* e objectivos são de tal modo distintos que a regulamentação susceptível de se revelar pertinente e equilibrada para um sector não o é necessariamente para o outro. A pertinência e a proporcionalidade das medidas penais não deveriam, consequentemente, ser debatidas à luz da avaliação política das medidas implementadas pelos serviços de informações.

No intuito de pôr termo a eventuais mal-entendidos, impõe-se, no presente contexto, abordar as questões suscitadas e escalrecer determinados conceitos. Seguidamente, proceder-se-á, em primeiro lugar, à diferenciação entre a intercepção das comunicações para fins de acção penal e para fins dos serviços de segurança (2), referir-se-ão, em segundo lugar, tendo em conta as competências da UE, os actos jurídicos que contemplam a intercepção das comunicações para fins de acção penal (3), e indicar-se-ão, finalmente, ainda outros conceitos repetidamente enunciados em comissão a propósito de trabalhos transfronteiriços em matéria de intercepção das comunicações(4).

2. Distinção entre a intercepção de comunicações para fins de acção penal e a intercepção de comunicações por parte dos serviços de informações

A intercepção das comunicações levada a efeito pelos serviços de informações estrangeiros (caso do sistema „ECHELON“) não visa a vigilância de pessoas isoladas no interior do país, mas sim uma vigilância geral de actividades no estrangeiro com vista à obtenção prévia de informações relevantes em matéria de segurança. Essa actividade é exercida secretamente, não se pretendendo, mesmo a longo prazo, que aquela seja levada ao conhecimento da opinião pública. Alegando que apenas o sigilo é susceptível de garantir a segurança e que não estão em causa os cidadãos nacionais, permite-se, frequentemente, que os serviços secretos actuem numa zona indefinida do direito em que os regulamentos são imprecisos e os controlos deficientes.

Em contrapartida, a intercepção das comunicações para fins de acção penal visa impedir, em caso de suspeita, a consumação do acto pela pessoa em questão ou a penalização de delitos. As medidas de intercepção são implementadas pelas autoridades nacionais. Caso sejam necessárias medidas de intercepção no estrangeiro, são as mesmas levadas a cabo pelas autoridades do país em causa mediante a apresentação de carta rogatória por parte do país requerente. Uma vez que as acções são dirigidas contra os próprios cidadãos nacionais, existem, desde a queda dos

Estados policiais, regulamentos específicos e mecanismos de controlo eficazes que asseguram o equilíbrio dos interesses em causa. As medidas de intercepção só podem, por conseguinte, ser aplicadas num caso concreto em que se observe manifesta suspeita de delito, sendo em alguns Estados-Membros requerida autorização para o efeito, emanada de um juiz. Ainda que a intercepção se processe sigilosamente, tem a mesma por objectivo a utilização das provas no quadro de um processo penal público, pelo que as próprias autoridades têm interesse na obtenção legal das mesmas.

3. Actividades desenvolvidas na UE em matéria de intercepção de comunicações para fins de acção penal

3.1. Observações gerais

A introdução de um Título relativo à política externa e de segurança comum no Tratado da UE foi portadora da possibilidade de cooperação entre os serviços de informações a nível europeu. Todavia, não se verificou, até ao momento presente, qualquer recurso à mesma.
Quando existentes na UE, as regulamentações e os trabalhos em matéria de intercepção das comunicações respeitam exclusivamente à vertente penal, ou seja, à cooperação nos domínios da justiça e dos assuntos internos.

3.2. Limitação da competência da UE a regulamentações técnicas

A regulamentação da questão da admissibilidade de medidas de escuta inscreve-se exclusivamente, no momento presente, nas competências nacionais dos Estados-Membros. Em conformidade com o princípio da delegação limitada de poderes, a UE só pode intervir nos domínios em que os Tratados lhe confiram competências. O título VI do TUE "Disposições relativas à cooperação policial e judiciária em matéria penal" não prevê, no entanto, quaisquer competências nesse sentido. No domínio da cooperação policial (artigo 30º, nº1, do Tratado UE) só está prevista uma acção em comum no tocante aos aspectos operacionais, ou seja, aqueles relacionados com os moldes em que se processa a actividade policial. No domínio da cooperação judiciária, a alínea c) do artigo 31º prevê, em termos muito gerais, que a acção em comum tem por objectivo «assegurar a compatibilidade das normas aplicáveis nos Estados-Membros», mas apenas «na medida do necessário para melhorar a referida cooperação», ou seja, visa sobretudo regulamentações específicas de cooperação. Por último, a «aproximação das disposições de direito penal dos Estados-Membros», nos termos do disposto no último travessão do artigo 29º, limita-se ao estabelecimento de regras mínimas quanto aos elementos constitutivos das infracções penais (alínea e) do artigo 31º). Em suma, pode dizer-se que a competência para regulamentar a questão relativa às condições em que é admissível efectuar medidas de vigilância continua a estar reservada ao direito nacional. O relator não tem conhecimento de que algum Estado-Membro tenha alguma vez envidado esforços no sentido de alterar esta situação.
Por conseguinte, a cooperação entre os Estados-Membros ao abrigo dos Tratados da UE só poderá realizar-se no tocante à execução das medidas de vigilância consideradas admissíveis à luz do direito nacional, ou seja a um nível inferior. Nos casos em que a intercepção das telecomunicações é permitida pela ordem jurídica nacional, está previsto que o Estado-Membro interessado possa recorrer à ajuda dos outros Estados-Membros para fins de execução técnica das medidas de vigilância. Se a pretendida simplificação técnica, que certamente contribuirá para uma maior eficácia das escutas transfronteiras no âmbito do procedimento penal, sobretudo no que respeita à criminalidade organizada, deverá ou não ser considerada positiva, dependerá em larga medida da confiança de cada um no seu próprio Estado de direito. Em todo o caso, convém

salientar uma vez mais o seguinte: mesmo que a uniformização técnica permita simplificar, em termos técnicos, a intercepção de comunicações transfronteiras e atendendo a que não será certamente possível evitar abusos num ou noutro caso, tal não afecta de forma alguma as condições em que é admissível realizar escutas, já que esta questão é regulamentada pela legislação nacional.

3.3. Iniciativas e actos jurídicos no domínio da intercepção de telecomunicações

Em matéria de intercepção das telecomunicações, apenas foram adoptados, até à data, dois actos jurídicos comunitários: a resolução do Conselho, de 17 de Janeiro de 1995, relativa à intercepção legal de telecomunicações, cujo teor deveria ter-se estendido a países terceiros mediante a celebração de um memorando nesse sentido e relativamente à qual estava também prevista uma proposta de actualização (ambos foram preparados em documentos ENFOPOL), e a convenção relativa ao auxílio judiciário mútuo em matéria penal.

