PARLAMENTO EUROPEO

1999 *2004*

Commissione temporanea sul sistema d'intercettazione Echelon

PROVVISORIO

18 maggio 2001

PROGETTO DI RELAZIONE

sull'esistenza di un sistema d'intercettazione globale per le comunicazioni private ed economiche (sistema d'intercettazione ECHELON)

Commissione temporanea sul sistema d'intercettazione Echelon

Relatore: Gerhard Schmid

INDICE

Pagina

PAGINA REGOLAMENTARE

Nella riunione del 5 luglio 2000 il Parlamento europeo ha approvato una decisione in merito alla costituzione di una commissione temporanea sul sistema d'intercettazione Echelon. Per ottemperare al proprio mandato, nella riunione costituente del 5 luglio 2000 la commissione temporanea ha nomicano relatore Gerhard Schmid.

Nella riunione (Nelle riunioni) del … ha esaminato il progetto di relazione.

In quest'ultima riunione/Nell'ultima riunione indicata ha approvato le conclusioni in appresso con … voti favorevoli, … contrario(i) e … astensione(i)/all'unanimità.

Erano presenti al momento della votazione … (presidente/presidente f.f.), … (vicepresidente), … (vicepresidente), … (relatore), …, … (in sostituzione di …), … (in sostituzione di …, a norma dell'articolo 153, paragrafo 2, del regolamento), … e … .

La relazione è stata presentata il … .

Il termine per la presentazione di emendamenti sarà indicato nel progetto di ordine del giorno della tornata nel corso della quale la relazione sarà/è stata esaminata, alle ore… .

PROPOSTA DI RISOLUZIONE

Risoluzione del Parlamento europeo sull'esistenza di un sistema d'intercettazione globale per le comunicazioni private ed economiche (sistema d'intercettazione ECHELON)

Il Parlamento europeo,

– vista la decisione del Parlamento europeo del 5 luglio 2000 di costituire una commissione temporanea sul sistema d'intercettazione Echelon e il relativo mandato,

– visto il trattato CE che mira all'istituzione di un mercato comune caratterizzato da un elevato livello di competitività,

– visto il trattato sull'Unione europea, in particolare l'articolo 6, paragrafo 2, che sancisce l'obbligo per l'Unione europea a rispettare i diritti fondamentali, e al suo titolo V, che riguarda le disposizioni in merito a una politica estera e di sicurezza comune,

– vista la Carta dei diritti fondamentali dell'Unione europea, il cui articolo 7 tutela la vita privata e la vita familiare, e cita espressamente il diritto al rispetto delle comunicazioni,

– vista la Convenzione europea per la salvaguardia dei diritti dell'uomo, in particolare l'articolo 8 che tutela la vita privata, nonché gli altri numerosi accordi internazionali che contemplano la tutela della vita privata,

– vista la relazione sull'esistenza di un sistema d'intercettazione globale per le comunicazioni private ed economiche (sistema d'intercettazione Echelon) della commissione temporanea sul sistema d'intercettazione Echelon (A5-…/2001),

Sull'esistenza di un sistema di intercettazione globale per comunicazioni private ed economiche (sistema di intercettazione ECHELON)

A. considerando che non si può nutrire più alcun dubbio in merito all'esistenza di un sistema di intercettazione delle comunicazioni a livello mondiale, cui cooperano in proporzione gli Stati Uniti, il Regno Unito, il Canada, l'Australia e la Nuova Zelanda nel quadro del Patto UKUSA; che sulla base degli attuali indizi sembri verosimile che il suo nome in codice sia effettivamente "ECHELON" e che comunque ciò rivesta un'importanza secondaria,

B. considerando che il sistema non è destinato all'intercettazione delle comunicazioni di carattere militari, bensì di quelle private ed economiche, ma dall'analisi riportata nella relazione è emerso che questo sistema non può di certo essere così potente come sostenuto da una parte dei media,

Sui limiti del sistema di intercettazione

C. considerando che il sistema di sorveglianza si basa sull'intercettazione globale delle comunicazioni via satellite; che tuttavia nelle aree ad elevata densità di comunicazioni solo un volume estremamente ridotto di queste viene trasmesso tramite satellite; che in tal modo la maggior parte di esse non può essere intercettata dalle stazioni di terra, bensì solo inserendosi nei cavi o captando le trasmissioni via radio, operazioni, queste, che - come

hanno dimostrato le ricerche riportate nella relazione - sono possibili solo entro limiti ristretti; che l'impiego di personale per l'analisi finale delle comunicazioni intercettate comporta ulteriori limiti; che di conseguenza gli Stati ECHELON hanno accesso solo ad una parte molto esigua delle comunicazioni via cavo e via radio e sono in grado di analizzare solo una percentuale ridotta delle comunicazioni,

Sulla possibile esistenza di altri sistemi di intercettazione

D. considerando che l'intercettazione di comunicazioni costituisce un usuale strumento di spionaggio impiegato nell'ambito dei servizi di informazione e che anche altri Stati potrebbero gestire un simile sistema, nella misura in cui dispongano delle corrispondenti risorse finanziarie e delle circostanze geografiche adeguate; che la Francia sarebbe - o perlomeno era per quanto riguarda le circostanze geografiche - l'unico Stato membro dell'Unione europea in grado di istituire da solo un sistema di intercettazione globale, in considerazione dei suoi territori d'oltremare e che inoltre vi sono elementi che consentono di supporre che anche la Russia potrebbe gestire un sistema di questo genere,

Sulla compatibilità con il diritto dell'Unione europea

E. considerando che la questione attinente alla compatibilità di un sistema del tipo ECHELON con il diritto dell'Unione europea richiede di operare una distinzione: se il sistema viene impiegato solo nell'ambito dei servizi di informazione, non si pone alcun elemento di contrasto con la normativa europea, in quanto le attività di sicurezza degli Stati non sono contemplate dal trattato CE, ma rientrerebbero nel titolo V del trattato sull'Unione europea (PESC), benché al momento non sia prevista ancora alcuna regolamentazione pertinente e quindi manchino punti di contatto. Per converso, se l'impiego del sistema è abusivo, quest'ultimo è in contrasto con l'obbligo di lealtà degli Stati membri e con il concetto di un mercato comune caratterizzato dalla libera concorrenza, e quindi uno Stato membro che vi partecipi agisce in violazione del diritto dell'Unione europea.

Sulla compatibilità con il diritto fondamentale alla vita privata (articolo 8 della CEDU)

F. considerando che tutte le intercettazioni di comunicazioni rappresentano una profonda ingerenza nella vita privata del singolo; che l'articolo 8 della CEDU tutela la vita privata e ammette queste interferenze solo se sono necessarie per salvaguardare la sicurezza nazionale, nella misura in cui le disposizioni in materia siano previste dalla legge nazionale e accessibili in generale, e stabiliscano in quali circostanze e a quali condizioni l'autorità pubblica può ricorrervi; che inoltre le ingerenze nella vita privata devono essere proporzionate rispetto all'interesse da tutelare, e quindi conformemente a quanto sancito dalla CEDU non è sufficiente che siano meramente utili o auspicabili.

G. considerando che un sistema del servizio di informazione che captasse qualsiasi comunicazione senza garantire il rispetto del principio di proporzionalità non sarebbe compatibile con la CEDU; che parimenti si sarebbe in presenza di una violazione della CEDU nel caso in cui la normativa che disciplina la sorveglianza delle comunicazioni non preveda alcuna base giuridica, non sia accessibile in generale o sia formulata in maniera tale da non poter ipotizzare quali siano le eventuale conseguenze per i singoli; che le norme che disciplinano l'attività dei servizi di informazione americani all'estero sono in gran parte riservate, pertanto vi è ragione almeno di dubitare che il principio di proporzionalità venga rispettato e di sostenere che si è in presenza di una violazione dei principi di accessibilità del diritto e di prevedibilità del rispetto sanciti dalla CEDU,

H. considerando che gli Stati membri non si possono sottrarre agli obblighi che incombono loro in virtù della CEDU, in quanto consentono di operare sul loro territorio ai servizi di informazione di altri Stati che prevedono normative meno rigide, poiché altrimenti il principio di legalità verrebbe privato delle sue due componenti, l'accessibilità e la prevedibilità del rispetto, e quanto sancito dalla CEDU svuotato di contenuto,

I. considerando che la compatibilità con i diritti fondamentali dell'attività dei servizi di informazione legittimata in virtù di una legislazione in materia richiede la presenza di sistemi di controllo adeguati, in modo da controbilanciare il pericolo insito nell'azione segreta di una parte dell'apparato amministrativo; che la Corte europea dei diritti dell'uomo ha sottolineato espressamente la necessità di avvalersi di un sistema di controllo efficiente nell'ambito dell'attività dei servizi di informazione, e pertanto desta preoccupazioni il fatto che alcuni Stati membri non dispongano di alcun proprio organo parlamentare di controllo che si occupi dei servizi segreti,

Sulla questione se i cittadini dell'Unione europea sono tutelati in modo adeguato nei confronti dei servizi di informazione

J. considerando che la tutela dei cittadini dell'Unione europea dipende dalla situazione giuridica propria dei singoli Stati membri, i quali sono tuttavia strutturati in modo diverso, e a volte non dispongono di alcun organo parlamentare di controllo, tanto da rendere quasi impossibile sostenere che sia garantita una tutela sufficiente; che i cittadini europei hanno un interesse fondamentale a che i rispettivi parlamenti nazionali siano dotati di una commissione di controllo speciale strutturata formalmente, che sorvegli e controlli le attività dei servizi di informazione; che persino laddove un organo di controllo è presente questo è più interessato ad occuparsi dell'attività dei servizi di informazione nazionali che non di quelli esteri, in quanto normalmente i cittadini del proprio Stato rientrano solo nel primo caso,

K. considerando che qualora i servizi di informazione cooperino nel quadro della PESC si chiede alle istituzioni di creare condizioni di protezione sufficienti a favore dei cittadini europei,

Sullo spionaggio economico

L. considerando che rientra nell'attività dei servizi di informazione esteri occuparsi di dati economici, quali sviluppi settoriali, andamento dei mercati delle materie prime, rispetto di embarghi economici, rispetto delle regole di fornitura di beni a duplice uso, e così via, e che questi elementi spiegano il motivo per cui spesso le imprese pertinenti vengano sorvegliate,

M. considerando che non è in alcun caso tollerabile che i servizi di informazione, nello svolgimento di indagini su imprese estere, vengano sfruttati per lo spionaggio economico al fine di avvantaggiare la concorrenza sul territorio nazionale; che tuttavia non vi è alcun elemento a sostegno del fatto che il sistema d'intercettazione globale sia stato creato a tale scopo, benché sia stato affermato più volte,

N. considerando che spesso i dati aziendali sensibili si trovano all'interno delle stesse imprese, e pertanto lo spionaggio della concorrenza si traduce principalmente nel tentativo di ottenere informazioni dai dipendenti o tramite soggetti introdotti clandestinamente oppure cercando di inserirsi nelle reti informatiche interne; che solo nel caso in cui i dati sensibili vengano trasmessi all'esterno via cavo o via radio (satellite) si può impiegare un sistema di sorveglianza delle comunicazioni a fini di spionaggio della concorrenza e che tale situazione

si verifica in modo sistematico solo nei seguenti tre casi:
- imprese che operano in tre aree geografiche con fuso orario diverso, i cui risultati intermedi vengono inviati dall'Europa verso l'America e quindi trasmessi in Asia;
- videoconferenze di gruppi multinazionali trasmesse tramite sistemi V-sat o via cavo;
- ordini importanti le cui trattative si svolgono in loco (ad esempio costruzione di impianti, installazione di infrastrutture delle telecomunicazioni, costruzione di nuovi sistemi di trasporto e così via) e da lì devono essere definiti con la sede centrale.

Sulle possibilità di autotutelarsi

O. considerando che la sicurezza delle imprese si può conseguire solo rendendo sicuro l'intero ambiente di lavoro e proteggendo tutte le vie di comunicazione attraverso le quali vengono trasmesse le informazioni sensibili; che il mercato europeo offre sistemi di cifratura sufficientemente sicuri e a prezzi convenienti; che anche i privati devono ricorrere con urgenza alla crittazione dei messaggi di posta elettronica; che un messaggio non crittato è alla stregua di una lettera senza busta; che in Internet sono disponibili gratuitamente per gli utenti privati sistemi di uso relativamente facile.

Sulla cooperazione dei servizi di informazione nell'ambito dell'Unione europea

P. considerando che l'Unione europea ha comunicato la propria intenzione di coordinare la raccolta di informazione da parte dei servizi di informazione nel quadro di una propria politica di sicurezza e di difesa, senza tuttavia interrompere la cooperazione in questi settori con altri partner,

Q. considerando che una cooperazione dei servizi di informazione nell'ambito dell'Unione europea sarebbe anche auspicabile, poiché, da un lato, una politica di sicurezza comune che escluda la partecipazione dei servizi segreti non sarebbe sensata, e, dall'altro, vi sarebbero collegati non pochi vantaggi sotto il profilo professionale, finanziario e politico; che essa corrisponderebbe più adeguatamente al concetto di un partner che si pone di fronte agli USA su un piano di parità e potrebbe riunire tutti gli Stati membri in un sistema pienamente compatibile con quanto sancito dalla CEDU; che ovviamente il controllo di tale cooperazione deve essere affidato al Parlamento europeo,

R. considerando che il Parlamento europeo ha in programma di elaborare propri regolamenti in merito all'accesso a informazioni e documenti confidenziali e sensibili,

Sulla conclusione e modifica di accordi internazionali sulla tutela dei cittadini e delle imprese

1. invita il Segretario generale del Consiglio d'Europa a chiedere al comitato dei ministri di valutare se sia opportuno adeguare la tutela della vita privata garantita ai sensi dell'articolo 8 della CEDU ai moderni metodi di comunicazione e alle possibilità di intercettazione inserendola in un protocollo addizionale o considerandola insieme alla normativa sulla tutela dei dati nel quadro di una revisione della convenzione sulla tutela dei dati, a condizione di non ridurre il livello di protezione giuridica conseguito attraverso il tribunale né di diminuire il grado di flessibilità necessaria per gli adeguamenti agli sviluppi futuri;

2. esorta gli Stati membri a istituire una piattaforma europea allo scopo di esaminare le disposizioni di legge per quanto riguarda il rispetto del segreto epistolare e delle comunicazioni, e ad accordarsi su un testo comune, che garantisca a tutti i cittadini europei la tutela della vita privata sull'intero territorio degli Stati membri in conformità di quanto

stabilito all'articolo 7 della Carta dei diritti fondamentali dell'Unione europea, e che garantisca altresì che l'attività dei servizi di informazione sia compatibile con i diritti fondamentali, nonché esercitata in base alle condizioni di cui all'articolo 8 della CEDU, indicate al capitolo 8 della relazione, in particolare al punto 8.3.4;

3. invita gli Stati membri ad approvare un protocollo addizionale che consenta alle Comunità europee di aderire alla CEDU, oppure a riflettere su altre eventuali misure intese ad ovviare ai conflitti giurisprudenziali tra la Corte di Strasburgo e la Corte di Lussemburgo;

4. invita il Segretario generale dell'ONU ad incaricare la commissione responsabile di presentare proposte intese ad adeguare alle innovazioni tecniche l'articolo 17 del Patto internazionale sui diritti civili e politici che garantisce la tutela della vita privata;

5. esorta gli Stati Uniti a firmare il protocollo addizionale al Patto internazionale sui diritti civili e politici, affinché, in caso di sua violazione, sia possibile presentare ricorsi individuali contro gli Stati Uniti dinanzi alla tradizionale commissione per i diritti umani; sollecita le ONG americane di pertinenza, in particolare l'ACLU (American Civil Liberties Union) e l'EPIC (Electronic Privacy Information Center) ad esercitare la dovuta pressione sul governo americano;

Sulle misure legislative nazionali intese a tutelare cittadini e imprese

6. invita gli Stati membri a verificare che la legislazione nazionale in materia di attività dei servizi di informazione sia compatibile con i diritti fondamentali;

7. sollecita gli Stati membri ad adoperarsi per conseguire l'obiettivo, riguardo all'attività dei servizi di informazione, di una tutela comune il cui livello corrisponda al più elevato tra quelli garantiti dagli Stati dell'Unione europea, poiché i soggetti interessati dall'attività di un servizio di informazione estero sono di solito i cittadini di paesi terzi e pertanto anche di altri Stati membri;

8. invita le istituzioni dell'Unione europea a creare condizioni di protezione sufficienti a favore dei cittadini europei nel caso in cui i servizi di informazione cooperino nel quadro della PESC; il Parlamento europeo in qualità di logico organo di controllo deve, dal canto proprio, predisporre le circostanze necessarie per la sorveglianza di questo settore altamente sensibile, in modo da esigere in modo realistico ma anche fondato i dovuti diritti attinenti al controllo;

Sulle misure legislative speciali volte alla lotta contro lo spionaggio industriale

9. esorta gli Stati membri a riflettere sul modo in cui sia possibile in forza di normative del diritto europeo e di quello internazionale lottare contro lo spionaggio economico e la corruzione come mezzo per assicurarsi appalti, in particolare valutare se sia possibile elaborare una regolamentazione nel quadro dell'OMC che tenga conto delle distorsioni della concorrenza imputabili a un tale comportamento, ad esempio considerando nulli simili accordi;