Resolução do Conselho de 17 de Janeiro de 1995 relativa à intercepção legal de telecomunicações[265]

Ao que parece, a resolução do Conselho, de 17 de Janeiro de 1995, relativa à intercepção legal de telecomunicações será fruto da cooperação entre os peritos no âmbito dos seminários ILET (ver ponto 4 *infra*) e corresponde, essencialmente, aos IUR (international user requirements) elaborados nesses mesmos seminários.

A resolução visa alcançar que em todos os Estados-Membros sejam criadas as condições técnicas necessárias para que, no exercício dos seus poderes no plano nacional, as autoridades competentes possam efectivamente ter acesso aos dados, ou seja, que possam exercer, na prática, as competências que lhe foram atribuídas ao abrigo do direito nacional.

Para este efeito, a resolução inclui um anexo que assume «requisitos» bastante pormenorizados dos Estados-Membros, relativamente aos quais o Conselho «toma nota» de que «representam uma síntese importante das necessidades das autoridades competentes na execução técnica da intercepção legal, designadamente nos modernos sistemas de telecomunicações». Estes requisitos incluem, por exemplo, o acesso, em tempo real, a dados associados à chamada ou a possibilidade de os operadores de rede transmitirem as comunicações interceptadas ao serviço de controlo. Na sua resolução, o Conselho considera que «na definição e execução de medidas [...] devem ser tidos em conta os requisitos» e insta os Estados-Membros e os ministros responsáveis «a cooperar [...] na aplicação dos requisitos relativos aos operadores de rede e aos prestadores de serviços».

Neste contexto, cumpre assinalar que o tipo de acto jurídico escolhido, isto é, a resolução, não assume qualquer carácter vinculativo, ou seja, dela não resultam direitos nem obrigações para os Estados-Membros. A agitação gerada em torno desta resolução e dos documentos associados à mesma não se deveu tanto ao seu conteúdo, mas antes às condições em que foram elaborados, sobretudo falta de transparência.

Memorando de Entendimento

No subsequente Memorando de Entendimento[266] convidavam-se os países terceiros a transpor os requisitos técnicos contidos na resolução do Conselho de 17 de Janeiro de 1995. Além disso,

[265] JO C 329 de 4.11.1996.

pretendia-se que as inovações técnicas e os novos requisitos daí resultantes fossem comunicados ao FBI e ao Secretariado do Conselho. A razão desta medida prendia-se com o facto de, muitas vezes, a produção das telecomunicações estar nas mãos de empresas multinacionais, tornando assim imprescindível a cooperação com as autoridades competentes dos países terceiros onde esses centros de produção se encontram sediados.

O memorando foi assinado, em 23 de Novembro de 1995, pelos Estados-Membros da UE e por um único país terceiro, a Noruega. Os Governos dos Estados Unidos da América, do Canadá e da Austrália apenas informaram, por escrito, que iriam providenciar no sentido da transposição dos requisitos para a ordem interna dos seus países[267].

Lamentavelmente, até à data, o texto ainda não foi publicado, tendo dado azo a inúmeras especulações na imprensa.

O projecto de resolução do Conselho relativa à intercepção legal de telecomunicações no que respeita às novas tecnologias

Como o relator já teve oportunidade de referir no seu relatório de 23 de Abril de 1999[268], o «projecto de resolução do Conselho relativa à intercepção legal de telecomunicações no que respeita às novas tecnologias» constitui uma «actualização» da resolução de 1995. A nova resolução do Conselho pretende esclarecer que os "requisitos" da resolução do Conselho de 1995, aos quais são acrescentados alguns novos, também se aplicam às novas tecnologias, por exemplo, as comunicações por satélite e a Internet e que os termos técnicos utilizados actualmente devem ser entendidos por analogia no sector das novas tecnologias (por exemplo, o número de telefone é equivalente ao código de identificação para acesso à Internet). Apesar de o Parlamento Europeu ter aprovado o projecto[269], o Conselho decidiu congelá-lo provisoriamente.

---

[266] Sobre o conteúdo, cf. resposta escrita do Ministro dos Assuntos Internos austríaco, Karl Schlögel, em 6.12.1998, à pergunta parlamentar do deputado Van der Bellen; 4739/AB XX. GP. http://www.parlinkom.gv.at/pd/pm/XX/AB/texte/AB04739_.html.

[267] Declaração expressa pelo Ministro dos Assuntos Internos Austríaco, Karl Schlögel (cf. nota de rodapé anterior) ; um tanto imprecisa foi a resposta formulada por Michiel Patijn, na sua qualidade de Presidente do Conselho em exercício, à pergunta oral de Jonas Sjödstaedt H-0330/97, em 14.5.1997, no decurso do período de perguntas, referindo que „estes requisitos“ (reporta-se o mesmo aos requisitos enunciados na Resolução do Conselho de 17.1.1995) foram co-subscritos pelos Estados Unidos, pelo Canadá, pela Austrália e pela Noruega.

[268] A4-0243/99

[269] Resolução legislativa que contém o parecer do Parlamento Europeu, de 7 de Maio de 1999, JO C 279, p. 498, de 1 de Outubro de 1999.

A Convenção relativa ao auxílio judiciário mútuo em matéria penal[270]

O segundo acto jurídico é a convenção relativa ao auxílio judiciário mútuo em matéria penal. Os artigos 17º e seguintes da Convenção estabelecem as condições em que serão executados os pedidos de auxílio judiciário mútuo em matéria penal que envolvam a intercepção de telecomunicações. Sem querer entrar nos detalhes da regulamentação, fica apenas o apontamento de que a Convenção não limita de forma alguma os direitos das pessoas sujeitas a intercepção, uma vez que o Estado-Membro onde a pessoa em causa se encontra pode recusar-se a prestar auxílio judiciário, sempre que à luz da sua legislação nacional tal auxílio não seja admissível.

4. Actividades de carácter transnacional no domínio da intercepção de telecomunicações: definições e comentários

Paralelamente aos vários actos jurídicos da UE, os diferentes grupos de trabalho constituídos no domínio da política de segurança têm suscitado reiteradamente alguns equívocos, razão pela qual nos propomos, seguidamente, esclarecer alguns dos conceitos utilizados.

ILETS (International Law Enforcement Telecommunications Seminar)

Os seminários ILET surgiram na sequência de uma iniciativa do FBI. Em 1993, o FBI convidou as autoridades responsáveis pela aplicação da lei e os serviços de informações de países amigos a assistir a uma conferência subordinada ao tema da intercepção de telecomunicações, em Quantico. Nessa conferência participaram grande parte dos actuais Estados-Membros da UE, bem como a Austrália e o Canadá[271]. Desde então, têm-se realizado encontros periódicos para debater os requisitos necessários a uma vigilância eficaz das comunicações internacionais.