10. sollecita gli Stati membri ad impegnarsi in una esplicita dichiarazione comune a non condurre alcuna attività di spionaggio economico gli uni nei confronti degli altri, e a dimostrare di conseguenza di essere in armonia con lo spirito e le disposizioni del trattato CE;

Sulle misure intese all'applicazione del diritto e loro controllo

11. esorta i parlamenti nazionali che non dispongono di un proprio organo di controllo incaricato di sorvegliare i servizi d'informazione a istituirne uno;

12. invita gli organi di controllo nazionali dei servizi segreti ad attribuire grande peso alla tutela della vita privata nell'esercizio dell'attività di controllo a loro affidata, a prescindere dal fatto che si tratti di sorvegliare i cittadini del proprio Stato, di un altro Stato membro o di paesi terzi;

13. sollecita la Germania e l'Inghilterra a subordinare l'ulteriore autorizzazione sul loro territorio di intercettazioni di comunicazioni ad opera dei servizi di informazione degli USA alla compatibilità con la CEDU, vale a dire tali attività devono soddisfare il principio di proporzionalità, avere base giuridica accessibile e conseguenze prevedibili per il singolo, ed esorta altresì i due Stati ad esercitare un controllo efficiente, poiché sono responsabili sul loro territorio della compatibilità dell'attività dei servizi di informazione, sia essa autorizzata o anche solo tollerata;

Sulle misure intese a promuovere l'autotutela di cittadini e imprese

14. invita la Commissione e gli Stati membri a sviluppare programmi volti a promuovere la sensibilizzazione di cittadini e imprese in merito alla questione della sicurezza e intesi al contempo ad offrire un sostegno pratico all'elaborazione e all'attuazione di concetti di protezione di ampia portata;

15. esorta la Commissione e gli Stati membri ad elaborare misure adeguate intese a promuovere, sviluppare e realizzare tecnologie e software di cifratura europei e volte soprattutto a sostenere i progetti incentrati sullo studio di software di crittazione di facile uso il cui testo sorgente sia noto;

16. sollecita la Commissione e gli Stati membri a sviluppare software di cui sia reso pubblico il testo sorgente, in modo da poter garantire l'assenza di eventuali "backdoor" (cosiddetti "open-source software" o "software liberi");

17. invita le istituzioni europee e le amministrazioni pubbliche degli Stati membri a ricorrere in modo sistematico alla cifratura dei messaggi di posta elettronica, in modo che nel lungo periodo la crittazione diventi un procedimento consueto;

Su altre misure

18. sollecita le imprese a rafforzare la cooperazione con i servizi di controspionaggio e a informarli in merito a particolari attacchi dall'esterno a fini di spionaggio industriale, in modo da potenziare l'efficienza di detti servizi;

19. esorta la Commissione a presentare una proposta in merito all'istituzione di un servizio di consulenza europeo nel settore della sicurezza delle informazioni delle imprese, volto non solo ad accrescere la sensibilizzazione in tale ambito, ma anche ad offrire un sostegno pratico;

20. ritiene opportuno organizzare un congresso transeuropeo sulla tutela della vita privata contro la sorveglianza delle telecomunicazioni, affinché ONG europee, statunitensi e di altri Stati creino una piattaforma che consenta di confrontarsi su aspetti transfrontalieri e internazionali

e di coordinare i settori di attività e gli interventi;

21. incarica la sua Presidente di trasmettere la presente risoluzione al Consiglio, alla Commissione, ai governi e ai parlamenti degli Stati membri e dei paesi candidati all'adesione e al Consiglio d'Europa.

MOTIVAZIONE

1. INTRODUZIONE:

1.1. Istituzione della commissione

Il 5 luglio 2000 il Parlamento europeo ha deciso di istituire una commissione temporanea sul sistema ECHELON. All'origine di questa decisione vi è il dibattito sullo studio commissionato dallo STOA[1] in merito al cosiddetto sistema ECHELON[2], presentato dall'autore Duncan Campbell in occasione di un'audizione della commissione per le libertà e i diritti dei cittadini, la giustizia e gli affari interni sull'argomento "Unione europea e tutela dei dati".

1.2. Le tesi dei due studi STOA su un sistema globale d'intercettazione con il ECHELON

1.2.1. La prima relazione STOA del 1997

In una relazione commissionata nel 1997 alla Omega Foundation dallo STOA[3], per conto del Parlamento europeo, sulla tematica "Valutazione delle tecnologie di controllo politico", nel capitolo "Reti nazionali ed internazionali di sorveglianza delle telecomunicazioni" veniva descritto anche ECHELON. Il redattore dello studio vi affermava che, in ambito europeo, tutte le comunicazioni tramite e-mail, telefono e fax sono oggetto di regolari intercettazioni da parte dell'NSA (il servizio americano d'informazione estera)[4]. Questa relazione ha reso nota l'esistenza di ECHELON quale sistema globale di intercettazione, presumibilmente onnicomprensivo, a livello europeo.

1.2.2. Le relazioni STOA del 1999

Per ottenere maggiori informazioni in materia, nel 1999 la STOA ha commissionato uno studio in cinque volumi relativo a "Sviluppo delle tecnologie di sorveglianza e rischio di impiego abusivo di informazioni economiche". Il volume 2/5, redatto da Duncan Campbell, riguardava l'esame delle potenzialità dei servizi d'informazione esistenti all'epoca, ed in particolare le modalità operative di ECHELON.[5]

---

[1] Lo STOA (Scientific and Technological Options Assesment) è un servizio della Direzione generale degli Studi del Parlamento europeo, che elabora studi di ricerca.

[2] Il livello tecnologico raggiunto dai servizi di communications intelligence (COMINT) in materia di elaborazione automatizzata a fini di spionaggio delle informazioni intercettate da sistemi di comunicazione multilingue a banda larga e relativa applicabilità alla programmazione e selezione di attività COMINT, compreso il riconoscimento vocale (ottobre 1999).

[3] Scientific and Technological Options Assesment

[4] Steve Wright, An appraisal of technologies for political control (1998), 20

[5] Il livello tecnologico raggiunto dai servizi di communications intelligence (COMINT) in materia di elaborazione automatizzata a fini di spionaggio delle informazioni intercettate da sistemi di comunicazione multilingue a banda larga e relativa applicabilità alla programmazione e selezione di attività COMINT, compreso il riconoscimento vocale (ottobre 1999), PE 168.184.

Ha suscitato particolare attenzione l'affermazione, contenuta nella relazione, secondo cui ECHELON ha abbandonato l'obiettivo originario, vale a dire la difesa dall'Oriente, per essere oggi utilizzato a fini di spionaggio economico. Questa tesi è confortata, nella relazione, da esempi di presunto spionaggio economico, che avrebbero in particolare arrecato pregiudizio all'Airbus e a Thomsom CFS.

A seguito dello studio STOA, ECHELON è stato oggetto di dibattito in quasi tutti i parlamenti degli Stati membri, e in Francia e Belgio sono state persino elaborate relazioni in merito.

1.3. Il mandato della commissione

Contestualmente alla decisione sull'istituzione di una commissione temporanea, il Parlamento europeo ne ha deciso il mandato. Di conseguenza, alla commissione temporanea si è attribuito mandato di:

"- verificare l'esistenza del sistema d'intercettazione delle comunicazioni noto come ECHELON, la cui attività è descritta nella relazione STOA sullo sviluppo della tecnologia di sorveglianza e i rischi di abuso dell'informazione economica;
- verificare la compatibilità di tale sistema con la legislazione comunitaria, in particolare l'articolo 286 del trattato CE e le direttive 95/46/CE e 97/66/CE nonché l'articolo 6, paragrafo 2, del trattato sull'Unione europea, alla luce dei seguenti quesiti:
  - i diritti dei cittadini europei sono tutelati nei confronti delle attività di servizi segreti?
  - la cifratura costituisce una protezione adeguata e sufficiente per garantire la privacy dei cittadini o sarebbe opportuno adottate misure aggiuntive e, in caso affermativo, di quale tipo?
  - come sviluppare la consapevolezza delle istituzioni europee riguardo ai rischi connessi a tali attività e quali misure adottare?
- verificare se l'industria europea è esposta a rischi a causa dell'intercettazione globale delle comunicazioni;
- eventualmente, formulare proposte relative ad iniziative politiche e legislative."

1.4. Perché non è stata istituita una commissione d'inchiesta

Il Parlamento europeo si è quindi pronunciato a favore dell'istituzione di una commissione temporanea, in quanto l'insediamento di una commissione d'inchiesta è previsto soltanto per verificare le infrazioni al diritto comunitario nell'ambito del trattato CE (articolo 193 TCE), ed essa può quindi occuparsi esclusivamente delle questioni ivi disciplinate. Sono esclusi i settori che rientrano nei titoli V (PESC) e VI TUE (cooperazione di polizia e giudiziaria in materia penale). Inoltre, le prerogative particolari di una commissione d'inchiesta in materia di citazione ed esame della pratica, ai sensi dell'accordo interistituzionale[6], sussistono soltanto qualora non vi si oppongano motivi di segretezza o di ordine pubblico e di sicurezza nazionale, il che esclude comunque l'indagine sui servizi segreti. Inoltre, una commissione d'inchiesta non può estendere le proprie attività a paesi terzi, in quanto, per definizione, questi ultimi non possono infrangere il diritto comunitario. L'istituzione di una commissione d'inchiesta avrebbe quindi comportato soltanto una limitazione di contenuti senza diritti aggiuntivi, per cui è stata respinta dalla maggioranza dei deputati del Parlamento europeo.

[6] Decisione del 19 aprile 1995 del Parlamento europeo, del Consiglio e della Commissione relativa alle modalità per l'esercizio del diritto d'inchiesta del Parlamento europeo (95/167/CE), articolo 3, paragrafi 3-5.

1.5. Metodi di lavoro e piano di lavoro

Per poter svolgere appieno il proprio mandato, la commissione ha scelto la procedura riportata qui di seguito. In un programma di lavoro proposto dal relatore ed approvato dalla commissione sono state elencate le seguenti aree tematiche di rilievo: 1. Conoscenze certe su ECHELON, 2. Discussione a livello di parlamenti nazionali e governi, 3. Servizi d'informazione e loro attività, 4. Sistemi di comunicazione e possibilità d'intercettarli, 5. Cifratura, 6. Spionaggio economico, 7. Obiettivi spionistici e misure di tutela e 8. Condizioni quadro giuridiche e tutela della vita privata. Questi argomenti sono stati trattati nell'ordine nelle singole riunioni, per cui la sequenza si è incentrata sui punti di vista pratici e non consente di desumere alcunché sul valore delle singole priorità tematiche. Nei lavori preparatori delle singole riunioni, il relatore ha esaminato e valutato in modo sistematico il materiale disponibile. Inoltre, in considerazione delle peculiarità dei vari argomenti, alle riunioni sono stati invitati rappresentanti delle amministrazioni nazionali (in particolare dei servizi segreti) e dei parlamenti nella loro funzione di organi di controllo, nonché esperti giuridici e nei settori delle tecniche di comunicazione ed intercettazione, della sicurezza d'impresa e della cifratura, a livello teorico e pratico. Si sono altresì tenuti incontri con giornalisti che avevano svolto ricerche in merito. Le riunioni si sono in genere svolte pubblicamente, ma talvolta anche a porte chiuse, laddove è sembrato opportuno per lo scambio d'informazioni. Inoltre, il presidente della commissione ed il relatore si sono recati congiuntamente a Londra e Parigi per incontrare persone impossibilitate, per vari motivi, a partecipare alle riunioni della commissione, il cui coinvolgimento nei lavori sembrava comunque necessario. Per lo stesso motivo il presidente della commissione, i coordinatori ed il relatore si sono recati negli USA. A ciò si aggiunga che il relatore ha avuto numerosi incontri individuali, talvolta confidenziali.

1.6. Le caratteristiche attribuite al sistema ECHELON

Il sistema d'intercettazione denominato "ECHELON" si differenzia da altri sistemi dei servizi d'informazione in virtù di due caratteristiche e presenta una peculiarità del tutto particolare:
La prima caratteristica è la capacità di consentire una sorveglianza pressoché totale. Ogni informazione trasmessa via telefono, telefax, Internet o e-mail, indipendentemente dal soggetto che la invia, deve poter essere intercettata in particolare da stazioni di ricezione satellitare e da satelliti spia, allo scopo di venire a conoscenza dei contenuti della stessa.

La seconda peculiarità di ECHELON è che il sistema funziona globalmente, grazie all'interazione di diversi Stati (Regno Unito, Stati Uniti, Canada, Australia e Nuova Zelanda), circostanza che rappresenta un valore aggiunto rispetto ai sistemi nazionali: gli Stati che aderiscono al sistema ECHELON (Stati ECHELON) possono mettere reciprocamente a disposizione le apparecchiature di intercettazione, accollarsi assieme le relative spese ed utilizzare assieme le informazioni di cui vengono a conoscenza. Questa interazione internazionale risulta particolarmente indispensabile per la sorveglianza a livello mondiale delle comunicazioni via satellite, perché solo in tal modo è possibile assicurare l'intercettazione di entrambi gli interlocutori nelle comunicazioni internazionali. È infatti evidente che le stazioni di ricezione satellitare, in considerazione delle loro dimensioni, non possono essere installate sul territorio di uno Stato senza l'autorizzazione dello stesso. È quindi indispensabile il reciproco consenso e l'interazione di vari Stati in diverse aree del mondo.

I possibili pericoli per la vita privata e l'economia derivanti da un sistema del tipo ECHELON non vanno tuttavia individuati solo nel fatto che si tratta di un sistema d'intercettazione

particolarmente potente, ma piuttosto nel fatto che esso opera spesso in assenza di diritto. Un sistema d'intercettazione destinato alle comunicazioni internazionali non riguarda solitamente gli abitanti del proprio Stato. La persona intercettata non gode quindi, quale straniero, di alcuna protezione giuridica nazionale. I soggetti intercettati sarebbero quindi totalmente esposti a tale sistema. In questo settore anche la sorveglianza parlamentare è insufficiente, dal momento che gli elettori, ritenendo che il sistema non riguardi loro bensì "esclusivamente" persone all'estero, non sono particolarmente interessati ed i rappresentanti eletti difendono in primo luogo gli interessi dei loro elettori. Non ci si deve quindi meravigliare del fatto che le consultazioni condotte in seno al Congresso americano sull'attività dell'NSA vertano esclusivamente sulla questione se dalle intercettazioni sono interessati anche cittadini americani, mentre l'esistenza di un tale sistema non provoca di per sé ulteriori riflessioni. Sembra quindi assumere particolare importanza confrontarsi a livello europeo.

2. L'attività dei servizi d'informazione esteri

2.1. Introduzione

La maggior parte dei governi gestisce, per garantire la sicurezza del paese, servizi d'informazione oltre a quelli di polizia. Poiché la loro attività è per lo più segreta, essi sono anche denominati servizi segreti. Questi servizi sono destinati

- ad ottenere informazioni volte a sventare pericoli per la sicurezza dello Stato
- al controspionaggio in genere
- a sventare pericoli che possano minacciare le forze armate
- ad ottenere informazioni su questioni all'estero

2.2. Cos'è lo spionaggio

I governi hanno bisogno di raccogliere e valutare sistematicamente informazioni su determinate situazioni degli altri Stati: si tratta di elementi fondamentali per prendere decisioni in materia militare, di politica estera ecc. È per questo che essi gestiscono servizi d'informazione esteri, che procedono anzitutto alla valutazione sistematica di fonti informative accessibili al pubblico. Il relatore dispone di affermazioni che provano che ciò costituisce, in media, perlomeno l'80% dell'attività dei servizi d'informazione.[7] Tuttavia, le informazioni particolarmente rilevanti nei suddetti settori vengono tenute segrete da governi o imprese e non sono quindi accessibili al pubblico. Chi tuttavia voglia entrare in loro possesso deve sottrarle: lo spionaggio non è altro che il furto organizzato di informazioni.

2.3. Obiettivi dello spionaggio

Gli obiettivi classici dello spionaggio sono i segreti militari, altri segreti di Stato o informazioni sulla stabilità dei governi o le minacce che incombono su di essi. Ciò riguarda, ad esempio, i nuovi sistemi di armamenti, le strategie militari od informazioni sullo stazionamento delle truppe. Altrettanto rilevanti sono le informazioni sulle decisioni a venire in materia di politica estera, decisioni in materia valutaria o informazioni privilegiate su tensioni all'interno di un governo. Vi è altresì un interesse per informazioni rilevanti sotto il profilo economico: vi possono rientrare, oltre alle informazioni settoriali, anche dettagli sulle nuove tecnologie o su affari esteri.