Por ocasião de uma reunião realizada em Bona, em 1994, os membros do ILETS aprovaram um documento que estabelecia orientações políticas e cujo anexo incluía uma lista de "international user requirements" (IUR 1.0 ou IUR 95). Esta lista continha os requisitos que deveriam ser impostos aos vários operadores de telecomunicações, a fim de simplificar as operações de intercepção. Embora não oficialmente, estas IUR 1.0 serviram de base à resolução do Conselho, de 17 de Janeiro de 1995, relativa à intercepção legal das telecomunicações. Posteriormente, realizaram-se ainda outras reuniões de peritos para debater as IUR e a sua possível aplicação e adaptação aos modernos sistemas de telecomunicações.

Grupo TREVI

Antes da entrada em vigor do Tratado de Maastricht (que, com o TUE, veio introduzir as disposições relativas à cooperação no domínio da justiça e dos assuntos internos), era no quadro do grupo TREVI que os ministros da Justiça e dos Assuntos Internos dos Estados-Membros da Comunidade Europeia debatiam as questões de segurança interna. Entretanto, o grupo TREVI deixou de estar activo, já que os temas debatidos no seu seio transitaram para os grupos de trabalho específicos do Conselho (GTC).

---

[270] Acto do Conselho, de 29 de Maio de 2000, que estabelece, em conformidade com o artigo 34º do Tratado da União Europeia, a Convenção relativa ao auxílio judiciário mútuo em matéria penal entre os Estados-Membros da União Europeia; JO C 197 de 12 de Julho de 2000, p. 1.

[271] Sobre o conteúdo, cf. resposta escrita do Ministro dos Assuntos Internos austríaco, Karl Schlögel, à pergunta parlamentar do deputado Van der Bellen ; 4014/AB XX. GP. http://www.parlinkom.gv.at/pd/pm/XX/AB/texte/AB04014_.html.

Para efeitos da presente análise, importa sobretudo referir dois GTC: o GTC "Auxílio judiciário mútuo em matéria penal" que, no âmbito da cooperação no domínio da justiça e dos assuntos internos, estudou a convenção relativa ao auxílio judiciário mútuo em matéria penal e o grupo de trabalho do Conselho "Cooperação policial" que tratou das questões relacionadas com a intercepção legal das telecomunicações, incluindo a intercepção dos novos sistemas de comunicação (telemóveis, Internet, correio electrónico). Este último também tratou da aproximação das legislações no que respeita aos requisitos impostos pelos serviços de controlo legalmente autorizados aos operadores de rede e prestadores de serviços.

"ENFOPOL"

Contrariamente ao que muitos autores pensam, o "ENFOPOL" não é um grupo de trabalho ou uma organização, mas sim uma abreviatura que designa os documentos de trabalho em matéria de acções penais e policiais, inclusive da autoria do GTC "Cooperação policial"[272]. O ENFOPOL não figura no título dos respectivos documentos, mas estes são classificados segundo o mesmo.

[272] Cf. resposta oral do Ministro dos Assuntos Internos austríaco, Karl Schlögel, à pergunta parlamentar do deputado Van der Bellen; 4739/AB XX. GP http://www.parlinkom.gv.at/pd/pm/XX/AB/texte/040/AB04014_.html, bem como o relatório Campbell: ECHELON a mão invisível por detrás do ENFOPOL 98, http://heise.de/tp/deutsch/special/enfo/6396/1.html.

Anexo IV.:

SINOPSE

DOS

SERVIÇOS DE INFORMAÇÕES E DOS ÓRGÃOS DE FISCALIZAÇÃO PARLAMENTAR

DOS

ESTADOS-MEMBROS E DOS ESTADOS UKUSA

País	Serviço de informações	Base jurídica	Missões	SIGINT Satélites	Autoridade de fiscalização	Base jurídica	Competências
AUSTRIA	***Heeresnachrichtenamt (HnA)*** ***Abwehramt (AbwA)*** serviço de informações militares sob tutela do Ministro da Defesa	*§ 20 Abs 3 Militärbefugnisgesetz (MBG) BGBl I 86/2000'*	serviço de informações militares; protecção movida contra actividades estrangeiras que põem em perigo a segurança nacional		subcomissão parlamentar: *Ständiger Unter-ausschuss des Landesverteidigungs-ausschusses zur Überprüfung von nachrichten-dienstlichen Maß-nahmen zur Siche-rung der militärischen Landesverteidigung (14 membros, encontrando-se representados todos os partidos com assento parlamentar)* *1 Responsável pela observância do direito*	*Art 52a Bundesverfassungs-gesetz (B-VG);* *§§ 32b ff GeschäftsordnungsG 1975*	autorizados a obter qualquer informação relevante do ministro competente e a examinar os documentos relevantes, sob condição de não comprometer a segurança nacional ou das pessoas

AUSTRIA	**Sondereinheit für Observation (SEO)** serviço de informações civis sob tutela do Ministro do Interior	*§§ 6, 14, 15 Sicherheitspolizeigesetz (SPG, BGBl 566/1991 idgF);* *Sondereinheiten-Verordnung* (BGBl II 207/1998)	defesa da segurança pública; contra-espionagem a nível nacional; defesa dos princípios garantidos pela Constituição; acção contra os movimentos extremistas, o terrorismo e o crime organizado		subcomissão parlamentar: *ständiger Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit (14 membros, encontrando-se representados todos os partidos com assento parlamentar)* *1 Responsável pela observância do direito*		

País	Serviço de informações	Base jurídica	Missões	SIGINT Satélites	Autoridade de fiscalização	Base jurídica	Competências
BÉLGICA	**Service Général du Renseignement et de la Sécurité des Forces armées(SGR)** serviço de informações e de segurança militares sob tutela do Ministro da Defesa	*Loi du 30 novembre 1998 organique des services de renseignement et de sécurité*	recolha de informações relevantes do ponto de vista político, militar, económico e tecnológico/cientifico, salvaguarda da segurança de instalações militares e de pessoal militar		*Comité permanent de contrôle des services de renseignements et de sécurité (Comité permanent R),* três membros nomeados pelo Senado, que não têm direito de exercer um mandato electivo ou outra actividade que possa comprometer a sua independência; *Service d'enquêtes des services de renseignements* subordinado ao Comité permanente R, os membros são nomeados pelo Comité R	*Loi du 18 juillet 1991 (VI) organique du contrôle des services de police et de renseignements*	autorizado a inspeccionar regulamentações e documentos internos dos departamentos; autorizado a interrogar os serviços; a recusa de cooperar implica uma sanção de até um ano; a recusa de fornecer informações é admissível em processos pendentes; no caso de recusa por risco de pôr em perigo uma pessoa singular, o presidente do Comité permanente R decide da admissibilidade
BÉLGICA	**Sûreté de l'Etat (VS)** Serviço de informações e de segurança civis sob tutela do Ministro da Justiça	*Loi du 30 novembre 1998 organique des services de renseignement et de sécurité*	Salvaguarda da segurança interna e externa, contra-espionagem, observação do extremismo político				