2.4. I metodi dello spionaggio

Spionaggio significa creare accesso alle informazioni che il loro possessore intende tutelare dall'accesso da parte di estranei. La tutela deve essere quindi elusa e violata, il che avviene sia nello spionaggio politico che in quello economico. Perciò, per lo spionaggio si pongono gli stessi problemi in entrambi i settori; ne consegue che in entrambi si applicano le stesse tecniche di spionaggio. Logicamente non vi sono differenze, ma il livello di tutela nel contesto economico è per lo più inferiore, per cui lo spionaggio di questo tipo è talvolta più semplice. In particolare, la

[7] La "Commission on the Roles and Capabilities of the US Intelligence Community" ha riscontrato nella sua relazione "Preparing for the 21st Century: An Appraisal of U.S. Intelligence" che il 95% delle informazioni di carattere economico proviene da fonti pubbliche (Capitolo 2, "The Role of intelligence").

consapevolezza del rischio cui si va incontro quando si ricorre a comunicazioni intercettabili in economia è meno accentuata di quella delle autorità governative nei settori della sicurezza.

2.4.1. Impiego del fattore umano nello spionaggio

La tutela delle informazioni segrete è organizzata sempre nello stesso modo:
- solo poche controllate persone hanno accesso alle informazioni segrete
- esistono regole fisse per l'accesso a queste informazioni
- le informazioni non lasciano in genere l'ambiente protetto, o lo lasciano soltanto secondo modalità sicure o crittate. Di conseguenza, lo spionaggio organizzato mira anzitutto ad ottenere accesso alle informazioni volute, in modo diretto, tramite le **persone** (cosiddetta "human intelligence"). Può trattarsi di
    - persone infiltrate (agenti) del proprio servizio/impresa
    - persone acquisite dal settore bersaglio

Le persone reclutate lavorano per servizi/imprese stranieri per lo più per i seguenti motivi:
- adescamento sessuale
- corruzione con denaro o prestazioni pecuniarie
- concussione
- appello alle ideologie
- conferimento di un particolare significato od onore (appello all'insoddisfazione o senso d'inferiorità)

Un caso limite è costituito dalla collaborazione involontaria tramite "raggiro": i collaboratori di autorità o imprese vengono indotti a confidenze facendo appello all'orgoglio personale o a sentimenti analoghi, in situazioni apparentemente innocue (discussioni al tavolo di conferenze, in congressi specializzati, al bar dell'albergo).

Il ricorso alle persone presenta il vantaggio dell'accesso diretto alle informazioni desiderate. Esso comporta tuttavia anche svantaggi:
- il controspionaggio si concentra sempre sulle persone o sugli agenti-guida
- nel caso delle persone reclutate, i punti deboli utilizzati per acquisirle alla propria causa possono produrre un effetto "boomerang"
- le persone possono pur sempre commettere errori e finire quindi nella rete del controspionaggio.

Laddove possibile si cerca quindi di sostituire il ricorso ad agenti o persone reclutate con forme di spionaggio anonime ed indipendenti dalle persone. Ciò è particolarmente semplice nella valutazione di segnali radio di dispositivi o veicoli di rilevanza militare.

2.4.2. Analisi dei segnali elettromagnetici

La forma di spionaggio più nota al pubblico che ricorre alla tecnologia è la fotografia scattata da satellite. Oltre ad essa, vengono captati e valutati segnali elettromagnetici di ogni tipo (la cosiddetta "signal intelligence", SIGINT).

2.4.2.1. Segnali elettromagnetici non utili alla comunicazione

Determinati segnali elettromagnetici, ad esempio le trasmissioni delle stazioni radar, possono fornire in ambito militare informazioni utili in merito all'organizzazione della contraerea nemica

(cosiddetta “electronic intelligence”, ELINT). Vi sono poi le trasmissioni elettromagnetiche, che possono fornire informazioni sulla posizione di truppe, aerei, navi o sottomarini, e costituiscono una fonte preziosa per i servizi d’informazione. È altresì importante individuare i satelliti spia di altri Stati, intenti ad effettuare riprese, nonché registrare e decifrare i segnali di tali satelliti.

I segnali vengono captati da stazioni fisse, da satelliti in orbita a livelli più bassi o da satelliti SIGINT semigeostazionari. Questo settore delle attività dei servizi d’informazioni collegate ai segnali elettromagnetici costituisce una parte quantitativamente significativa delle capacità d’intercettazione dei servizi. Ma con questo non sono esaurite le possibilità di ricorrere alla tecnologia.

2.4.2.2. Analisi delle comunicazioni intercettate

I servizi d’informazione esteri di molti Stati intercettano le comunicazioni militari e diplomatiche di altri paesi. Alcuni di questi servizi sorvegliano inoltre, nella misura in cui vi abbiano accesso, le comunicazioni civili di altri Stati. In alcuni Stati, i servizi d’informazione hanno il diritto di sorvegliare anche le comunicazioni in entrata o in uscita dal proprio paese. Nelle democrazie, la sorveglianza delle comunicazioni fra i **propri** cittadini ad opera dei servizi d’informazione è soggetta a determinati controlli e disposizioni. Gli ordinamenti giuridici nazionali tutelano comunque soltanto i cittadini che si trovino nel proprio ambito territoriale (cfr. capitolo 8).

2.5. L’attività di determinati servizi d’informazione

Il dibattito pubblico si è incentrato in particolare sull’attività d’intercettazione dei servizi d’informazione statunitensi e britannici. Oggetto di diatriba è l’intercettazione e la valutazione delle comunicazioni (conversazioni, fax, e-mail). Una valutazione politica di tale attività necessita di un parametro; il parametro di riferimento scelto è l’attività d’intercettazione dei servizi d’informazione nell’ambito dell’Unione europea. La tabella 1, riportata appresso, fornisce una panoramica in merito: ne emerge che l’intercettazione delle comunicazioni private da parte dei servizi d’informazione esteri non è una peculiarità dei servizi americani o britannici.

Paese	Comunicazioni estere	Comunicazioni nazionali	Comunicazioni civili
Austria	+	+	-
Belgio	+	+	+
Danimarca	+	+	+
Finlandia	+	+	+
Francia	+	+	+
Germania	+	+	-
Grecia	-	-	-
Irlanda	+	+	+
Italia	-	-	-
Lussemburgo	+	+	+

Paesi Bassi	+	+	-
Portogallo	+	+	-
Regno Unito	+	+	+
Spagna	+	+	+
Svezia	+	+	+
USA	+	+	+
Canada	+	+	+
Australia	+	+	+
Nuova Zelanda	+	+	+

Tabella 1: Attività d'intercettazione dei servizi d'informazione nell'ambito dell'UE e negli Stati ECHELON

Legenda delle singole colonne:
Colonna 1: Paese corrispondente
Colonna 2: Intercettazione delle comunicazioni estere
Colonna 3: Intercettazione delle comunicazioni nazionali (militari, messaggi ecc.)
Colonna 4: Intercettazione delle comunicazioni civili

3. Condizioni generali di carattere tecnico per l'intercettazione delle telecomunicazioni

3.1. L'intercettabilità di diversi supporti di comunicazione

Per chi voglia comunicare ad una certa distanza è necessario un supporto di comunicazione. Può trattarsi di:

- aria (onde sonore)
- luce (segnali Morse, cavi in fibre ottiche)
- corrente elettrica (telegrafo, telefono)
- onda elettromagnetica (impulso radio nelle forme più svariate)

Chiunque quale terzo si procuri l'accesso al supporto della comunicazione, può intercettarla. L'accesso può essere agevole o difficile, possibile da qualsiasi punto o soltanto da determinate posizioni. Qui appresso vengono discussi due casi estremi: le possibilità tecniche di una spia in loco, da un lato, e le possibilità di un sistema d'intercettazione a livello mondiale, dall'altro.

3.2. Le possibilità dell'intercettazione in loco[8]

In loco può essere intercettata ogni comunicazione, se l'intercettatore è risoluto ad infrangere la legge e il soggetto intercettato non si tutela.

- Le **conversazioni** in locali possono essere intercettate tramite microfoni installati (le cosiddette cimici) o esplorando le vibrazioni dei vetri delle finestre con il laser.
- Gli **schermi** inviano radiazioni che possono essere captate sino a 30 m di distanza; ciò ne rende visibile il contenuto.
- **Telefono, telefax** ed **e-mail** possono essere intercettati se l'intercettatore si inserisce nei cavi che si diramano dall'edificio.
- Un **telefono cellulare** può essere intercettato da una distanza fino a ..... chilometri.
- La **radio aziendale** può essere intercettata entro la portata delle onde UKW.

In loco le condizioni d'utilizzo di strumenti tecnici per lo spionaggio sono ideali, in quanto le misure d'intercettazione si limitano ad una persona o ad un obiettivo e praticamente si può intercettare qualsiasi comunicazione. L'unico svantaggio è che in caso di installazione di "cimici" o di inserimento nei cavi si corre il rischio di essere scoperti.

3.3. Le possibilità di un sistema d'intercettazione che funzioni a livello mondiale

Oggigiorno, per le comunicazioni intercontinentali vi sono vari supporti per tutti i tipi di comunicazione (conversazioni, fax e dati). Le possibilità di un sistema d'intercettazione che funzioni a livello mondiale sono limitate da due fattori:

[8] Manfred Fink, Lauschziel Wirtschaft – Abhörgefahren und –techniken, Vorbeugung und Abwehr, Richard Boorberg Verlag, Stoccarda 1996.

- la limitata accessibilità al supporto di comunicazione
- la necessità di filtrare le comunicazioni pertinenti dall'enorme volume di comunicazioni in corso.

3.3.1. Accesso ai supporti di comunicazione

3.3.1.1. Comunicazione via cavo

I cavi veicolano ogni tipo di comunicazione (conversazioni, fax, e-mail, dati). La comunicazione via cavo può essere intercettata solo quando è possibile accedere al cavo; tale accesso è comunque possibile al punto terminale di un collegamento via cavo, se questo si trova sul territorio dello Stato che intercetta. A livello nazionale è quindi **tecnicamente** possibile intercettare tutti i cavi, se l'intercettazione è consentita dalla legge. Tuttavia, i servizi d'informazione esteri non hanno per lo più alcun accesso legale a cavi che si trovano sul territorio soggetto alla sovranità di altri Stati; comunque, tramite vie illegali essi possono procurarsi un accesso ad un punto specifico, correndo il grande rischio di essere scoperti.

I collegamenti intercontinentali via cavo sono realizzati, sin dall'era del telegrafo, tramite cavi sottomarini. Un accesso a tali cavi è sempre possibile nel punto in cui fuoriescono dall'acqua. Qualora diversi Stati cooperino nell'ambito di un'unione d'intercettazione, si ha un accesso a tutti i punti terminali dei collegamenti via cavo che percorrono questi paesi. Ciò si è rivelato di portata storica in quanto sia i cavi telegrafici sottomarini sia i primi cavi coassiali telefonici sottomarini tra l'Europa e l'America emergevano in superficie a Terranova (territorio canadese) ed i collegamenti con l'Asia attraversavano l'Australia, poiché erano necessari ripetitori intermedi. Oggigiorno, i cavi in fibre ottiche vengono posati sotto il livello del mare, trascurando i rilievi orografici, e i ripetitori intermedi sul percorso diretto, senza tappe intermedie in Australia o Nuova Zelanda.
Sui cavi elettrici è possibile inserirsi anche tramite induzione (ossia, elettromagneticamente con una bobina annessa al cavo) fra i punti terminali di un collegamento senza creare un collegamento elettrico diretto. Ciò è possibile, con notevole dispendio, anche in caso di cavi elettrici sottomarini, operando da sommergibili. Questa tecnica è stata utilizzata dagli USA per allacciarsi ad un determinato cavo sottomarino dell'URSS, tramite il quale venivano trasmessi ordini non cifrati ai sommergibili atomici sovietici. Un utilizzo estensivo di questa tecnica è proibitivo, non fosse altro che per motivi di costi.

Nei cavi in fibre ottiche della vecchia generazione utilizzati attualmente è possibile realizzare un allacciamento induttivo solo nei ripetitori intermedi. In tali ripetitori, il segnale ottico viene trasformato in segnale elettrico, che si amplifica e poi viene di nuovo trasformato in segnale ottico. Si tratta comunque di capire in quale modo trasmettere gli enormi quantitativi di dati, veicolati da tale cavo, dal luogo d'intercettazione al luogo di valutazione senza ricorrere ad un proprio cavo in fibre ottiche. L'impiego di un sommergibile con a bordo una dotazione di analisi è contemplabile soltanto in rarissimi casi, ad esempio in guerra, per l'intercettazione di comunicazioni militari strategiche del nemico. Il relatore non ritiene che il sommergibile sia adatto alla normale sorveglianza delle comunicazioni internazionali. I cavi in fibre ottiche della nuova generazione utilizzano come ripetitore intermedio il laser all'erbio, ma un collegamento elettromagnetico per l'intercettazione a questi ripetitori non è più possibile. Tali cavi possono quindi essere oggetto d'intercettazione soltanto in corrispondenza dei punti terminali del collegamento.

Sotto il profilo pratico, ciò significa, per l'unione d'intercettazione dei cosiddetti **Stati ECHELON,** che essi possono intercettare, con un dispendio di risorse sostenibile, solo in corrispondenza dei punti terminali dei cavi sottomarini che si trovano sul loro territorio. Sostanzialmente, essi possono quindi captare soltanto le comunicazioni via cavo in entrata o in uscita dal loro paese. Questo significa che il loro accesso alle comunicazioni via cavo ricevute o trasmesse dal paese, **in Europa** si limita al **territorio del Regno Unito**. Infatti, le comunicazioni nazionali si effettuano sinora per lo più sulla rete via cavo nazionale; con la privatizzazione delle telecomunicazioni vi possono essere eccezioni, ma sono parziali e non prevedibili.

Ciò vale perlomeno per telefono e telefax; per le comunicazioni via cavo tramite Internet valgono altre condizioni-quadro. Riassumendo, ci si può limitare a quanto di seguito riportato:

- La comunicazione via Internet avviene tramite pacchetti di dati, per cui i pacchetti inviati ad un destinatario possono prendere diverse vie nella rete.
- All'inizio dell'era di Internet venivano utilizzate nicchie libere della rete scientifica pubblica per la trasmissione di e-mail. Il percorso di un'informazione era quindi del tutto imprevedibile, ed i singoli pacchetti percorrevano vie caotiche e non predefinibili. All'epoca il più importante collegamento internazionale era la "spina dorsale scientifica" tra Europa ed America.
- Alla commercializzazione di Internet ed alla creazione degli "Internet provider" (fornitori di servizi di connessione ad Internet) ha fatto seguito una commercializzazione della rete. Gli "Internet provider" gestiscono o noleggiano reti proprie. Essi hanno quindi cercato di mantenere sempre più le comunicazioni nell'ambito della propria rete per evitare il pagamento di commissioni d'utilizzo ad altri partecipanti alla rete. Di conseguenza, il percorso di un pacchetto di dati all'interno della rete non è oggi determinato esclusivamente dal suo carico, ma anche da considerazioni di costi.
- Una e-mail inviata dal cliente di un "provider" a quello di un altro "provider" rimane generalmente all'interno della rete dell'impresa, anche quando non si tratta della via più rapida. I computer che decidono del trasporto di pacchetti di dati, posizionati in corrispondenza dei nodi della rete (cosiddetti "router") organizzano il passaggio ad altre reti, in determinati punti di transito (cosiddetti "switch").
- All'epoca della spina dorsale scientifica gli "switch" della comunicazione globale via Internet si trovavano negli USA. Di conseguenza, i servizi d'informazione del paese potevano accedere ad una parte rilevante delle comunicazioni europee via Internet. Oggi, per contro, solo una parte limitata delle comunicazioni interne europee via Internet avviene tramite gli Stati Uniti.
- Una parte ridotta delle comunicazioni interne europee avviene tramite uno "switch" a Londra, cui ha accesso il servizio d'informazione britannico GCHQ. La parte preponderante delle comunicazioni non lascia il continente europeo: ad esempio, oltre il 95% delle comunicazioni tedesche via Internet avviene tramite uno "switch" a Francoforte.

In pratica questo significa che gli Stati ECHELON possono accedere solo ad una **parte estremamente limitata** della comunicazione di Internet via cavo.

3.3.1.2. Comunicazione via radio[9]

L'intercettabilità della comunicazione via radio dipende dalla portata delle onde elettromagnetiche utilizzate. Se le onde radio emesse corrono lungo la superficie terrestre (cosiddette **onde dirette**), la loro portata è limitata e dipende dalla struttura del terreno, dalle costruzioni e dalla vegetazione; se invece tali onde si muovono in direzione dello spazio (cosiddette **onde indirette)**, possono superare considerevoli distanze, in seguito alla riflessione contro gli strati della ionosfera. Le riflessioni molteplici ampliano considerevolmente la portata.

La portata dipende dalla lunghezza d'onda:

- Le onde lunghissime e lunghe (3kHz – 300kHz) si diffondono soltanto lungo l'onda diretta, in quanto l'onda indiretta non viene riflessa. Esse hanno una portata ridotta.
- Le onde medie (300kHz-3 MHz) si diffondono lungo l'onda diretta e, di notte, anche lungo l'onda indiretta; hanno una portata intermedia.
- Le onde corte (3MHz-30 MHz) si diffondono per lo più lungo l'onda indiretta e consentono, per via delle riflessioni molteplici, una ricezione **che avvolge il globo**.
- Le onde ultracorte (30 MHz-300MHz) si diffondono soltanto come onde dirette, perché le onde indirette non vengono riflesse. Si diffondono in modo relativamente rettilineo come la luce, per cui la loro portata, a causa della curvatura terrestre, dipende dall'altezza delle antenne di trasmettitore e ricevitore. A seconda delle prestazioni, esse hanno una portata sino a circa 100 km (circa 30 km per i telefoni cellulari).
- Le onde decimetriche e centimetriche (30MHz-30 GHz) si diffondono, ancor più delle onde ultracorte, in modo quasi-ottico. Si possono raggruppare facilmente e consentono quindi trasmissioni orientate con poco dispendio (ponti radio collegati a terra). Possono essere captate soltanto con un'antenna che si trovi nell'immediata prossimità del ponte radio e sia ad esso parallela o si trovi sul percorso stesso o sul suo prolungamento.

Le onde lunghe e medie vengono utilizzate soltanto per emittenti radio, radiofari ecc. Le comunicazioni militari e civili via radio utilizzano le onde corte e soprattutto le onde ultracorte e decimetriche/centimetriche.

Dalle precedenti osservazioni emerge che un sistema d'intercettazione che funzioni globalmente per le comunicazioni può avere accesso soltanto alle comunicazioni su onde corte. Per tutti gli altri tipi di comunicazioni via radio, la stazione d'intercettazione deve essere a una distanza pari o inferiore a 100 chilometri (ad esempio su un'imbarcazione, in un'ambasciata).

In pratica questo significa che gli Stati ECHELON possono accedere solo ad una parte estremamente limitata della comunicazione via radio.

3.3.1.3. Comunicazione tramite satelliti geostazionari per telecomunicazioni[10]

Le onde decimetriche e centimetriche, come indicato in precedenza, si raggruppano molto facilmente in ponti radio. Se si costruisce un ponte radio verso un satellite di comunicazione stazionario collocato ad una notevole altezza, che riceva, converta e rinvii a terra il segnale radio, si possono coprire grandi distanze senza utilizzare cavi. La portata di tale collegamento è limitata soltanto dal fatto che il satellite non può ricevere e trasmettere intorno al globo terrestre. Di

[9] U. Freyer, Nachrichtenübertragungstechnik, Hanser Verlag 2000.

[10] Hans Dodel, Satellitenkommunikation, Hüthig Verlag 1999

conseguenza, per la copertura a livello globale si utilizzano più satelliti (cfr. capitolo 4). Se gli Stati ECHELON gestiscono stazioni d'intercettazione nelle regioni del globo pertinenti, in linea di massima possono intercettare tutte le comunicazioni via telefono e fax e tutti i flussi di dati veicolate tramite questi satelliti.

3.3.1.4. Possibilità d'intercettare da aerei e navi

È risaputo da tempo che aerei speciali del tipo AWACS vengono utilizzati per individuare a distanza altri velivoli. Il radar di questi apparecchi viene azionato da un sistema computerizzato di rilevamento per l'identificazione di bersagli riconosciuti, in grado di rilevare, classificare e correlare con contatti radar le radiazioni elettroniche. Non è disponibile un sistema SIGINT separato.[11] Per contro, l'aereo spia a volo lento EP-3 della US-Navy dispone di possibilità d'intercettazione per microonde, onde corte ed ultracorte. I segnali vengono analizzati direttamente a bordo, e l'aereo viene utilizzato a scopi esclusivamente militari.[12]

Inoltre, per l'intercettazione delle comunicazioni militari via radio si ricorre anche a navi di superficie e sottomarini destinati all'uso in prossimità della terraferma.[13]

3.3.1.5. Possibilità d'intercettare da satelliti spia

Fintantoché non sono collegate alle antenne corrispondenti, le onde radio vengono emesse in tutte le direzioni, quindi anche nello spazio. I satelliti di "signal intelligence" posizionati su orbite basse possono captare i relativi trasmettitori da individuare solo per pochi minuti. Nelle aree ad elevata concentrazione demografica e fortemente industrializzate, l'intercettazione è resa difficile dall'alta densità di trasmettitori della medesima frequenza, per cui è pressoché impossibile filtrare i singoli segnali.[14] Questi satelliti non sono adatti alla sorveglianza continua della comunicazione civile via radio.
Vi sono inoltre i cosiddetti satelliti quasi-stazionari SIGINT degli USA, posizionati in altitudine (42000km).[15] Diversamente dai satelliti di comunicazione geostazionari, essi hanno un'inclinazione che varia dai 3 ai 10 gradi, un apogeo compreso tra 39000 e 42000 km ed un perigeo compreso tra 30000 e 33000 km. I satelliti non sono quindi immobili in orbita, ma si muovono su un'orbita ellittica complessa. Di conseguenza, nel corso della giornata essi coprono una regione più vasta e consentono di scandagliare le sorgenti radio. Tutto ciò, e le caratteristiche accessibili al pubblico dei satelliti, denotano un utilizzo puramente militare.
I segnali ricevuti vengono trasmessi alla stazione ricevente con una tratta di discesa fortemente connessa ad un punto, a 24 GHz.

3.3.2. Possibilità di analisi automatica delle comunicazioni intercettate: l'utilizzo di filtri

In caso di intercettazione di comunicazioni estere non si sorveglia in modo mirato un collegamento telefonico. Si procede piuttosto ad intercettare tutta o parte della comunicazione

[11] Lettera del Segretario di Stato presso il ministero federale della Difesa Walter Kolbow del 14.2.2001.

[12] Süddeutsche Zeitung n. 80, del 5.4.2001, pag. 6.

[13] Jeffrey T. Richelson, The U.S. Intelligence Community, Ballinger, New York 1989, pagg. 188, 190.

[14] Lettera del Segretario di Stato preso il ministero federale della Difesa Walter Kolbow del 14.2.2001.

[15] Maggiore Andronov, Zarubezhnoye voyennoye obozreniye, n.12, 1993, pagg. 37-43.

che avviene tramite il satellite o il cavo sorvegliato, e a filtrarla con l'ausilio di computer e di concetti chiave. Di fatto, la valutazione dell'intera comunicazione captata è del tutto impossibile.

Filtrare le comunicazioni lungo determinati collegamenti è semplice. Con concetti chiave si possono anche elaborare in modo specifico telefax e messaggi di posta elettronica. Anche una determinata voce può essere captata, se il sistema è addestrato a riconoscere le voci.[16] Per contro, il riconoscimento automatico di parole pronunciate da una qualsiasi voce non è ancora possibile, stando a quanto è a conoscenza del relatore. Le possibilità di filtrare le comunicazioni sono inoltre limitate anche da altri fattori: la ridotta capacità dei computer, i problemi linguistici e soprattutto il numero esiguo di addetti all'analisi che possano leggere e valutare le notizie cifrate.

Nella valutazione delle possibilità dei sistemi per filtrare le comunicazioni si deve anche tener conto del fatto che le piene possibilità tecniche di tale sistema d'intercettazione, che funziona secondo il principio dell'"aspiratore", si ripartiscono su diverse temi. Parte delle parole chiave riguarda la sicurezza militare, parte il traffico di droga ed altre forme di criminalità internazionale, parte il mondo del commercio con i beni a duplice uso e parte il rispetto di un embargo. Alcuni concetti chiave riguardano anche l'economia, il che significa che le potenzialità del sistema si suddividono fra più settori. Una limitazione delle parole chiave ai settori rilevanti sotto il profilo economico sarebbe in conflitto con le esigenze della leadership politica dei servizi, e non si è mai verificata dalla fine della Guerra Fredda.[17]

3.3.3. L'esempio del servizio d'informazione federale tedesco

Il Dipartimento n. 2 del servizio d'informazione federale tedesco fornisce informazioni intercettando comunicazioni estere: tale attività è stata oggetto di una verifica da parte della Corte costituzionale tedesca. I dettagli resi pubblici nel corso del processo[18], insieme alle affermazioni rese dinanzi alla commissione ECHELON il 21.11.2000 dal coordinatore per i servizi segreti presso la Cancelleria federale Ernst Uhrlau, forniscono una panoramica delle potenzialità dei servizi d'informazione nell'intercettazione delle comunicazioni via satellite.

Può essere che nei dettagli le possibilità di altri servizi d'informazione, tenendo conto del loro diritto d'accesso alle comunicazioni via cavo o del maggior numero di analisti, siano anche più elevate. In particolare, tenendo conto del traffico via cavo aumenta la probabilità statistica, ma non necessariamente il numero di traffici valutabili. Sostanzialmente, l'esempio del BND chiarisce al relatore in modo esemplare quali sono le possibilità e le strategie di cui dispongono i servizi d'informazione esteri nell'intercettazione delle comunicazioni, anche quando non le espongono apertamente.

Il servizio d'informazione federale tenta, tramite il controllo **strategico** delle telecomunicazioni, di procurarsi informazioni dall'estero e sull'estero. A tal fine, si intercettano le comunicazioni via satellite con una serie di concetti chiave per la ricerca (che in Germania devono essere autorizzati preventivamente dalla cosiddetta commissione G10[19]). I flussi si strutturano come segue (dati dell'anno 2000): dei circa 10 milioni di comunicazioni internazionali/giorno da e

[16] Comunicazione privata al relatore, fonte riservata.

[17] Comunicazione privata al relatore, fonte riservata.

[18] BverfG, 1 BvR 2226/94 del 14.7.1999, paragrafo 1.

[19] Gesetz zur Beschränkung des Brief-,Post- und Fernmeldegeheimnisses (Legge sulla limitazione del segreto epistolare, postale e nelle telecomunicazioni) (Legge sull'articolo 10 GG.) del 13.8.1968.

verso la Germania, circa 800 000 avvengono tramite satellite; appena il 10% di queste (75 000) viene filtrato da un motore di ricerca. Secondo il relatore, questa limitazione non deriva dalla legge (teoricamente, almeno prima del processo dinanzi alla Corte costituzionale, sarebbe stato consentito il 100%), ma da altre restrizioni di carattere tecnico, ad esempio la ridotta capacità d'analisi.

Anche il numero dei concetti-chiave gestibili è limitato tecnicamente e con riserva d'autorizzazione. Nella motivazione della sentenza della Corte costituzionale, oltre ai concetti meramente formali (collegamenti di stranieri o imprese straniere all'estero), si riportano 2 000 concetti in materia di proliferazione, 1 000 in materia di commercio di armamenti, 500 in materia di terrorismo e 400 in materia di narcotraffico. Per il terrorismo ed il narcotraffico, tuttavia, la procedura non si è rivelata particolarmente fruttuosa.

Il motore di ricerca verifica se i telefax e i telex contengono concetti autorizzati. Un sistema di riconoscimento automatico delle parole non è attualmente possibile nei collegamenti vocali. Se i concetti non vengono reperiti, le richieste vengano automaticamente cestinate: non possono essere valutate in quanto non sussiste la base giuridica per farlo. Quotidianamente, si hanno circa 5 comunicazioni di utenti delle telecomunicazioni che rientrano nella tutela accordata dalla Costituzione tedesca. La linea strategica del servizio d'informazione federale consiste nel trovare i tasselli del mosaico quali punti d'appoggio per ulteriori chiarimenti: esso non si prefigge assolutamente la sorveglianza assoluta delle comunicazioni estere. Secondo gli elementi a disposizione del relatore, ciò vale anche per l'attività di SIGINT di altri servizi d'informazione esteri.

4. La tecnica della comunicazione via satellite

4.1. Il ruolo dei satelliti per le comunicazioni

Attualmente i satelliti per le comunicazioni costituiscono un elemento irrinunciabile della rete globale di telecomunicazioni e della diffusione di programmi televisivi e radiofonici nonché di servizi multimediali. Tuttavia, negli scorsi anni, nell'Europa centrale la quota del traffico via satellite sulle comunicazioni internazionali si è fortemente ridotta, sino a scendere, in alcune regioni, addirittura al disotto del 10%[20]. Ciò è dovuto ai vantaggi offerti dai cavi in fibre ottiche, che possono assorbire molto più traffico, con una maggiore qualità di collegamento.

Oggi le comunicazioni avvengono per via digitale anche in ambito vocale. La capacità dei collegamenti digitali via satellite si limita, per ogni trasponditore di satellite, a **1890** canali vocali con standard ISDN (64 kbits/sec). Per contro, su un'unica fibra ottica possono essere trasmessi, oggi, ben **241920** canali vocali con il medesimo standard. Ciò corrisponde ad un rapporto di **1:128**!

A ciò si aggiunga che la qualità dei collegamenti via satellite è inferiore a quella tramite cavi marini in fibre ottiche. Le perdite in termini di qualità, dovute ai lunghi tempi di transito dei segnali - varie centinaia di millisecondi - sono pressoché impercettibili in una normale trasmissione vocale, anche se sono udibili. Nei collegamenti via fax e negli scambi di dati che avvengono tramite una complessa "procedura handshaking", il cavo presenta chiari vantaggi quanto alla sicurezza del collegamento. Tuttavia, al contempo solo il 15% della popolazione mondiale è connessa alla rete globale via cavo[21].

Per determinate applicazioni, i sistemi satellitari sono quindi, a lungo termine, più vantaggiosi dei cavi. Alcuni esempi in ambito civile:

- Comunicazioni telefoniche e scambi di dati nazionali, regionali ed internazionali nelle aree con scarso flusso di comunicazioni, ossia laddove non varrebbe la pena attuare un collegamento via cavo, per mancanza di saturazione.
- Comunicazioni limitate nel tempo in caso di catastrofi, rappresentazioni, cantieri ecc.
- Missioni ONU in regioni con infrastruttura per le comunicazioni non adeguatamente sviluppata.
- Comunicazione economica flessibile/mobile con microstazioni radio di terra (V-SAT, cfr. *infra*).

Questo spettro d'utilizzo dei satelliti nel campo delle comunicazioni è dovuto alle seguenti caratteristiche: l'irraggiamento di un unico satellite geostazionario può coprire quasi il 50% della superficie terrestre, anche le zone impraticabili. In questa regione viene coperto il 100% degli utenti, su terra, mare o nell'aria. I satelliti sono operativi in pochi mesi, indipendentemente dall'infrastruttura della località, sono più affidabili dei cavi e possono essere eliminati con meno dispendio.

[20] Cfr. la motivazione per la modifica della legge G10 in Germania.

[21] Homepage della Deutsche Telekom: www.detesat.com/deutsch/.

Vanno considerate negative le seguenti caratteristiche della comunicazione via satellite: i tempi di transito del segnale relativamente lunghi; la degradazione di propagazione; la durata di vita di 12-15 anni, inferiore a quella del cavo; la maggiore vulnerabilità nonché la facile intercettabilità.

4.2. Funzionamento di un collegamento via satellite

Le microonde, come già indicato in precedenza (cfr. capitolo 3), si raggruppano bene con le antenne corrispondenti: perciò si possono sostituire i cavi con ponti radio. Se le antenne di trasmissione e di ricezione non si situano sullo stesso livello, ma, come nel caso del globo terrestre, sulla superficie di una collina, l'antenna di ricezione "sparisce" dall'orizzonte, a causa della curvatura, a partire da una determinata distanza. Entrambe le antenne, a questo punto, non si "vedono" più: ciò accadrebbe, ad esempio, anche ad un ponte radio intercontinentale fra Europa ed USA. Le antenne dovrebbero situarsi su pilastri alti 1,8 km, in modo da poter creare un collegamento: ciò basta a rendere inattuabile tale ponte radio intercontinentale, a prescindere dall'attenuazione del segnale, a causa dell'aria e del vapore, lungo il percorso. Qualora si dovesse invece riuscire a creare nello spazio, a notevole altezza, una sorta di specchio in una "posizione fissa" per il ponte radio, si potrebbero superare, nonostante la curvatura terrestre, notevoli distanze, proprio come uno specchietto retrovisore consente di vedere dietro l'angolo. Il principio appena descritto viene realizzato con l'utilizzo dei cosiddetti satelliti geostazionari.

4.2.1. Satelliti geostazionari

Se un satellite, parallelamente all'Equatore, effettua in 24 ore un'orbita circolare intorno alla Terra, segue esattamente la rotazione del nostro pianeta. Visto dalla superficie terrestre, esso è immobile a 36 000 km di altezza – ha una posizione **geostazionaria**. La maggior parte dei satelliti per le comunicazioni e televisivi rientrano in questa categoria.

4.2.2. Il percorso del segnale in un collegamento per le comunicazioni via satellite

La trasmissione dei segnali via satellite si può descrivere nel modo riportato di seguito.

Il segnale proveniente da una linea viene inviato al satellite da una stazione radio di terra con un'antenna parabolica, attraverso un ponte radio rivolto verso l'alto, il cosiddetto **uplink**. Il satellite riceve il segnale, lo amplifica e lo rinvia attraverso un ponte radio rivolto verso il basso, il cosiddetto **downlink,** ad un'altra stazione radio di terra. Da quest'ultima, il segnale torna ad una rete cablata.

In caso di comunicazione mobile, il segnale viene trasmesso direttamente dall'unità mobile di comunicazione al satellite, da dove, tramite una stazione radio di terra, può essere nuovamente immesso in una linea, o essere direttamente ritrasmesso ad un'altra unità mobile.