País	Serviço de informações	Base jurídica	Missões	SIGINT Satélites	Autoridade de fiscalização	Base jurídica	Competências
DINAMARCA	Forsvarets Efterretningstjeneste (FE(T)) 'Serviço secreto da defesa' sob tutela do Ministério da Defesa	*Lov om forsvarets formål, opgaver og organisation m.v.* *Lov 909 af 8/12/1993* ['lei-quadro', onde não é mencionado o FE(T)] [existirá num futuro próximo nova lei para FET & PET]	recolha e avaliação de informação secreta relevante para a defesa sobre a CEI, a Europa central e oriental nos domínios militar, político, económico e tecnológico/cientifico, SIGINT; decifração pessoal & orçamento: informação classificada	sim	2 comissões de controlo: *Kontroludvalget vedrørende Politiets og Forsvarets efterretningstjenester (Wamberg-udvalget) (composta por funcionários públicos e advogados)* nomeada pelo Ministro da Justiça *Udvalget vedrørende efterretningstjenestern* (comissão parlamentar composta por) cinco membros do *Folketing*	não existe base jurídica específica *Lov om etablering af et udvalg om forsvarets og politiets efterretningstjenester* lov 378 af 6/7/88	direito de acesso a informações sobre as actividades do Serviço de informações
DINAMARCA	Politiets Efterretningstjeneste (PET) 'Serviço secreto da polícia' sob tutela do Ministério da Justiça	não existe legislação específica [existirá num futuro próximo nova lei para FET & PET]	contra-espionagem, prevenção de e acção contra actividades que possam pôr em perigo a segurança da Dinamarca: espionagem, terrorismo, etc.; segurança do governo e da família real pessoal: cerca de 370 (1998) orçamento: informação classificada.				

País	Serviço de informações	Base jurídica	Missões	SIGINT Satélites	Autoridade de fiscalização	Base jurídica	Competências
FINLÂNDIA	**Pääesikunnan tiedusteluosasto** 'Serviço de informações militares das forças de defesa da Finlândia sob tutela do Ministério da Defesa	*Laki puolustusvoimista* N:o 402/1974 2§ 'Lei das forças de defesa' (não menciona a divisão de Informações)	vigilância do espaço terrestre, marítimo e aéreo do País em cooperação com outras autoridades de supervisão, garantia da integridade territorial do País	sim	não existe órgão de fiscalização específico Ministério da Defesa apresenta um relatório anual sobre as intercepções ao Ombudsman parlamentar	*Poliisilaki 493/1995 §33* 'Polícia Act' *Laki pakkokeinolain muuttamisesta N:o 402/1995 §15* 'Lei das Medidas Coercivas' [no que respeita à missão do Ombudsman parlamentar de controlar as intercepções reportadas pelo ministério]	'Controlo do controlo' no que se refere aos relatórios de intercepção do ministério, investigação de queixas dos cidadãos

FINLÂNDIA	**Suojelupoliisi (SUPO)** 'Polícia de Segurança Finlandesa' sob tutela do Ministério do Interior	*Laki poliisin hallinnosta N:o 110/1992, 1§, 10§ 1. ja 2. momentti* *Asetus poliisin hallinnosta N:o 158/1996 8§* *Laki poliisin henkilörekistereistä N:o 509/1995 23§, 9§* 'Lei e Decreto sobre a Administração da Polícia', 'Lei relativa ao tratamento pela polícia de dados pessoais'	contra-espionagem; evitar actividades que poderiam pôr em perigo a segurança interna da Finlândia e as relações internacionais, agir contra o terrorismo, fazer trabalho de prevenção para a segurança		não existe órgão de fiscalização específico; a polícia tem que informar de todos os casos de intercepção o Ministério do Interior, que apresenta um relatório anual ao Ombudsman parlamentar		
FINLÂNDIA	**Tullin tiedusteluyksikkö** 'Secção de Informação das Alfândegas Finlandesas' sob a tutela do Ministério das Finanças	*Tullilaki N:o 1466/1994* 'Lei das Alfândegas'	recolha e análise de dados para evitar e detectar infracções aduaneiras, e fornecimento das mesmas às unidades respectivas para seguimento		não existe órgão de fiscalização específico; as alfândegas devem reportar todos os casos de intercepção ao Conselho Nacional das Alfândegas e ao Ministério do Interior, que apresenta um relatório anual ao Ombudsman parlamentar		

País	Serviço de informações	Base jurídica	Missões	SIGINT Satélites	Autoridade de fiscalização	Base jurídica	Competências
FRANÇA	*Direction générale de la sécurité extérieure (DGSE)* sob a tutela do Ministério da Defesa	*Décret n°82-306 du 2 avril 1982*	recolha de informações relevantes do ponto de vista político, militar, económico e tecnológico/cientifico pesquisa e uso de informações de interesse para a segurança da França; Contra-espionagem (fora do território nacional) pessoal 4100; FF 1.7 milhões	sim	Actualmente não existe um órgão parlamentar de fiscalização específico (em discussão; a Comissão de Defesa da Assembleia Nacional propôs, por duas vezes, que se estabeleça uma comissão de vigilância; nº1951 e 2270) Commission nationale de contrôle desenvolvimento interceptions de sécurité (controlo exclusivo de medidas de intercepção de cabos) Constituída, *inter alia*, por 1 deputado e 1 senador		

FRANÇA	**Direction du renseignement militaire (DRM)** sob a tutela do Ministério da Defesa	*Décret n°92-523 du 16 juin 1992*	Fornece as informações militares necessárias às forças armadas; pessoal 1700, FF 90 milhões, segurança militar interna, apoia o exército;				
FRANÇA	**Direction de la surveillance du territoire (DST)** Serviço de informações civis sob a tutela do Ministro do Interior	*Décret n°82-1100 du 22 décembre 1982*	Contra-espionagem em território francês pessoal: 1500 ; protecção da segurança pública, contra-espionagem a nível nacional				