4.2.3. I più importanti sistemi di comunicazione via satellite esistenti

La comunicazione proveniente dalle **reti cablate accessibili al pubblico** (non necessariamente statali) viene eventualmente trasmessa tramite sistemi satellitari di diversa ampiezza da e verso stazioni radio di terra in posizioni fisse, e viene poi nuovamente immessa nella rete cablata. Si distinguono sistemi satellitari:

- globali (ad esempio INTELSAT)

- regionali (continentali) (ad esempio EUTELSAT)

- nazionali (ad esempio ITALSAT)

La maggior parte di questi satelliti si trova in una posizione geostazionaria; a livello mondiale, 120 società private gestiscono circa 1000 satelliti[22].

Inoltre, per i paesi dell'estremo Nord vi sono satelliti dotati di un'orbita speciale ad elevata eccentricità (orbite russe di Molnyia), in cui i satelliti sono visibili all'utente nell'estremo Nord per la metà del tempo di rotazione. Con due satelliti si ottiene quindi una copertura regionale, non attuabile da una posizione geostazionaria sopra l'Equatore.

Inoltre, con il sistema INMARSAT che funziona globalmente vi è un **sistema di comunicazione mobile**, creato inizialmente per l'utilizzo in mare, con cui si possono realizzare in tutto il mondo comunicazioni via satellite. Detto sistema funziona anche con satelliti geostazionari.

Il sistema satellitare che opera a livello mondiale, sulla base di diversi satelliti situati in orbite inferiori con sfasamento temporale, noto come IRIDIUM ha smesso di recente di funzionare per motivi economici, per mancanza di saturazione.

Esiste inoltre un mercato in rapida evoluzione per i cosiddetti collegamenti VSAT (VSAT = very small aperture terminal). Si tratta di microstazioni radio di terra, con antenne di diametro compreso fra 0,9 e 3,7 m, utilizzate dalle aziende per esigenze specifiche (ad esempio videoconferenze) o da fornitori di servizi mobili per esigenze di collegamento limitate nel tempo (ad esempio riunioni). Nel 1996 erano attive nel mondo 200 000 microstazioni radio di terra. La Volkswagen AG gestisce 3 000 unità VSAT, la Renault 4 000, la General Motors 100 000 e la maggiore impresa europea di oli minerali 12 000. La comunicazione è libera se non è il cliente stesso a cifrarla[23].

4.2.3.1. Sistemi satellitari globali

Questi sistemi satellitari coprono l'intero globo grazie al posizionamento di vari satelliti nella zona atlantica, indiana e pacifica.

INTELSAT[24]

INTELSAT (International Telecomunications Satellite Organisation) è stata fondata nel 1964 quale autorità dotata di una struttura organizzativa analoga a quella delle Nazioni Unite e con l'obiettivo di gestire comunicazioni internazionali. Ne facevano parte gli operatori postali nazionali statali; oggi sono membri di INTELSAT 144 governi. Nel 2001 INTELSAT verrà privatizzata.

Nel frattempo INTELSAT gestisce una flotta di 19 satelliti geostazionari, che collegano oltre 200 paesi, di cui affitta le prestazioni ai propri membri, i quali gestiscono le proprie stazioni di

[22] G. Thaller, Satelliten im Erdorbit, Franzisverlag, Monaco 1999.

[23] H. Dodel, comunicazione privata.

[24] INTELSAT-Homepage http://www.intelsat.com

terra. Dal 1984 il Business Service (BS) di INTELSAT permette anche ai non membri (ad esempio società telefoniche, grandi imprese, multinazionali) di utilizzare i satelliti. INTELSAT offre, a livello globale, servizi in diversi settori quali la comunicazione, la televisione ecc. La trasmissione delle telecomunicazioni avviene in banda C e Ku (cfr. *infra*).

I satelliti INTELSAT sono i più importanti satelliti di comunicazione internazionali, che consentono la trasmissione della maggior parte delle comunicazioni internazionali via satellite.

I satelliti coprono la zona dell'Oceano atlantico, indiano e pacifico (cfr. tabella, capitolo 5, 5.3).

Sopra l'Oceano Atlantico ci sono 10 satelliti fra i 304° E e i 359° E, sopra l'Oceano Indiano 6 satelliti fra i 62° E e i 110,5° E, sopra l'Oceano Pacifico 3 satelliti fra i 174° E e i 180° E. L'intenso traffico sull'area atlantica è coperto da diversi satelliti singoli.

INTERSPUTNIK[25]

Nel 1971 9 paesi fondarono l'organizzazione internazionale di comunicazione via satellite INTERSPUTNIK, agenzia dell'ex Unione Sovietica, con un compito analogo a quello di INTELSAT. Oggi INTERSPUTNIK è un'organizzazione intergovernativa i cui membri possono essere governi di uno Stato: essa annovera 24 membri (fra cui la Germania) e circa 40 utenti (fra l'altro Francia e Gran Bretagna), rappresentati dalle loro amministrazioni postali o Telecom. Ha sede a Mosca.

La trasmissione delle telecomunicazioni avviene in banda C e Ku (cfr. *infra*).

I satelliti (Gorizont, Express, Express A della Federazione russa e LMI-1 dell'impresa comune Lockhead-Martin) coprono altresì l'intero globo: nell'area atlantica vi è 1 satellite, e ne è previsto un secondo; nell'area indiana vi sono 3 satelliti; nell'area del Pacifico ve ne sono 2 (cfr. tabella, capitolo 5, 5.3).

INMARSAT

INMARSAT (Interim International Maritime Satellite) mette a disposizione dal 1979, con un sistema satellitare, comunicazioni **mobili** a livello mondiale via mare, aria e terra, nonché un sistema di emergenza radio. INMARSAT è nata da un'iniziativa della "International Maritime Organisation" quale organizzazione internazionale; nel frattempo, è stata privatizzata. Ha sede a Londra.

Il sistema INMARSAT è formato da nove satelliti in orbite geostazionarie. Quattro di essi, appartenenti alla generazione INMARSAT-III, coprono l'intero globo sino ai territori estremi dei Poli. Ogni singolo satellite copre circa 1/3 della superficie terrestre; il loro posizionamento nelle quattro regioni oceaniche (Atlantico occidentale, Atlantico orientale, Pacifico, Indiano) consente una copertura totale. Nel contempo, ogni INMARSAT presenta anche un certo numero di "spot-beam", che consentono il raggruppamento di energia in aree con un flusso di comunicazioni più intenso.

La trasmissione delle telecomunicazioni avviene in banda L e Ku (cfr. *infra*).

[25] Homepage di INTERSPUTNIK: http://www.intersputnik.com.

4.2.3.2. Sistemi satellitari regionali

Le zone di copertura dei sistemi satellitari regionali coprono singole regioni/continenti. Di conseguenza, le comunicazioni trasmesse tramite essi possono essere ricevute soltanto all'interno di queste regioni.

EUTELSAT[26]

EUTELSAT è stata fondata nel 1977 da 17 amministrazioni postali europee, con l'obiettivo di soddisfare le esigenze specifiche dell'Europa nell'ambito della comunicazione satellitare e di appoggiare l'industria spaziale europea. Ha sede a Parigi e circa 40 Stati membri. Nel 2001 EUTELSAT sarà privatizzata.

EUTELSAT gestisce 18 satelliti geostazionari, che coprono l'Europa, l'Africa e gran parte dell'Asia, e consentono il collegamento con l'America. I satelliti si situano fra i 12,5° O e i 48°E. EUTELSAT offre per lo più collegamenti televisivi (850 canali digitali ed analogici) e radiofonici (520 canali), ma serve anche alla comunicazione, soprattutto in ambito europeo (ivi inclusa la Russia): ad esempio, per videoconferenze, reti private di grandi imprese (fra l'altro, General Motors, Fiat), agenzie di stampa (Reuters, AFP), operatori di dati finanziari nonché servizi mobili di trasmissione dati.

La trasmissione delle telecomunicazioni avviene in banda Ku.

ARABSAT[27]

ARABSAT è l'equivalente di EUTELSAT nel mondo arabo, ed è stata fondata nel 1976: ne sono membri 21 paesi arabi. I satelliti ARABSAT vengono utilizzati sia per la trasmissione televisiva che per la comunicazione.

La trasmissione delle telecomunicazioni avviene per lo più in banda C.

PALAPA[28]

Il sistema indonesiano PALAPA è attivo dal 1995 ed è l'equivalente di EUTELSAT nel Sud-Est asiatico. La sua zona di copertura comprende Malesia, Cina, Giappone, India, Pakistan ed altri paesi della regione.

La trasmissione delle telecomunicazioni avviene in banda C e Ku.

4.2.3.3. Sistemi satellitari nazionali[29]

Molti Stati, per soddisfare le esigenze nazionali, utilizzano propri sistemi satellitari con zone di copertura limitate.

Il satellite di comunicazione francese **TELECOM** serve fra l'altro a collegare con la madrepatria i dipartimenti francesi di Africa e Sudamerica. La trasmissione delle telecomunicazioni avviene in banda C e Ku.

---

[26] Homepage di EUTELSAT: http://www.com.

[27] Homepage di ARABSAT: http://www.arabsat.

[28] H.Dodel, Satellitenkommunikation, Hüthigverlag 1999.

[29] H.Dodel e ricerche su Internet.

ITALSAT gestisce satelliti di comunicazione, che coprono l'intera penisola italiana con zone di copertura adiacenti e delimitate. Lo si riceve quindi soltanto in Italia. La trasmissione delle telecomunicazioni avviene in banda Ku.

AMOS è un satellite israeliano destinato principalmente alla comunicazione in loco, la cui zona di copertura ("footprint") copre il Medio Oriente. La trasmissione delle telecomunicazioni avviene in banda Ku.

I satelliti spagnoli HISPASAT coprono Spagna e Portogallo (Ku-Spot) e veicolano i programmi televisivi spagnoli verso il Nordamerica e il Sudamerica.

4.2.4. Ripartizione delle frequenze

Per la ripartizione delle frequenze è competente l'Unione internazionale delle telecomunicazioni. Per motivi logistici, si è suddiviso il globo in tre regioni, ai fini delle comunicazioni via radio:

1. Europa, Africa, ex Unione Sovietica, Mongolia

2. Nordamerica e Sudamerica nonché Groenlandia

3. Asia, esclusi i paesi della regione 1, Australia e Pacifico del Sud

Questa suddivisione acquisita storicamente è stata adottata ai fini della comunicazione satellitare e porta ad un accumulo di satelliti in determinate zone geostazionarie.

Le principali bande di frequenza per la comunicazione via satellite sono:

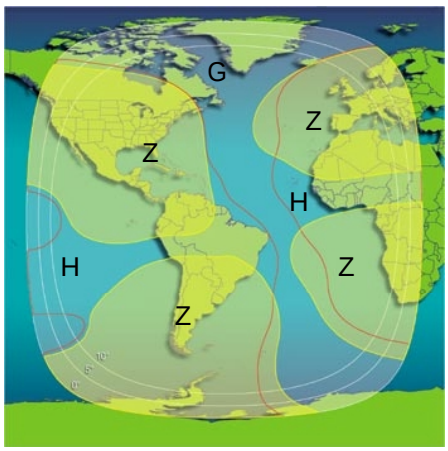
- banda L (0,4 - 1,6 GHz) per la comunicazione satellitare mobile, ad es. tramite INMARSAT
- banda C (3,6 - 6,6 GHz) per stazioni radio di terra, ad es. tramite INTELSAT
- banda Ku (10 - 20GHz) per stazioni radio di terra, ad es. INTELSAT-Ku-Spot ed EUTELSAT
- banda Ka (20 - 46 GHz) per stazioni radio di terra, ad es. tramite satelliti nazionali come ITALSAT
- banda V (46 - 56 GHz) per microstazioni radio di terra (V-SAT).

4.2.5. Zone di copertura dei satelliti (footprint)

Per zona di copertura o "footprint" si intende la zona della Terra illuminata dall'antenna del satellite: può estendersi sino al 50% della superficie terrestre oppure essere limitata, a seguito del raggruppamento dei segnali, a piccoli "spot" a livello regionale.

Quanto più è elevata la frequenza del segnale irradiato, tanto più si può raggruppare, e tanto più si riduce, di conseguenza, la zona di copertura. Il raggruppamento del segnale satellite irradiato in zone di copertura più minore estensione consente di aumentare la capacità del segnale. Quanto più la zona di copertura è limitata, tanto più forte può essere il segnale, e tanto più piccole le antenne di ricezione.

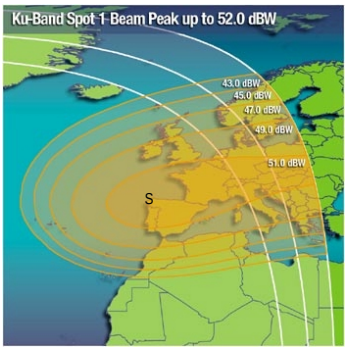
Quanto ai satelliti INTELSAT, si può illustrare brevemente questo principio come segue:

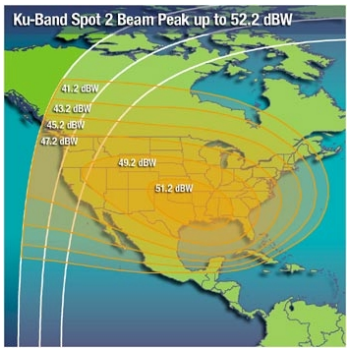


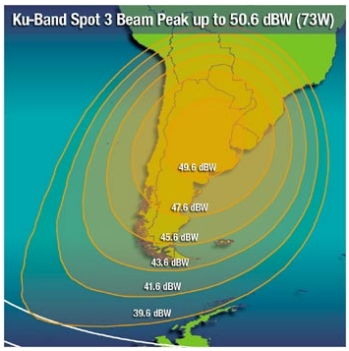
Le zone di copertura dei satelliti INTELSAT sono ripartite in diversi "beam":

Il "Global-Beam" (G) di ogni satellite copre circa un terzo della superficie terrestre.

Gli "Hemi-Beam" (H) coprono una superficie leggermente inferiore alla metà del "Global-Beam". Gli "Zone-Beam" (Z) sono "spot" in determinate zone della Terra; sono più piccoli degli Hemi-Beams. Inoltre vi sono i cosiddetti Spot-Beam, ossia piccole e precise zone di copertura o impronte (cfr. *infra*).







Le frequenze della banda C si trovano nei Global-, Hemi- e Zone-Beams. Negli Spot-Beams si trovano le frequenze della banda Ku.

4.2.6. Requisiti dimensionali per un'antenna di una stazione radio di terra

Le antenne riceventi di terra sono antenne paraboliche. Lo specchio parabolico riflette tutte le onde in entrata e le raggruppa nel suo punto focale: in tale punto si trova il sistema di ricezione vero e proprio. Maggiore è la capacità del segnale nel punto di ricezione, inferiore sarà il diametro dell'antenna parabolica.

Ai fini della ricerca condotta con questa relazione, è determinante che parte delle comunicazioni intercontinentali avvenga sulla banda C nei Global-Beam dei satelliti INTELSAT e di altri satelliti (ad es. INTERSPUTNIK), per la cui ricezione sono talvolta necessarie parabole satellitari dal diametro di circa 30 m (cfr. capitolo 5). Le antenne da 30 m erano necessarie anche per le prime stazioni d'intercettazione di satelliti per le comunicazioni, in quanto la prima generazione INTELSAT disponeva soltanto di Global-Beam e la trasmissione del segnale era molto meno sofisticata rispetto ad oggi. Queste parabole, con diametri che talvolta superano i 30 m, vengono ancora utilizzate, nelle rispettive stazioni, anche se non sono più necessarie tecnicamente.

Le antenne tipiche, che sono oggi necessarie per la comunicazione INTELSAT nella banda C, hanno un diametro che varia da 13 a 18 m. In singoli casi (ad es. per INTELSAT 511) è necessaria un'antenna di dimensioni maggiori per il Global-Beam. Nei più recenti satelliti INTELSAT, anche per il Zone-Beam della banda C, bastano antenne con un diametro fino a 5 m.

Per la ricezione della comunicazione della banda C di Intersputnik sono necessarie antenne dal diametro che varia da 2 a 25 m.

Per gli spot Ku dei satelliti INTELSAT ma anche di altri satelliti (Banda Ku di EUTELSAT, Banda Ku di AMOS ecc.) sono necessarie antenne dal diametro compreso tra 2 e 10 m.

Per le microstazioni radio di terra, che operano nella banda V ed il cui segnale può essere raggruppato maggiormente rispetto alla banda Ku, date le elevate frequenze, bastano diametri d'antenna che variano da 0,9 a 3,7 m (ad es. VSAT di EUTELSAT o INMARSAT).

5. La prova indiziale dell'esistenza di almeno un sistema globale d'intercettazione

5.1. Perché una prova indiziale

Naturalmente, i servizi segreti non espongono i dettagli del loro lavoro: non vi sono quindi dichiarazioni ufficiali dei servizi d'informazione estera degli Stati ECHELON circa il fatto che essi gestiscano congiuntamente un sistema globale d'intercettazione. Si deve quindi procedere raccogliendo il maggior numero possibile di indizi che possano fornire una prova convincente.

A questo riguardo, la catena di indizi si compone di tre elementi:

- la prova che negli Stati ECHELON i servizi d'informazione intercettano le comunicazioni private e commerciali;
- la prova che in determinate regioni della Terra, in considerazione del funzionamento del sistema satellitare di comunicazione civile, sono reperibili stazioni d'intercettazione gestite da uno degli Stati ECHELON;
- la prova che vi è un raggruppamento dei servizi d'informazione di questi Stati che va ben oltre la collaborazione consueta. Che ciò si spinga sino a far sì che i partner accettino mandati d'intercettazione e che il materiale grezzo intercettato venga loro trasmesso direttamente, senza analisi propria, è irrilevante ai fini della dimostrazione dell'esistenza di tale struttura. Questo quesito è pertinente solo qualora si vogliano chiarire i rapporti gerarchici all'interno di tale raggruppamento.

5.1.1. La prova dell'attività d'intercettazione dei servizi d'informazione esteri

Perlomeno nelle democrazie, i servizi d'informazione operano sulla base di leggi che ne descrivono scopi e/o poteri. Se ne evince agevolmente che in molti di questi Stati vi sono servizi che intercettano le comunicazioni civili: ciò vale anche per i cinque cosiddetti Stati ECHELON, che gestiscono tutti questi servizi. Per ognuno di questi Stati è superfluo addurre ulteriori prove del fatto che essi intercettano le comunicazioni in entrata e in uscita dal paese. Nelle comunicazioni via satellite, dal proprio territorio si può anche intercettare parte dei flussi di notizie destinati a riceventi all'estero: in tutti e cinque gli Stati ECHELON, ai servizi non sono frapposte limitazioni giuridiche in tal senso. Dalla logica interna del metodo di controllo strategico delle comunicazioni con l'estero e dal suo scopo, in parte pubblico, risulta inevitabile che i servizi agiscano in tal modo.[30]

5.1.2. La prova dell'esistenza di stazioni nelle aree geograficamente rilevanti

La sola limitazione al tentativo di elaborare a livello mondiale una sorveglianza della comunicazione via satellite è dovuta alla tecnica di questa comunicazione. Non vi è alcuna località da cui si possano captare **tutti** i flussi via satellite a livello mondiale (cfr. capitolo 4, 4.2.5).

Un sistema d'intercettazione globale potrebbe essere creato a tre condizioni:

[30] Il relatore dispone di informazioni circa la veridicità di quest'affermazione. La fonte è riservata.

- il gestore ha un proprio territorio statale in tutte le parti del mondo rilevanti a tal fine;
- il gestore ha, in tutte le parti del mondo rilevanti a tal fine, in parte un territorio proprio, nonché un diritto d'ospite nelle altre regioni del mondo, e può gestirvi o coutilizzare stazioni;
- il gestore è un raggruppamento di servizi d'informazione di vari Stati e gestisce il sistema nelle parti del mondo rilevanti.

Nessuno degli Stati ECHELON potrebbe gestire un sistema globale. Gli USA, perlomeno formalmente, non hanno colonie. Il Canada, l'Australia e la Nuova Zelanda, a loro volta, non esercitano alcuna sovranità territoriale al di fuori dei confini nazionali *strictu sensu*. Neppure il Regno Unito potrebbe gestire da solo un sistema globale d'intercettazione (cfr. capitolo 6).

5.1.3. La prova della stretta collaborazione fra servizi d'informazione

Viceversa, non è chiarito pubblicamente se e come gli Stati ECHELON collaborino nell'ambito dei servizi d'informazione. In genere, una collaborazione dei servizi avviene bilateralmente e sulla base dello scambio di materiale analizzato. Un raggruppamento multilaterale è già di per sé assai inconsueto; se vi si aggiunge lo scambio regolare di materiale grezzo, ne emerge una qualità del tutto nuova. L'esistenza di un raggruppamento di questo tipo può essere dimostrata soltanto con indizi.

5.2. Come riconoscere una stazione d'intercettazione per comunicazioni via satellite

5.2.1. Criterio 1: l'accessibilità dell'impianto

Gli impianti delle poste, delle radio o degli istituti di ricerca dotati di grandi antenne sono accessibili perlomeno ai visitatori su richiesta, contrariamente a quelli delle stazioni d'intercettazione. Formalmente, essi vengono per lo più gestiti da militari, che procedono all'intercettazione anche tecnicamente. Ad esempio, è il Naval Security Group (NAVSECGRU), o l'Air Intelligence Agency dell'US Airforce (AIA), a gestire la stazione per la NSA. Quanto alle stazioni britanniche, è la Royal Airforce britannica a gestire gli impianti per il servizio d'informazione nazionale GCHQ. Questo accordo consente una rigorosa sorveglianza militare dell'impianto e contribuisce nel contempo al suo occultamento.

5.2.2. Criterio 2: il tipo di antenna

Negli impianti che soddisfano il criterio 1 si possono reperire diversi tipi di antenne, la cui struttura si differenzia. La loro forma fornisce informazioni sullo scopo dell'impianto: ad esempio, si utilizzano configurazioni circolari di antenne ad asta alte, con diametro ampio (cosiddette "antenne del tessitore"), per individuare l'orientamento dei segnali radio. Analogamente, configurazioni anulari di antenne a forma di rombo (cosiddette antenne "pusher") soddisfano lo stesso obiettivo. Le antenne destinate alla ricezione da ogni direzione o le antenne direzionali, che hanno l'aspetto di antenne televisive gigantesche, servono ad intercettare segnali radio non direzionati. **Viceversa, per la ricezione di segnali satellitari si utilizzano esclusivamente antenne paraboliche**. Se le antenne paraboliche sono all'aperto, conoscendone ubicazione, inclinazione (elevazione) e angolo goniometrico (azimut) si può calcolare quale satellite viene ricevuto. Ciò sarebbe possibile a Morwenstow (Regno Unito) o a Yakima (USA) e Sugar Grove (USA). Tuttavia, le antenne paraboliche sono per lo più nascoste sotto rivestimenti

bianchi di forma rotondeggiante, i cosiddetti radomi, che servono a proteggerle e, al tempo stesso, ad occultarne l'orientamento.

Se si trovano antenne paraboliche o radomi sul terreno di una stazione d'intercettazione, senz'altro vi si captano segnali satellitari. Peraltro, non è ancora chiaro di che tipo di segnali si tratti.

5.2.3. Criterio 3: le dimensioni dell'antenna

Le antenne di ricezione satellitare in un impianto che soddisfi il criterio 1 possono essere destinate a diversi obiettivi:
- stazioni di ricezione per la comunicazione militare
- stazioni di ricezione per satelliti spia (immagini, radar)
- stazioni di ricezione per satelliti militari SIGINT
- stazioni di ricezione per l'intercettazione di satelliti per le comunicazione civili

Dall'esterno non è chiaro lo scopo delle antenne/radomi. Peraltro, vi sono misure minime prefissate tecnicamente per le antenne che siano destinate a ricevere il cosiddetto "global beam" nella banda C della comunicazione civile internazionale via satellite. Nella prima generazione di satelliti di questo tipo, erano necessarie antenne aventi un diametro di circa 25-30 m, mentre oggi bastano 15-18 m. Il filtraggio automatico dei segnali intercettati tramite computer consente una qualità del segnale ottimale, per cui, ai fini dell'intercettazione, si sceglie la grandezza d'antenna al limite superiore della gamma. Dato che le antenne sono montate su pilastri, i diametri dei radomi sono ancora superiori a quelli delle antenne.

5.2.4. Conclusioni

A conoscenza del relatore, non vi sono utilizzi militari per antenne di questa grandezza. Perciò, se le si reperisce su un terreno che soddisfa il criterio 1, si tratta dell'intercettazione di comunicazioni satellitari civili.

5.3. Riscontri accessibili al pubblico su stazioni d'intercettazione note

5.3.1. Metodi

Per appurare quali stazioni soddisfino i criteri indicati al Capitolo 5.2 e facciano parte del sistema d'intercettazione globale e quali siano i loro compiti, si sono consultati la letteratura pertinente, in parte contradditoria (Hager[31], Richelson[32], Campbell[33]), documenti derubricati[34], la

[31] Hager, Nicky: EXPOSING THE GLOBAL SURVEILLANCE SYSTEM http://www.ncoic.com/echelon1.htm
Hager, Nicky: Secret Power. New Zealands´s Role in the international Spy Network, Nuova Zelanda 1996.

[32] Richelson, Jeffrey, Desperately seeking Signals, 4 2000, The Bulletin of the Atomic Scientists, http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html
Richelson,T.Jeffrey, The U.S. Intelligence Community, Westview Press 1999.

[33] Campbell, Duncan, Sviluppo delle tecnologie di sorveglianza e rischio di impiego abusivo di informazioni economiche, Vol 2/5, 10 1999, STOA, http://www.europarl.eu.int/dg4/stoa/en/publi/pdf/98-14-01-2en.pdf
Campbell, Duncan: Inside Echelon, 25.7.2000http://www.heise.de/tp/deutsch/special/ech/6928/1.html
Campbell, Duncan: Interception Capabilities n- Impact and Exploitation – Echelon and its role in COMINT, presentato in seno alla commissione Echelon del Parlamento europeo il 22 gennaio 2001
Federation of American Scientists, http://www.fas.org/irp/nsa/nsafacil.html

homepage della Federation of American Scientists[35] nonché le homepage degli utenti[36] (NSA, AIA, u.a.) ed altre pubblicazioni Internet. Inoltre, si sono registrate le zone di copertura dei satelliti per comunicazioni, si sono calcolate le dimensioni d'antenna necessarie e le si è riportate sulle cartine del globo con le possibili stazioni.

5.3.2. Analisi esatta

Per l'analisi valgono i seguenti principi della fisica della comunicazione via satellite (cfr. anche capitolo 4):

- Un'antenna per satellite può registrare soltanto ciò che si trova all'interno della zona di copertura in cui si situa. Per poter ricevere comunicazioni che avvengono principalmente nella banda C e Ku, un'antenna deve situarsi entro le zone di copertura che contengono la banda C o Ku.
- Per ogni Global-Beam è necessaria un'antenna per satellite, anche se i beam di due satelliti si sovrappongono.
- Se un satellite dispone di più zone di copertura rispetto al semplice Global-Beam, il che è tipico delle attuali generazioni di satelliti, con un'unica antenna satellitare non è più possibile registrare l'intera comunicazione effettuata tramite questo satellite, poiché una sola antenna satellitare non può rientrare in tutte le zone di copertura del satellite stesso. Per captare gli Hemi-Beam ed il Global-Beam di un satellite sono quindi necessarie due antenne satellitari in ubicazioni diverse (cfr. la raffigurazione delle zone di copertura nel capitolo 4). Se si vengono ad aggiungere altri beam (Zone-Beam e Spot-Beam), sono necessarie ulteriori antenne. Diversi beam di un satellite che si sovrappongano possono tuttavia essere captati da un'antenna satellitare, in quanto è tecnicamente possibile separare alla ricezione diverse bande di frequenza.

Valgono inoltre i requisiti di cui al Capitolo 5.2: la non accessibilità degli impianti, in quanto sono gestiti da militari[37] il fatto che per la ricezione dei segnali via satellite sono necessarie antenne paraboliche ed il fatto che le dimensioni delle antenne per satelliti destinate a captare la banda C del Global-Beam per la prima generazione INTELSAT devono superare i 25 m, e per le generazioni successive i 15-18 m.

5.3.2.1. Il parallelismo fra l'evoluzione INTELSAT e la costruzione di stazioni

Un sistema d'intercettazione globale deve progredire parallelamente alle comunicazioni. Di conseguenza, con l'inizio delle comunicazioni via satellite bisogna procedere alla creazione di stazioni, e con l'introduzione di nuove generazioni di satelliti all'installazione di nuove stazioni nonché alla fabbricazione di nuove antenne per satelliti che corrispondano alle rispettive esigenze. Il numero delle stazioni e delle antenne per satelliti deve crescere allorché ciò è necessario per la registrazione delle comunicazioni.

---

[34] Richelson, Jeffrey: 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

[35] Federation of American Scientists

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

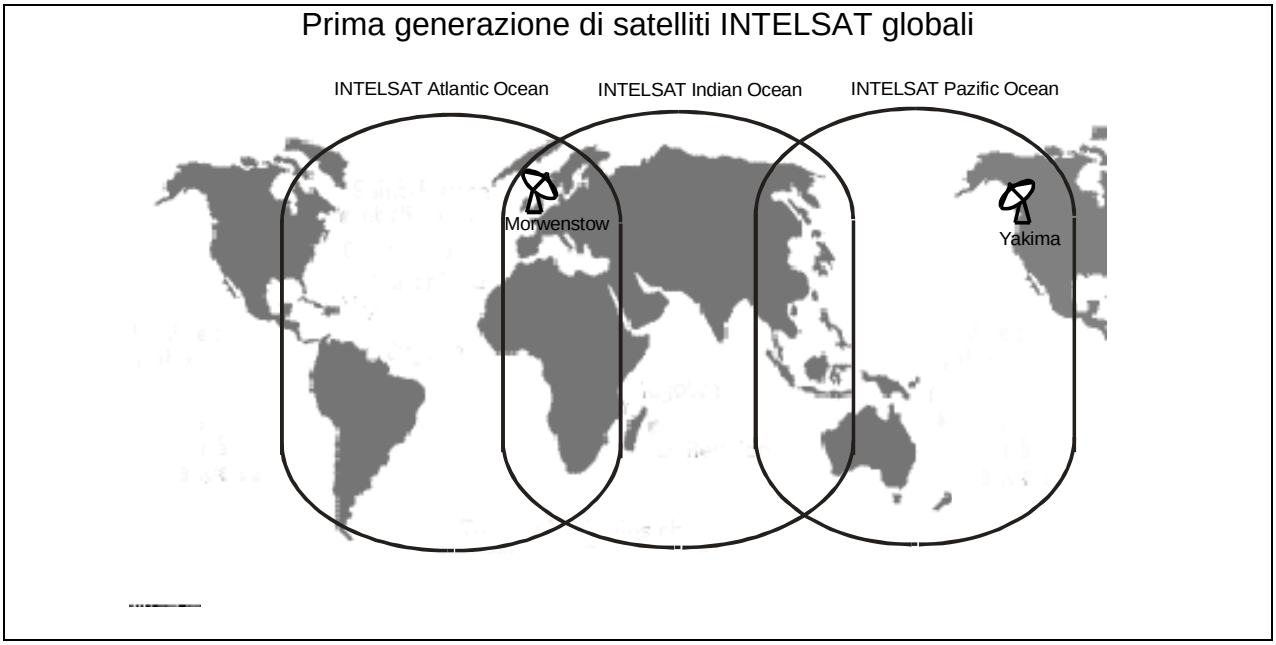
[37] Sigle utilizzate: NAVSECGRU: Naval Security Group, INSCOM: United States Army Intelligence And Security Command, AIA: Air Intelligence Agency, IG: Intelligence Group, IS: Intelligence Sqadron, IW: Intelligence Wing, IOG: Information Operation Group, MIG: Military Intelligence Group.

Viceversa, il fatto che si creino nuove stazioni e si costruiscano nuove antenne satellitari laddove si formano nuove zone di copertura, non è un caso, ma può essere considerato un indizio della presenza di una stazione d'intercettazione delle comunicazioni.
Poiché i satelliti INTELSAT sono stati i primi satelliti per le comunicazioni, che fra l'altro hanno coperto l'intero globo, è logico che l'installazione e l'ampliamento di stazioni vengano effettuati con le generazioni INTELSAT.

La prima generazione

Già nel 1965 il primo satellite INTELSAT (Early Bird) è stato posto in orbita geostazionaria. La sua capacità di trasmissione era ancora ridotta e la sua zona di copertura si estendeva solo all'emisfero Nord.
Con le generazioni INTELSAT II e III, entrate in funzione nel 1967 e 1968, si è raggiunta per la prima volta una copertura globale. I Global-Beam dei satelliti coprivano il settore atlantico, pacifico ed indiano: non vi erano ancora le zone di copertura più piccole. Per captare le intere comunicazioni erano quindi necessarie tre antenne satellitari. Poiché due dei Global-Beam si sovrapponevano sopra il territorio europeo, in quest'area una stazione dotata di due antenne satellitari di diverso orientamento poteva captare le zone di copertura globali di due satelliti.