País	Serviço de informações	Base jurídica	Missões	SIGINT Satélites	Autoridade de fiscalização	Base jurídica	Competências
ALEMANHA	**Bundesnachrichtendienst (BND)** sob tutela do Chanceler Federal	*Gesetz über den Bundesnachrichten-dienst (BNDG),* BGBl 1990 I 2954 idgF	recolha e análise de informações sobre o estrangeiro relevantes para a segurança e a política externa	sim	*Parlamentarisches Kontrollgremium (PKGR*) órgão de fiscalização parlamentar dos 3 serviços secretos, composto por 9 deputados do *Bundestag* *G 10-Kommission* Órgão independente; pode ser composta por deputados, mas não necessariamente; 4 membros nomeados pelo PKGR;	*Gesetz über die Kontrolle nachrichten-dienstlicher Tätigkeit des Bundes (PKGrG)vom 17. Juni 1999 BGBl I 1334 idgF* *§ 5 Abs 5, § 9 Abs 2-4 Gesetz zu Art 10 Grundgesetz (G10-G) vom 13. August 1968, BGBl I 949 idgF (Gesetz zur Beschränkung desenvolvimento Brief -, Post – und Fernmeldegeheim-nisses)*	autorizado a examinar documentos e actas dos serviços, a ouvir o pessoal dos serviços e a visitar os serviços; o exercício desses direitos pode ser recusada por motivos de força maior Missões de controlo no sector da vigilância de correio e telecomunicações, autorização de medidas de intercepção. Informação mensal por parte do Ministro do Interior antes da execução da medida em causa
ALEMANHA	**Bundesamt für Verfassungsschutz (BfV)** sob a tutela do Ministro do Interior	*Gesetz über die Zusammenarbeit des Bundes und der Länder in Angele-genheiten des Ver-fassungsschutzes und über das Bundsamt für den Verfassungs-schutz* (BVerfSchG, BGBl 1090 I 2954)	recolha e análise de informações sobre actividades que põem em perigo a segurança e actividades dos Serviços de informações genéricos no interior da Alemanha				
ALEMANHA	**Militärischer Abschirmdient (MAD)** sob a tutela do Ministro da Defesa	*Gesetz über den militätischen Ab-schirmdienst (MADG*) BGBl 1990 I 2954 idgF	defender a eficácia do exército, salvaguardar a segurança de instalações militares e do pessoal militar				

País	Serviço de informações	Base jurídica	Missões	SIGINT Satélites	Autoridade de fiscalização	Base jurídica	Competências
GRÉCIA	*Ethniki Ypiresia Pliroforion (EYP)* 'Serviço Nacional de informações' sob tutela do KYSEA (Conselho de Segurança Nacional: Primeiro Ministro + Ministros dos Negócios Estrangeiros e da Defesa Nacional)	Lei 1645/86 *Nacional Serviço de informações (Ethniki Ypiresia Pliroforion)*	• recolha e processamento de informação pertinente para a segurança nacional (informações sobre o crime organizado, o terrorismo, informação militar, económica e política); divulgação às autoridades competentes • contra-espionagem; observação das actividades de agentes de serviços de informações estrangeiros que actuam contra o país.		Comissão especial parlamentar para a protecção da privacidade das comunicações. Inexistência de um direito especial de fiscalização. Composição: 1 vice-presidente do Parlamento, 1 deputado por grupo político, 1 especialista em questões de comunicação.	Lei 2225/1994 *Aporrito epikoinonion* (Segredo das comunicações)	*[Não recebemos informação]*
					Instituição para a protecção de dados pessoais	Lei 2472/1997 *Prostasia apo tin epeksergasia dedomenon prosopikou charaktira* (Protecção dos dados pessoais)	

País	Serviço de informações	Base jurídica	Missões	SIGINT Satélites	Autoridade de fiscalização	Base jurídica	Competências
IRLANDA	**Garda Síochána** (polícia nacional) cobre assuntos de segurança nacional A polícia encontra-se sob a tutela do Ministro de Justiça	Autoridade de intercepção baseada no *Interception of Postal Packets e Telecommunications Messages (Regulation) Act 1993*	Intercepção autorizada no interesse da segurança do Estado		*Joint Committee on Justice, Equality e Women's Rights* é responsável pelo âmbito geral dos direitos cívicos		
IRLANDA	Intelligence Staff		Interesses de segurança nacional da Irlanda (sobretudo IRA), segurança das forças armadas nacionais, desenvolvimento tecnológico das forças armadas estrangeiras		Inexistência de um órgão especial de fiscalização		

País	Serviço de informações	Base jurídica	Missões	SIGINT Satélites	Autoridade de fiscalização	Base jurídica	Competências
ITÁLIA	**Servizio per le informazioni e la sicurezza militare (SISMI)** **Servizio Informazione Operative Segrete (SIOS)** sob tutela do Ministro da Defesa; nomeia o director do Serviço e os altos funcionários públicos	*L. 24 ottobre 1977, n. 801, art. 4 Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato*	Missões de informação e segurança para a defesa, a nível militar, da independência e integridade do Estado; contra-espionagem, recolha de informações estrangeiras sobre assuntos políticos, militares, económicos e tecnológico/ científicos	sim	Comissão parlamentar (4 deputados + 4 senadores) O Governo apresenta ao Parlamento um relatório semestral sobre a política de informação e de segurança	L. 24 ottobre 1977, n. 801, art. 11 Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato	Fiscaliza a aplicação da lei
ITÁLIA	**Servizio per le informazioni e la sicurezza democratica (SISDE)** **Direzione investigazioni anti-mafia (DIA)** sob tutela do Ministro do Interior; nomeia o director do Serviço e os altos funcionários públicos	*L. 24 ottobre 1977, n. 801, art. 6 Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato*	Missões de informação e segurança para a defesa do Estado democrático e das instituições informações sobre actividades que põem em perigo a segurança interna, contra-espionagem, acção contra o terrorismo e o crime organizado				

País	Serviço de informações	Base jurídica	Missões	SIGINT Satélites	Autoridade de fiscalização	Base jurídica	Competências
LUXEM-BURGO	**Service de renseignement** Serviço nacional de informações e segurança sob tutela do Ministro de Estado (= primeiro ministro)	*Loi concernant la protection des secrets intéressant la sécurité extérieure de l'État* du 30 juillet 1960	Assegurar a protecção dos segredos visados no art. 120 acties do Código penal* e obter a informação necessária para defender a segurança externa do Grão-Ducado e dos Estados com quem o mesmo está unido por um acordo regional de defesa conjunta * 'infracções contra o Grão-Ducado do Luxemburgo'		não existe controlo parlamentar (a vigilância de comunicações com a finalidade de investigar infracções contra a segurança do Estado exige o acordo de uma comissão que engloba o presidente do Supremo Tribunal de Justiça, o presidente do Comité do Contencioso do Conselho de Estado e o presidente do Tribunal de Contas)	*(Loi du 26 novembre 1982 portant introduction au code d'instruction criminelle des articles 88-1, 88-2, 88-3 et 88-4)*	