Prima generazione di satelliti INTELSAT globali



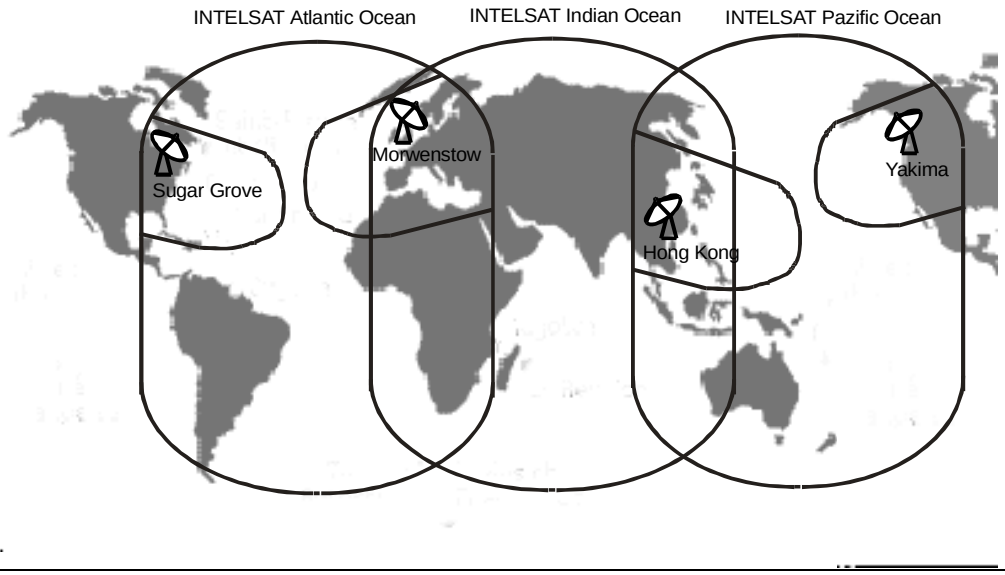
Nel 1970 è stata fondata **Yakima** nella parte nordoccidentale degli Stati Uniti, nel 1972/73 **Morwenstow** nell'Inghilterra meridionale. Yakima era dotata a suo tempo di una grande antenna (orientata verso il Pacifico), Morwenstow aveva due grandi antenne (una puntata sull'Atlantico, una sull'Oceano Indiano). L'ubicazione delle due stazioni consentiva di captare l'intera comunicazione. Nel 1974 fu inoltre costruita a Menwith Hill la prima grande antenna satellitare.

La seconda generazione globale

La seconda generazione di satelliti INTELSAT (IV e IVA) è stata sviluppata negli anni Settanta ed è stata messa in orbita geostazionaria (1971 e 1975). I nuovi satelliti, che a loro volta garantivano una copertura globale e disponevano di un numero molto maggiore di canali di comunicazione a distanza (4000 – 6000), erano dotati, oltre che di Global-Beam, anche di Zone-Beam nell'emisfero settentrionale (cfr. capitolo 4). Uno Zone-Beam copriva la parte orientale

degli USA, uno la parte occidentale, uno l'Europa occidentale ed uno l'Asia orientale. Non era quindi più possibile captare l'intera comunicazione con due stazioni dotate di tre antenne satellitari. L'esistente stazione di Yakima poteva coprire lo Zone-Beam della parte occidentale degli USA, e Morwenstow lo Zone-Beam sopra l'Europa. Per captare gli altri due Zone-Beams si sono rese necessarie una stazione negli USA orientali ed una nell'area dell'Asia orientale.

Seconda generazione di satelliti INTELSAT globali



Alla fine degli anni Settanta è stata costituita la base di **Sugar Grove** nell'Est degli USA (la stazione esisteva già per intercettare le comunicazioni russe); essa è entrata in funzione nel 1980. Alla fine degli anni Settanta è stata anche fondata la stazione di **Hong Kong**.
Con queste quattro stazioni - Yakima, Morwenstow, Sugar Grove ed Hong Kong - negli anni Ottanta si è reso possibile un sistema globale d'intercettazione delle stazioni INTELSAT.

I successivi satelliti INTELSAT, con Zone-Beam e Spot-Beam oltre ai Global-Beam ed Hemi-Beam, hanno rese necessarie ulteriori stazioni in diverse regioni del mondo. A questo riguardo, è molto difficile appurare un nesso fra la costruzione di ulteriori stazioni e l'installazione di altre antenne satellitari.
Poiché è inoltre assai difficile avere accesso ad informazioni sulle stazioni, non è agevole determinare con precisione quali satelliti vengono captati da quali Beam, e di quale stazione. Peraltro, si può constatare in quali Beam si situano le stazioni note.

5.3.2.2. La copertura globale tramite stazioni che intercettano chiaramente i satelliti per le comunicazioni

Oggigiorno, la comunicazione satellitare globale è garantita da satelliti di INTELSAT, INMARSAT e INTERSPUTNIK. La ripartizione in tre zone di copertura (settori indiano, pacifico ed atlantico) è mantenuta, come nelle prime generazioni di satelliti.

In ognuna delle zone di coperutra si trovano stazioni per cui valgono i criteri che contraddistinguono le stazioni d'intercettazione:

Satelliti sull'Oceano Indiano:

INTELSAT 604 (60°E), 602 (62°E), 804 (64°E), 704 (66°E) EXPRESS 6A (80°E) INMARSAT settore indiano	Geraldton, Australia Pine Gap, Australia Morwenstow, Inghilterra Menwith Hill, Inghilterra
INTELSAT APR1 (83°), APR-2 (110,5°)	Geraldton, Australia Pine Gap, Australia Misawa, Giappone

Satelliti sull'Oceano Pacifico:

INTELSAT 802 (174°), 702 (176°), 701 (180°) GORIZONT 41 (130°E), 42 (142°E), LM-1 (75°E) INMARSAT settore pacifico	Waihopai, Nuova Zelanda Geraldton, Australia Pine Gap, Australia Misawa, Giappone Yakima, USA - solo Intelsat ed Inmarsat

Satelliti sull'Oceano Atlantico:

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 settore atlantico	Sugar Grove, USA Buckley Field, USA Sabana Seca, Puerto Rico Morwenstow, Inghilterra Menwith Hill, Inghilterra
INTELSAT 707 (359°)	Morwenstow, Inghilterra Menwith Hill, Inghilterra

Da ciò risulta la possibilità di un sistema globale d'intercettazione delle comunicazioni.

Vi sono inoltre altre stazioni per cui il criterio delle dimensioni d'antenna non vale ma che possono far parte del sistema globale d'intercettazione. Con tali stazioni si potrebbero ad esempio captare gli Zone-Beam o gli Spot-Beam di satelliti i cui Global-Beam vengano intercettati da altre stazioni, o per i cui Global-Beam non siano necessarie grandi antenne satellitari.

5.3.2.3. Le stazioni nei dettagli

Nella descrizione dettagliata delle stazioni si distingue fra stazioni che intercettano chiaramente satelliti per le comunicazioni (criteri del capitolo 5.2) e stazioni il cui compito non può essere provato ricorrendo ai suddetti criteri.

5.3.2.3.1. Stazioni per l'intercettazione di satelliti per le comunicazioni

I criteri descritti al capitolo 5.2, che possono essere ritenuti indizi della presenza di una stazione d'intercettazione di satelliti per comunicazioni, valgono per le seguenti stazioni:

Yakima, USA (120°O, 46°N)
La stazione è stata fondata nel 1970, contemporaneamente alla prima generazione di satelliti. Dal 1995, la Air Intelligence Agency (AIA) si trova in loco con il 544° Intelligence Group (Distaccamento 4). Nella stessa località è stazionato il Naval Security Group (NAVSECGRU). Sul territorio sono installate 6 antenne satellitari, sulle cui dimensioni non si può dedurre nulla dalle fonti. Hager descrive tali antenne come di grandi dimensioni, e ne indica l'orientamento sui satelliti Intelsat sopra il Pacifico (2 antenne satellitari) e sopra l'Atlantico, così come l'orientamento sui satelliti Inmarsat 2.
La data di fondazione di Yakima, contemporanea alla prima generazione di satelliti Intelsat, nonché la descrizione generale del mandato del 544° Intelligence Group sembrano confermare il ruolo svolto dalla stazione nel sistema globale di sorveglianza delle comunicazioni. Un ulteriore indizio è la prossimità di Yakima ad una stazione satellitare ricevente, sita 100 miglia a nord.

Sugar Grove, USA (80°O, 39°N)
Sugar Grove è stata fondata contemporaneamente all'entrata in funzione della seconda generazione di satelliti Intelsat, alla fine degli anni Settanta. Qui sono stazionati il NAVSECGRU nonché l'AIA con il 544° Intelligence Group (Distaccamento 3). Secondo indicazioni di vari autori, la stazione dispone di 10 antenne satellitari, tre delle quali superano i 18m (18,2 m, 32,3 m e 46 m) e sono quindi chiaramente destinate all'intercettazione di satelliti per comunicazioni. Un compito del Distaccamento 3 del 544° IG presso la stazione è mettere a disposizione "Intelligence Support" per la raccolta di informazioni dei satelliti per comunicazioni da parte delle stazioni di campo della Navy.[38]
Inoltre, Sugar Grove si trova in prosimità (60 miglia) della stazione satellitare ricevente di Etam.

Sabana Seca, Puerto Rico (66°O, 18°N)
Nel 1952 il NAVSECGRU è stato stazionato a Sabana Seca; dal 1995 vi si trova anche l'AIA con il 544° IG (Distaccamento 2). La stazione ha perlomeno un'antenna satellitare dal diametro di 32 m e 4 altre antenne satellitari più piccole.
Secondo indicazioni ufficiali, compito della stazione è l'elaborazione delle comunicazioni satellitari ("performing satellite communication processing"), la fornitura di "cryptologic and communications service" nonché il supporto a compiti svolti dalla Marina USA e dal Dipartimento della Difesa (fra l'altro la raccolta di informazioni COMSAT (dalla descrizione del 544° IG)). In futuro, Sabana Seca dovrebbe divenire la prima stazione da campo per l'analisi e l'elaborazione di comunicazioni satellitari.

Morwenstow, Inghilterra (4°O, 51°N)
Morwenstow è stata fondata, come Yakima, contemporaneamente alla prima generazione di satelliti Intelsat, agli inizi degli anni Settanta: la gestisce il servizio d'informazione britannico (GCHQ). A Morwenstow si trovano circa 30 antenne satellitari, due delle quali con un diametro di 30 m; non vi sono indicazioni sulle dimensioni delle altre antenne.
Non vi sono indicazioni ufficiali circa il compito della stazione: le dimensioni ed il numero delle antenne satellitari nonché la loro ubicazione, a soli 110 km dalla stazione Telecom di Goonhilly, non lasciano dubbi circa la sua funzione quale stazione d'intercettazione di satelliti per comunicazioni.

[38] "It provides enhhanced intelligence support to Air Force operational commanders and other consumers of communications satellite information collected by Navy-commanded filed stations." dalla homepage del 144° Intelligence Group http://www.aia.af.mil

Menwith Hill, Inghilterra (2°O, 53°N)
Menwith Hill è stata fondata nel 1956, e nel 1974 erano già presenti 8 antenne satellitari. Nel frattempo, le antenne satellitari sono diventate circa 30, alcune delle quali hanno un diametro superiore ai 20 m. A Menwith Hill operano congiuntamente britannici ed americani. Per parte americana vi operano il NAVSECGRU, l'AIA (451° IOS) nonché l'INSCOM, che detiene il comando della stazione. Il terreno su cui si trova Menwith Hill appartiene al ministero della Difesa britannico ed è dato in locazione agli USA. Secondo indicazioni ufficiali, compito di Menwith Hill è "to provide rapid radio relay and to conduct communications research" ("fornire comunicazioni radio rapide e svolgere ricerche sulle comunicazioni"). Secondo indicazioni di Richelson e della Federation of American Scientists, si tratta di una stazione di terra sia per satelliti spia che per satelliti russi per le comunicazioni.

Geraldton, Australia (114°E, 28°S)
La stazione esiste dall'inizio degli anni Novanta: è sotto la direzione dei servizi segreti australiani (DSD); britannici che a suo tempo erano stazionati ad Hong Kong (cfr. *supra*) fanno ora parte del personale della stazione. Sei antenne satellitari, almeno una delle quali ha un diametro di circa 20 m (stima), sono orientate, secondo indicazioni di Hager, su satelliti posti sopra l'Oceano Indiano e su satelliti sopra il Pacifico.
Secondo indicazioni di un esperto, fornite sotto giuramento dinanzi al parlamento australiano, a Geraldton si intercettano satelliti per comunicazioni.[39]

Pine Gap, Australia (133°E, 23°S)
La stazione di Pine Gap è stata creata nel 1966, ed è diretta dal servizio segreto australiano (DSD); circa la metà delle 900 persone della stazione si compone di americani della CIA e del NAVSECGRU.[40]
Pine Gap ha 18 antenne satellitari, di cui una con diametro di circa 30 m ed una di circa 20. Secondo indicazioni ufficiali nonché di vari autori, la stazione è sin dall'inizio stazione di terra per satelliti SIGINT. Di qui si controllano ed orientano diversi satelliti di spionaggio e se ne ricevono, elaborano ed analizzano i segnali. Le grandi antenne sembrano comprovare anche l'intercettazione di satelliti per comunicazioni, in quanto i satelliti SIGINT non richiedono l'impiego di grandi antenne satellitari. Fino al 1980, gli australiani erano esclusi dal Dipartimento di Analisi dei segnali; da allora, essi hanno libero accesso a tutte le strutture ad eccezione del Dipartimento nazionale di crittografia degli americani.

Misawa, Japan (141°E, 40°N)
La stazione di Misawa esiste dal 1948: vi sono giapponesi ed americani. Da parte americana, vi si trovano il NAVSECGRU, l'INSCOM nonché alcuni gruppi dell'AIA (544° IG, 301° IS). Sul terreno si trovano circa 14 antenne satellitari, alcune delle quali hanno un diametro di circa 20 m (stima). Misawa funge ufficialmente da "Cryptology Operations Center". Secondo indicazioni di Richelson, con l'ausilio di Misawa si intercettano i satelliti russi Molnyia nonché altri satelliti russi per le comunicazioni.

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

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

Waihopai, Nuova Zelanda (173°E, 41°S)
Waihopai esiste dal 1989; da allora vi è una grande antenna di 18 m di diametro, e successivamente ne è stata installata una seconda, di dimensioni inferiori. Secondo Hager, l'antenna di dimensioni maggiori è orientata su Intelsat 701 sopra il Pacifico.

Buckley Field, USA, Denver Colorado (104°O, 40°N)
La stazione è stata fondata nel 1972: vi è di istanza il 544° IG (Dist. 45). Sul terreno vi sono circa 5 antenne satellitari, 4 delle quali hanno un diametro di circa 20 m. Compito ufficiale della stazione è raccogliere, valutare ed analizzare i dati su esperimenti nucleari ottenuti tramite satelliti SIGINT. Le dimensioni dell'antenna fanno supporre un'attività d'intercettazione delle comunicazioni civili.

Hong Kong (22°N, 114°E)
La stazione è stata fondata alla fine degli anni Settanta congiuntamente alla seconda generazione INTELSAT, e dotata di grandi antenne satellitari. Non vi sono indicazioni circa le loro dimensioni esatte. Nel 1994 è iniziato lo smantellamento della stazione di Hong Kong, e le antenne sono state portate in Australia. Non è chiaro quale stazione abbia rilevato i compiti di Hong Kong: Geraldton, Pine Gap o Misawa in Giappone.
I compiti sono stati probabilmente ripartiti fra diverse stazioni.

5.3.2.3.2. Altre stazioni

La funzione delle seguenti stazioni non può essere illustrata chiaramente con l'aiuto dei suddetti criteri:

Leitrim, Canada (75°O, 45°N)
Leitrim fa parte di un programma di scambio fra unità militari USA e canadesi: perciò, secondo indicazioni della Marina USA, vi sono di istanza circa 30 persone. Nel 1985 è stata installata la prima di 4 antenne satellitari, le due maggiori delle quali hanno un diametro di circa 12 m soltanto (stima).
Secondo indicazioni ufficiali, compito della stazione è il "Cryptologic rating" e l'intercettazione delle conversazioni diplomatiche.

Bad Aibling, Germania (12°E, 47°N)
La stazione, che si trova in prossimità di Bad Aibling e in cui lavorano circa 750 americani, è stata rilevata nel 1952 dall'esercito USA (dal 1972 al 1994 è rimasta in possesso del ministero della Difesa). Vi sono di istanza il NAVSECGRU, INSCOM (66° IG, il 718 IG) nonché diversi gruppi dell'AIA (402° IG, 26° IOG). Vi si trovano 14 antenne satellitari, di cui nessuna superiore ai 18 m. Secondo indicazioni ufficiali, Bad Aibling ha i seguenti compiti: "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". Secondo Richelson, è una stazione di terra per satelliti SIGINT e per satelliti russi per le comunicazioni.

Ayios Nikolaos, Cipro (32°E, 35°N)
Ayios Nikolaos, a Cipro, è una stazione britannica. I compiti della stazione, dotata di 9 antenne satellitari, di dimensioni ignote, sono ripartite fra due unità, il "Signals Regiment Radio" e la "Signals Unit" (RAF).

L'ubicazione di Agios Nikolaos in prossimità degli Stati arabi ed il fatto che essa sia l'unica stazione all'interno di alcune zone di copertura (Spot-Beam) in questo settore provano la rilevanza del suo ruolo quanto alla raccolta d'informazioni.

Shoal Bay, Australia (134°E, 13°S)
Shoal Bay è una stazione gestita solo dai servizi d'informazione australiani: dovrebbe avere 10 antenne satellitari, le cui dimensioni non sono meglio descritte. Quanto alle antenne per satelliti che compaiono nelle foto, le 5 più grandi hanno un diametro massimo di 8 m, mentre la sesta visibile è ancora più piccola. Secondo indicazioni di Richelson, le antenne sono orientate sui satelliti indonesiani PALAPA. Resta in dubbio se la stazione faccia parte del sistema globale per l'intercettazione delle comunicazioni civili.

Guam, Pacifico (144°E, 13°S)
Guam esiste dal 1898: oggi vi si trovano una Naval Computer and Telecommunication Station, in cui sono di istanza il 544° IG dell'AIA nonché soldati della Marina USA.
La stazione è dotata di almeno due antenne satellitari, delle cui dimensioni non si sa nulla. La funzione di Guam resta tuttavia ambigua.