País	Serviço de informações	Base jurídica	Missões	SIGINT Satélites	Autoridade de fiscalização	Base jurídica	Competências
PAÍSES BAIXOS	**Militaire Inlichtingendienst (MID** ou, mais recentemente, MIVD) sob a tutela do Ministério da Defesa	*Wet op de inlichtingen- en veiligheidsdiensten Loi 635/87 du 3 décembre 1987, dernier amendement loi 194/1999 du 19 avril 1999.* [Nova lei em discussão]	serviço de informações militar; recolha de informações sobre forças armadas estrangeiras		*Tweede-Kamercommissie voor de Inlichtingen- en veiligheidsdiensten* 'Comissão da Segunda Câmara sobre Serviços de Informação e Segurança Interna Comissão parlamentar (4 membros: presidentes dos quatro maiores partidos)	*17. Reglement van orde van de Tweede Kamer der Staten-General, Art. 22* Regulamento da Segunda Câmara dos Países Baixos, Art. 22: Comissão para os serviços de Informação e de Segurança	responsável pela coordenação e controlo de todos os serviços de informação e segurança, incluindo do serviço de segurança militar
PAÍSES BAIXOS	**Binnenlandse Veiligheidsdienst** (**BVD** ou, mais recentemente, AIVD) sob a tutela do Ministério do Interior		serviço de segurança interna, acção contra o extremismo de direita e de esquerda, contra-espionagem				

País	Serviço de informações	Base jurídica	Missões	SIGINT Satélites	Autoridade de fiscalização	Base jurídica	Competências
PORTUGAL	**Serviço de Informações Estratégicas de Defesa e Militares (SIEDM)** sob a tutela do Ministro da Defesa	Lei 30/84 de 5 de Setembro de 1984, alterada pela Lei 4/95 de 21 de Fevereiro de 1995, Lei 15/96 de 30 de Abril de 1996 e Lei 75-A/97 de 22 de Julho de 1997	Serviço de informações para garantir a segurança externa; informações estratégicas para as questões políticas, militares e económicas		*Conselho de Fiscalização dos Serviços de Informações (CFSI).* é composto por três cidadãos eleitos pela *Assembleia da República* por um período de quatro anos. a *Assembleia República* pode convocar os directores do SIS e do SIEDM para serem ouvidos em comissão parlamentar	A constituição do órgão de fiscalização está estabelecida nas Leis mencionadas	Controla as actividades dos dois serviços e assegura que não haja violações da Constituição nem da lei e, em especial, dos direitos cívicos e das garantias fundamentais dos cidadãos portugueses
PORTUGAL	**Serviço de Informações de Segurança (SIS)** sob a tutela do Ministro do Interior		Serviço de informações para garantir a segurança interna; protecção da constituição (sem competências executivas); recolha e avaliação de informações sobre actividades criminosas e contra o Estado				

País	Serviço de informações	Base jurídica	Missões	SIGINT Satélites	Autoridade de fiscalização	Base jurídica	Competências
ESPANHA	**Centro Superior de Información de la Defensa (CESID)** sob tutela do Ministério da Defesa	*R.D. 2632/1985 de 27.12.1985 (BOE 20.01.1986) Estructura interna y relaciones del Centro Superior de la Defensa;* modificada por *R.D. 266/1996 de 16.02.1996 Modif. de la estructura organica del CESID*	Serviço de informações estrangeiro e interno; recolha de informação política, económica tecnológica/cientifica e militar; vigilância dos serviços de informa-ções estrangeiros, contra-espionagem dentro e fora de Espanha	sim	não existe um órgão de fiscalização específico; controlo parlamentar geral, enquanto órgãos governamentais, pelas comissões parlamentares idem idem		
ESPANHA	**Dirección General de la Guardia Civil (GC)** sob tutela do Ministério da Defesa e do Ministério do Interior	*L.Org. 2/1986 de 13.03.1986 (BOE 14.03.1986) de Fuerzas y cuerpos de seguridad*	autoridade policial paramilitar central espanhola, que inclui o Serviço de informações da polícia; luta contra a proliferação do crime organizado no território espanhol				
ESPANHA	**Dirección General de la Policia** sob tutela do Ministério do Interior		Autoridade policial central espanhola que inclui o Serviço de informações da polícia; informações internas e estrangei-ras, estruturas terroristas e fundamentalismo islâmico no Médio Oriente e no Norte de África				

País	Serviço de informações	Base jurídica	Missões	SIGINT Satélites	Autoridade de fiscalização	Base jurídica	Competências
SUÉCIA	*Säkerhetspolisen* (SÄPO) Serviço de Segurança e de informações civis sob a tutela do Ministro da Justiça	*Polislag (1984:387)* *Förordning (1989:773) med instruktion för Rikspolisstyrelsen* 'Lei da Polícia (1984:387) Decreto (1989:773) e Directiva para o Conselho Nacional da Polícia'	Responsabilidades: - Controlo da Segurança - Contra-espionagem - Contra-terrorismo - Protecção da Constituição Pessoal em 1999 cerca de 800. Orçamento em 1995 SEK 475 milhões (EUR 55.7 milhões)		Conselho do NPB, composto por cinco deputados, dois membros do pessoal e o Comissário Nacional da Polícia. *Registernämnd*, composto no máximo por oito membros. Actualmente há dois 'magistrados', dois deputados, um advogado e um perito. Ambos os órgãos dependem do governo	*Förordning (1989:773) med instruktion för Rikspolisstyrelsen* 'Decreto (1989:773) e Directiva para o Conselho Nacional da Polícia *Förordning (1996:730) med instruktion för Registernämnden* 'Decreto (1986:730) e Directiva para o Registernämnden'	O NPB deve garantir que : - o trabalho da polícia é conduzido em conformidade com as prioridades e directrizes para a acção da polícia estabelecidas pelo Parlamento e pelo Governo - o trabalho da polícia é conduzido com eficiência e respeita a lei - a administração no seio dos serviços de polícia funciona bem. Contudo, o controlo da polícia é exercido por vários outros órgãos como o Ombudsman Parlamentar, o Chanceler da Justiça, os auditores do Parlamento e o Gabinete de Auditoria Nacional Sueco.

País	Serviço de informações	Base jurídica	Missões	SIGINT Satélites	Autoridade de fiscalização	Base jurídica	Competências
SUÉCIA	**Militära Underrättelse och Säkerhetstjänsten (MUST)** 'Direcção do Serviço de informações militares e de segurança; Junto do quartel-general militar sueco. Serviço de segurança e de informações militares sob a tutela do Ministro da Defesa	*Act 2000:130 e Ordinance 2000:131 sobre o Serviço de informações militares*	serviço de informações e de segurança militares; recolha e avaliação de informações secretas militares ou políticas; contra-espionagem; acção contra a subversão, a sabotagem e a rebelião; protecção das forças armadas e da indústria de armamento		*Försvarets underrättelsenämnd* A Comissão de Fiscalização do Serviço de Informações Militares, composta, em parte, por deputados ao Parlamento	*Ordinance 1988:552 with Directive for Försvarets underrättelsenämnd /* 'Comissão de Informações de Defesa'	contra-espionagem, segurança de protecção, segurança das comunicações, segurança dos computadores
SUECIA	**Försvarets Radioanstalt (FRA) Unidade Especial Independente (estação de radiodifusão)**		serviço de informações militares e não militares, decifração de comunicados; vigilância por radar	sim			

País	Serviço de informações	Base jurídica	Missões	SIGINT Satélites	Autoridade de fiscalização	Base jurídica	Competências
REINO UNIDO	**Goverment Communications Headquarters (GCHQ)** sob tutela do Ministro dos Negócios Estrangeiros	*Intelligence Services Act 1994*	contra-espionagem/ contra-espionagem no estrangeiro, SIGINT no âmbito político, económico, tecnológico/científico e militar	sim	*The Security Service Commissioner* é nomeado pelo Primeiro-Ministro, juiz em exercício ou jubilado de um tribunal superior	*Intelligence Services Act 1994. §8*	Todos os membros do Serviço de informações, do GCHQ e todos os funcionários do departamento da Secretaria de Estado devem revelar ou fornecer ao Comissário qualquer documento .. que este requeira …
					The Investigatory Powers Tribunal	*Intelligence Services Act 1994. §9*	Investigar queixas sobre o Serviço de informações ou o GCHQ
	Secret Intelligence Service (SIS) = MI6 sob tutela do Ministro dos Negócios Estrangeiros	*Intelligence Services Act 1994*	recolha de informação sobre actividades de informação e acontecimentos políticos no estrangeiro		*The Intelligence and Security Committee (ISC)* A comissão é composta por 9 membros (Câmara dos Comuns + Câmara dos Lordes, não sendo nenhum Ministro da Coroa); nomeação pelo Primeiro-Ministro	*Intelligence Services Act 1994. §10*	Controlar os gastos, a administração e a política do Serviço de Segurança, do Serviço de informações e do GCHQ.

País	Serviço de informações	Base jurídica	Missões	SIGINT Satélites	Autoridade de fiscalização	Base jurídica	Competências
REINO UNIDO	**Security Service = MI5**, sob tutela do Ministro do Interior	*Security Services Acts 1989* ***and*** *1996*	recolha de informações para **garantir** a segurança interna; contra-espionagem, acção contra os movimentos extremistas (incluindo o IRA), terrorismo e elementos subversivos		*The Security Service* **Commissioner** *The Intelligence e Security Committee*	*Security Service Act* ***1989****. §4* *Intelligence Services Act 1994. §10*	Todos os membros do **Serviço de informações**, do GCHQ e todos os funcionários do departamento da Secretaria de Estado devem revelar ou fornecer ao Comissário qualquer documento .. que este requeira … Controlar os gastos, a administração e a política do Serviço de Segurança, do Serviço de informações e do GCHQ. A comissão é composta por nove membros (Câmara dos Comuns + Câmara dos Lordes, não sendo nenhum Ministro da Coroa)
REINO UNIDO	**Defence Intelligence Staff (DIS)** sob a tutela do Ministro da Defesa		Apoio à segurança militar; avaliação e análise de informações militares, políticas, técnico-científicas e económicas				

			escolhidas				
País	**Serviço de informações**	**Base jurídica**	**Missões**	**SIGINT Satélites**	**Autoridade de fiscalização**	**Base jurídica**	**Competências**
EUA	**Central Intelligence Agency (CIA)**	*National Security Act 1947*	Recolha, a nível mundial, de informações; contra-espionagem no estrangeiro, responsabilidade central por todas as questões dos serviços de informações nos EUA		*Senate*: S*enate Select Committee on Intelligence (SSCI)* *House of Representatives: House Permanent Select Committee on Intelligence (HPSCI)*	Instituída por decisão do Senado de 19.5.1976; regulamentada pela *Intelligence Oversight Act 1980* H. Res. 658 of the 95th Congress instituída pela decisão da House of Representatives de 17.7.1977, regulamentada pela *Intelligence Oversight Act 1980*	Ambas as comissões têm direito de inquérito; direito ilimitado de informação; ambas as comissões participam na nomeação dos principais responsáveis dos serviços de informações
EUA	**Defense Intelligence Agency (DIA)**	Instituída pela *Directive 5105.21 de* 1961, emanada do Ministro da Defesa *Executive Order 11905* de 1976 *DoD Directive 5105.21 1978 Executive Order 12036* *1981 Executive Order 12333*	responsável pela obtenção de informações militares para as tropas de combate e responsáveis políticos no Ministério da Defesa e no Governo		S*enate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI*	cf. supra	cf. supra

País	Serviço de informações	Base jurídica	Missões	SIGINT Satélites	Autoridade de fiscalização	Base jurídica	Competências
EUA	**National Security Agency (NSA)**	*Executive Order 12333 of 4 December 1981*	responsável pela segurança dos sistemas de informações norte-americanos, designadamente actividades de encriptação; responsável pela intercepção de comunicações no estrangeiro	sim	S*enate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI*	cf. supra	cf. supra
EUA	**National Imagery and Mapping Agency (NIMA)**	*National Imagery and Mapping Agency Act of 1996.*	responsável pela disponibilização de fotografias e de mapas, bem como pela respectiva apreciação;		S*enate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI*	cf. supra	cf. supra
EUA	**National Reconnaissance Office (NRO)**		Responsável pelo desenvolvimento e utilização de sistemas de satélite de espionagem (SIGINT, Imagens)		S*enate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI*	cf. supra	cf. supra

País	Serviço de informações	Base jurídica	Missões	SIGINT Satélites	Autoridade de fiscalização	Base jurídica	Competências
EUA	**US Army Intelligence (z.B Deputy Chief of Staff for Intelligence, Intelligence and Security command (INSCOM)**	*Executive Order 12333* (December 4,1981)	Recolha e análise de informações no sector militar; desenvolvimento de estratégias e de sistemas de informações militares e guerra electrónica	sim	S*enate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI*	cf. supra	cf. supra
USA	**Marine Corps Intelligence Activity (MCIA) National Maritime Intelligence Center (NMIC)**	*Executive Order 12333* (December 4, 1981)	Espionagem militar; desenvolvimento de encriptação e de meios electrónicos para fins bélicos	sim	S*enate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI*	cf. supra	cf. supra
USA	**Office of Naval Intelligence (ONI)**	*Executive Order 12333* (December 4, 1981)	Informações destinadas à Marinha Análise de armadas estrangeiras, recolha de dados sobre o sistema de vigilância dos oceanos, sobre plataformas e sistemas de armamento submarinos	sim	S*enate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI*	cf. supra	cf. supra

País	Serviço de informações	Base jurídica	Missões	SIGINT Satélites	Autoridade de fiscalização	Base jurídica	Competências
EUA	**Air Intelligence Agency (AIA)**	*Executive Order 12333* (December 4, 1981)	Informações destinadas à força aérea; espionagem militar	Sim	S*enate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI*	cf. supra	cf. supra
EUA	**Federal Bureau of Investigation (FBI)**	*Title 28, United States Code (U.S. Code)*, Section 533 Instituído em 1908; Nome desde 1935	Contra-espionagem; polícia federal;		S*enate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI*	cf. supra	cf. supra
EUA	**Drug Enforcement Administration**	*Executive Order on July 1, 1973*	Recolha de informações sobre estupefacientes e branqueamento de capitais no país e no estrangeiro		S*enate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI*	cf. supra	cf. supra

País	Serviço de informações	Base jurídica	Missões	SIGINT Satélites	Autoridade de fiscalização	Base jurídica	Competências
Canadá	**Communication Security Establishment (CSE);** é apoiado pelo **Canadian Forces Supplementary Radio System (CFSRS)**	O mandato formal é classificado, provavelmente estabelecido com o aval do Gabinete	Aconselhamento do Governo e do sector económico em questões de segurança relativas à transmissão e ao processamento de dados (Infosec); desenvolvimento de sistemas de encriptação	sim	Não existe um órgão de fiscalização independente (fiscalização efectuada pelo *Auditor General* e pelo Ministro da Defesa que é responsável perante o Parlamento)	(1977 *Auditor General Act)*	"value-for-money" auditing "compliance" auditing
Canadá	**Canadian Security Intelligence Service (CSIS)** sob a tutela do Ministro do Interior	*Canadian Security Intelligence Service Act (CSIS Act)* de 1984	Contra-espionagem, combate à sabotagem e ao terrorismo internacional no interior do país		**The Security Intelligence Review Committee (SIRC)** Órgão independente, constituído por 5 membros que não são deputados	*Canadian Security Intelligence Service Act (CSIS Act) de* 1984	Direito geral de inquérito e de informação
Canadá	**Director General Intelligence Division** (Parte integrante do *Deputy Chief of the Defence Staff)* sob a tutela do Ministro da Defesa		Informações destinadas ao sector militar				

País	Serviço de informações	Base jurídica	Missões	SIGINT Satélites	Autoridade de fiscalização	Base jurídica	Competências
Austrália	**Defence Signals Directorate (DSD**) sob a tutela do Ministro da Defesa		Recolha e difusão de „*signal intelligence*“; Disponibilização de produtos de segurança em matéria de informação (Infosec) para o Governo e as forças armadas.		*Inspector General of Intelligence and Security (IGIS)* (nomeado pelo Primeiro-Ministro)	Inspector-General of Intelligence and Security Act 1986	Direito geral de informação e inquérito; Fiscaliza a observância das leis
Austrália	**Defence Intelligence Organisation (DIO)** sob a tutela do Ministro da Defesa		Recolha e avaliação de informação e *intelligence* estragégicas e militares		*Inspector-General of Intelligence and Security (IGIS)*	cf. supra	cf. supra
Austrália	**Australian Secret Intelligence Service (ASIS)** Serviço de Informações Externa sob a tutela do Ministro dos Negócios Estrangeiros		Recolha de informações sobre o estrangeiro, designadamente o Sudeste Asiático, no interesse da segurança nacional, da economia e das relações externas		*Inspector-General of Intelligence and Security (IGIS)*	cf. supra	cf. supra

País	Serviço de informações	Base jurídica	Missões	SIGINT Satélites	Autoridade de fiscalização	Base jurídica	Competências
AUSTRÁLIA	**Australian Security Intelligence Organisation (ASIO)**	*The Australian Security Intelligence Organisation Act 1979 (the ASIO Act)*	Protecção contra a violência por razões de ordem política; segurança pessoal e material Combate ao terrorismo internacional e à transferência ilegal de tecnologia		*Parliamentary Joint Committee on the Australian Security Intelligence Organization* *Inspector-General of Intelligence and Security (IGIS)*	Section 92C of the ASIO Act cf. supra	Responde perante o "Attorney General" e, em caso de aprovação deste último, perante o Parlamento O "Parliamentary joint Committee" não pode examinar: - Obtenção e transmissão de "foreign intelligence"; - Actividades ASIO que não digam respeito a cidadãos australianos ou a outros habitantes da Austrália; - Questões sensíveis do ponto de vista operativo; - Queixas individuais.
AUSTRÁLIA	**Office of National Assessments** Órgão independente	*Office of National Assessments Act 1977*	Apresente o relato ao Primeiro-Ministro		*Inspector-General of Intelligence and Security (IGIS)*	cf. supra	cf. supra

País	Serviço de informações	Base jurídica	Missões	SIGINT Satélites	Autoridade de fiscalização	Base jurídica	Competências
Nova Zelândida	**Government Communications Security Bureau (GCSB)** sob a tutela do Primeiro-Ministro	Instituído em 1977 Inexistência, até à data, de base jurídica, encontrando-se já em apreciação no Parlamento a respectiva proposta de diploma (*Government Communications Security Bureau Bill*)	Aquisição de informação sobre o estrangeiro; Segurança das comunicações; Segurança informática e da informação (Infosec); Segurança técnica	sim	*Inspector-General of Intelligence and Security* *Intelligence and Security Committee* (Premierminister, Oppositionsführer, 3 Abgeordnete)	*The Inspector-General of Intelligence and Security Act 1996* *The Intelligence and Security Committee Act 1996*	Verificar as actividades do GCSB e SIS - quanto à observância das leis; - em caso de queixas apresentadas por uma "New Zealand person" apresenta relatório ao Ministro da tutela fiscaliza os sectores político e administrativo, bem como as despesas dos GCSB e SIS (obtém apenas de modo limitado informações de carácter operativo) apresenta relato ao Parlamento
Nova Zelândia	**New Zealand Security Intelligence Service (SIS)** Serviço de Informações Nacional sob a tutela do Primeiro-Ministro	*New Zealand Security Intelligence Service Act 1969*	Contra-espionagem; protecção contra o terrorismo e violência motivada por razões de ordem política; sensibilização do mundo científico e industrial para a espionagem industrial e para a transferência ilegal de tecnologia				

País	Serviço de informações	Base jurídica	Missões	SIGINT Satélites	Autoridade de fiscalização	Base jurídica	Competências
Nova Zelândia	**External Assessments Bureau (EAB)** Serviço de Informações externas sob a tutela do Primeiro-Ministro		Analisa a evolução da situação política e elabora relatórios sobre acontecimentos e tendências de ordem política e económica				
Nova Zelândia	**Directorate of Defense Intelligence and Security (DDIS)** Serviço de informações militares sob a tutela do Ministro da Defesa		Serviço de informações militares; Recolha de dados relevantes do ponto de vista militar, sobretudo referentes à Ásia e ao Pacífico; Análise de informação táctica e estratégica				