Kunia, Hawai (158°O, 21°N)
Questa stazione è attiva dal 1993 quale Regional Security Operation Center (RSOC), ed è gestita dal NAVSECGRU e dall'AIA. Fra i suoi compiti rientra la raccolta di informazioni e comunicazioni nonché il supporto crittologico. La sua funzione resta poco chiara.

Medina Annex, USA Texas (98°O, 29°N)
Medina, come Kunia, è un Regional Security Operation Center - fondato nel 1993 -, gestito dal NAVSECGRU e da unità AIA con compiti nei Caraibi.

Fort Gordon (81°O, 31°N)
Anche Fort Gordon è un Regional Security Operation Center, gestito da INSCOM e AIA (702° IG, 721° IB, 202° IB, 31° IS) con compiti ambigui.

Fort Mead, USA (76°O, 39°N)
Fort Mead è il quartier generale dell'NSA.

5.3.3. Sintesi dei risultati

I dati raccolti su stazioni, satelliti e i suddetti requisiti consentono di trarre le seguenti conclusioni:
1. In ogni zona di copertura esistono stazioni d'intercettazione per almeno alcuni Global-Beam, aventi un minimo di un'antenna con diametro superiore a 18 m, gestite dagli americani o dai britannici, ovvero dove americani o britannici svolgano attività di servizi di informazione. Questo è un forte indizio comprovante l'esistenza di un sistema globale d'intercettazione.
2. Lo sviluppo delle comunicazioni INTELSAT e la parallela installazione di stazioni d'intercettazione provano l'orientamento globale del sistema.
3. In base al punto 1 e 2 è possibile individuare chiaramente determinate stazioni quali stazioni destinate ad intercettare le comunicazioni internazionali via satellite.
4. I dati dei documenti derubricati e dei gestori (AIA, NSA, Navy ecc.) vanno valutati come prova dell'esistenza delle stazioni ivi indicate.

5. Alcune stazioni si trovano contemporaneamente nei beam o negli spot di diversi satelliti, sicché si può captare gran parte delle comunicazioni.
6. Vi sono alcune altre stazioni che non dispongono di grandi antenne ma possono far parte del sistema, in quanto possono ricevere comunicazioni dai beam e dagli spot. Nella fattispecie, bisogna rinunciare all'indizio delle dimensioni dell'antenna e reperirne altri.
7. È dimostrato che alcune delle suddette stazioni si trovano nell'immediata vicinanza delle regolari stazioni di terra di satelliti per comunicazioni.

5.4. Il Patto UKUSA

Si definisce Patto UKUSA un accordo SIGINT sotttoscritto nel 1948 fra Gran Bretagna (Regno Unito, UK), Stati Uniti (USA), Australia, Canada e Nuova Zelanda.

5.4.1. Lo sviluppo storico del Patto UKUSA[41]

Il Patto UKUSA è una continuazione della strettissima collaborazione avviata già durante la Seconda guerra mondiale da Stati Uniti e Gran Bretagna, peraltro delineatasi sin dai tempi della Prima guerra mondiale.
L'iniziativa della creazione di un'alleanza SIGINT venne presa nell'agosto 1940, da parte americana, nel corso di un incontro fra americani e britannici a Londra.[42] Nel febbraio 1941 i crittoanalisti americani fornirono un dispositivo di cifratura (PURPLE) alla Gran Bretagna; nella primavera 1941 cominciò la collaborazione in materia.[43] La collaborazione fra servizi d'informazione fu rafforzata con l'utilizzo congiunto delle flotte nel Nord Atlantico nell'estate 1941. Nel giugno 1941 i britannici riuscirono a decifrare il codice della flotta tedesca ENIGMA.
L'entrata in guerra dell'America potenziò ulteriormente la collaborazione SIGINT. Nel 1942 i crittoanalisti americani della "Naval SIGINT agency" cominciarono ad operare in Gran Bretagna.[44] La comunicazione fra le "Tracking-Rooms" per i sottomarini di Londra, Washington e, dal maggio 1943, anche di Ottawa, in Canada, divenne così stretta che, a detta di un collaboratore dell'epoca, queste agenzie operavano come un'unica organizzazione.[45]
Nella primavera 1943 fu sottoscritto l'accordo BRUSA-SIGINT, ed avviato uno scambio di personale. Il contenuto dell'accordo è incentrato in particolare sulla ripartizione dei compiti e si riassume nei primi tre paragrafi: riguardano lo scambio di informazioni di ogni tipo tratte dalla scoperta, individuazione ed intercettazione di segnali nonché la capacità di decrittare codici e

[41] Christopher Andrew, "The making of the Anglo-American SIGINT Alliance" in E. Hayden, H. Peake and S. Halpern eds, In the Name of Intelligence. Essays in honor of Washington Pforzheimer (Washington NIBC Press 1995) pagg. 95 -109.

[42] *Ibidem*, pag. 99: "At a meeting 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, pagg. 38, 43-4. Sir F.H. Hinsley, et al., British Intelligence in the Second World War, vol. I, pagg. 312-13).

[43] *Ibidem*, pag. 100: "In the spring of 1941, Steward Menzies, the Chief of SIS, appointed an SIS liason officer to the British Joint Services Mission in Washington, Tim O´Connor, …, to advice him on cryptologic collaboration".

[44] *Ibidem*, pag. 100 (Sir F.H. Hinsley, et al., British Intellgence in the Second Worls War, vol II, pag. 56).

[45] *Ibidem*, pag. 101 (Sir F.H. Hinsley, et al., British Intellgence in the Second Worls War, vol. II, pag. 48).

cifrature. Gli americani erano responsabili principalmente per il Giappone, i britannici per la Germania e l'Italia.[46]

Dopo la guerra, l'iniziativa volta al mantenimento di un'alleanza SIGINT partì principalmente dalla Gran Bretagna: se ne concordarono le basi durante un viaggio a livello internazionale dei responsabili del servizio d'informazione britannico (fra cui Sir Harry Hinsley, i cui libri costituiscono il presupposto del citato articolo) nella primavera 1945. Uno degli obiettivi era l'invio di personale SIGINT dall'Europa al Pacifico per la guerra con il Giappone. A questo riguardo, si decise con l'Australia che si sarebbero messi a disposizione del servizio australiano risorse e personale (inglesi). Lungo il viaggio di ritorno negli Stati Uniti, vi furono tappe intermedie in Nuova Zelanda e Canada.
Nel settembre 1945 Truman firmò un protocollo rigorosamente segreto, che costituisce la pietra miliare di un'alleanza SIGINT in tempi di pace.[47] A seguito di ciò, furono avviati negoziati fra inglesi ed americani in vista di un accordo. Una delegazione britannica prese poi contatto con canadesi ed australiani per dibattere una loro eventuale partecipazione: nel febbraio e marzo 1946 si tenne una conferenza angloamericana SIGINT altamente segreta, per discutere i dettagli. Gli inglesi ebbero l'autorizzazione di canadesi ed australiani, e la conferenza sfociò in un documento, tuttora riservato, di circa 25 pagine che suggellava i dettagli di un accordo SIGINT fra Stati Uniti e Commonwealth britannico. Nei due anni successivi seguirono altri negoziati, sicché il testo definitivo del cosiddetto patto UKUSA fu firmato nel giugno 1948.[48]

5.4.2. Prove dell'esistenza del patto

Sinora non vi è stato alcun riconoscimento ufficiale dell'accordo UKUSA da parte degli Stati firmatari. Tuttavia, vi sono diverse prove chiare della sua esistenza.

5.4.2.1. L'indicazione della Navy sull'acronimo

Secondo la Marina degli USA,[49] UKUSA sta per "United Kingdom – USA" e indica un "5-nation SIGINT agreement".

5.4.2.2. Affermazione del direttore del DSD

Il direttore del servizio d'informazione australiano (DSD) ha confermato l'esistenza di quest'accordo in un'intervista: secondo le sue informazioni, i servizi segreti australiani collaborano con i servizi di altri continenti nell'ambito del Patto UKUSA.[50]

---

[46] Ibidem, pagg.101-2: Interviste con Sir F.H. Hinsley, „Operations of the Military Intelligence Service War Department London (MIS WD London)," 11 giugno 1945, Tab A, RG 457 SRH-110, NAW

[47] Truman, Memorandum for the Secretaries of the State, War and the Navy, 12 sett. 1945: "The Secretary of War and the Secretary of the Navy are hereby authorised to direct the Chief of Staff, U.S. Army and the Commander in Chief, U.S. Fleet; and Chief of Naval Operations 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." (da Bradley F. Smith, The Ultra-Magic Deals and the Most Secret Special Relationship (Novato, Ca: Presidio 1993)).

[48] Christopher Andrew, "The making of the Anglo-American SIGINT Alliance" in E. Hayden, h. Peake and S. Halpern eds, In the Name of Inteligence. Essays in honor of Washington Pforzheimer (Washington NIBC Press 1995) pagg. 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.

[49] "Terms/Abbreviations/Acronyms" pubblicato dall'US Nave and Marine Corps Intelligence Training Centre (NMITC) in http://www.cnet.navy.mil/nmitc/training/u.html.

5.4.2.3. Relazione del Canadian Parliamentary Security and Intelligence Committee

In questa relazione si afferma che il Canada collabora con alcuni dei suoi alleati più stretti e di più lunga data in materia di servizi d'informazione. La relazione nomina questi alleati: Stati Uniti (NSA), Gran Bretagna (GCHQ), Australia (DSD) e Nuova Zelanda (GCSB), ma non riporta come viene indicato l'accordo.

5.4.2.4. Affermazione dell'ex vicedirettore dell'NSA, Dr. Louis Torella

In interviste concesse a Christopher Andrew, docente all'Università di Cambridge, nel novembre 1987 e nell'aprile 1992 l'ex vicedirettore dell'NSA, Dr. Louis Torella, presente all'atto della firma, conferma l'esistenza del patto.[51]

5.4.2.5. Lettera dell'ex direttore del GCHQ, Joe Hooper

L'ex direttore del GCHQ Joe Hooper menziona il Patto UKUSA in una lettera del… all'ex direttore dell'NSA Marshall S.Carter.

5.4.2.6. Interlocutori del relatore

Il relatore ha parlato del patto con diverse persone, necessariamente al corrente del Patto UKUSA e del suo contenuto date le funzioni che ricoprivano. Di conseguenza, la sua esistenza è stata comunque indirettamente confermata dal tipo di risposte.

5.5. Analisi di documenti statunitensi derubricati

5.5.1. Tipologia dei documenti

Nell'ambito del "Freedom of Information Acts" del 1966 (5 U.S.C. § 552) e della normativa del ministero della Difesa (DoD FOIA Regulation 5400.7-R del 1997), documenti a suo tempo riservati sono stati derubricati e resi quindi accessibili al pubblico.
I documenti sono accessibili al pubblico tramite il National Security Archive fondato nel 1985, presso la George Washington University di Washington D.C. L'autore Jeffrey Richelson, ex membro del National Security Archive, ha reso accessibili tramite Internet 16 documenti che forniscono una panoramica su inizi, evoluzione, gestione e mandato dell'NSA (National Security Agency) [52]. Inoltre, in due dei documenti si menziona "ECHELON": questi documenti sono costantemente citati da diversi autori, che hanno scritto in merito, e addotti come prova dell'esistenza del sistema di spionaggio globale ECHELON. Inoltre, nei documenti messi a disposizione da Richelson ve ne sono alcuni che confermano l'esistenza dell'NRO (National Reconnaissance Office) e ne descrivono la funzione quale gestore e responsabile dei satelliti SIGINT.[53]

---

[50] Martin Brady, direttore del DSD, Canberra, 16 marzo 2000.

[51] Andrew, Christopher "The growth of the Australian Intelligence Community and the Anglo-American Connection", pagg. 223-4.

[52] http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html
[53] http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB35/index.html

5.5.2. Contenuto dei documenti

I documenti contengono descrizioni frammentarie o citazioni sugli argomenti riportati di seguito.

5.5.2.1 Mandato e struttura dell'NSA (documenti 1, 4, 10, 11, 16)

Nella National Security Council Intelligence Directive 9 (NSCID 9) del 10 marzo 1950 si definisce il concetto di comunicazione estera ai fini del COMINT, ossia, il concetto di **comunicazione estera comprende qualsiasi comunicazione governativa in senso lato (non solo militare) nonché ogni altra comunicazione che possa contenere informazioni di utilità militare, politica, scientifica od economica**.

La direttiva (NSCID 9 rev, 29. 12. 52) espone chiaramente che solo l'FBI è responsabile della sicurezza interna.

La direttiva del ministero della Difesa (DoD) del 32 dicembre 1991 sull'NSA e sul Central Security Service (CSS) definisce come segue il concetto di NSA:

- l'NSA è un servizio organizzato separatamente nell'ambito del ministero della Difesa, sotto la guida del "Secretary of Defense";
- l'NSA si occupa da un canto dello svolgimento della missione SIGINT degli USA, dall'altro di mettere a disposizione sistemi di comunicazione sicuri per tutti i dipartimenti e servizi;
- l'attività SIGINT dell'NSA non riguarda l'elaborazione e la distribuzione di informazioni pronte. Ciò rientra nell'ambito d'attività di altri dipartimenti e servizi.

Inoltre, la direttiva DoD del 1991 delinea la struttura dell'NSA ovvero del CSS.

Nella sua dichiarazione al "House Permanent Select Committee on Intelligence" del 12 aprile 2000, il direttore dell'NSA Hayden definisce come segue i compiti dell'NSA:

- tramite la sorveglianza elettronica, la NSA raccoglie comunicazioni estere per militari e politici (policymaker);
- la NSA fornisce informazioni agli "U.S. Government consumers" su terrorismo internazionale, narcotraffico, proliferazione di armi;
- non rientra nei compiti dell'NSA raccogliere tutte le comunicazioni elettroniche;
- l'NSA può trasmettere informazioni solo a destinatari autorizzati dal governo, ma non direttamente ad imprese statunitensi.

In un memorandum del Viceammiraglio dell'U.S. Navy W.O. Studeman, redatto per conto del governo l'8 aprile 1992, si fa riferimento al mandato sempre più globale (access) dell'NSA, oltre al "support of military operations".

5.5.2.2. Prerogative delle Intelligence Agencies (documento 7)

Dalla United States Signals Intelligence Directive 18 (USSID 18) deriva che vengono intercettati sia i cavi che i segnali radio.

5.5.2.3. Cooperazione con altri servizi (documenti 2a, 2b)

Fra i compiti dell'U.S. Communications Intelligence Board rientrano fra l'altro tutti gli "arrangements" (accordi) con governi esteri per effettuare sorveglianze in ambito COMINT. Fra i compiti del direttore dell'NSA rientra l'elaborazione di tutti i collegamenti con i servizi esteri COMINT.

5.5.2.4. Elenco di unità attive in "siti ECHELON" (documenti 9, 12)

Nelle NAVSECGRU INSTRUCTIONs C5450.48A si descrivono mandato, funzione e obiettivo del Naval Security Group Activity (NAVSECGRUACT), 544th Intelligence Group di Sugar Grove, West Virginia. Viene riprotato che un compito specifico è "maintain and operate an ECHELON-Site"; inoltre, viene indicata come compito l'elaborazione di informazioni per i servizi segreti.

Nel documento "History of the Air Intelligence Agency – 1 January to 31 December 1994" (RCS: HAF-HO(A&SA)7101 Volume 1), al punto "Activation of Echelon Units", si menziona la Air Intelligence Agency (AIA), Distaccamento 2 e 3.

I documenti non forniscono informazioni su cosa sia un "sito ECHELON", su cosa si faccia su un "sito ECHELON", sul significato del nome in codice ECHELON. Dai documenti non emerge nulla sul Patto UKUSA.

5.5.2.5. Elenco di stazioni (documenti 6, 9, 12)

- Sugar Grove, West Virginia nelle NAVSECGRU INSTRUCTIONs C5450.48A
- Misawa Air Base, Japan in History of the Air Intelligence Agency - January to 31 December 1994 (RCS: HAF-HO(A&SA)7101 Volume 1)
- Puerto Rico (i.e. Sabana Seca), *ibidem*
- Guam, *ibidem*
- Yakima, Washington, *ibidem*
- Fort Meade, Maryland, una relazione COMINT dell'NSA da Fort George G. Meade, Maryland del 31 agosto 1972, che illustra le attività COMINT in loco.

5.5.2.6. Tutela della vita privata dei cittadini statunitensi (documenti 7, 7a- f, 11,16)

Nelle NAVSECGRU INSTRUCTIONs C5450.48A si afferma che si deve garantire la vita privata dei cittadini.

In vari documenti si spiega la necessità di tutelare la vita privata dei cittadini americani, e le modalità per farlo (Baker, General Counsel, NSA, lettera del 9 settembre 1992, United States Signals Intelligence Directive (USSID) 18, 20 ottobre 1980, e diverse integrazioni).[54]

5.5.2.7. Definizioni (documenti 4, 5a,7)

La direttiva del ministero della Difesa del 23 dicembre 1991 fornisce definizioni precise di SIGINT, COMINT, ELINT e TELINT, come la National Security Council Intelligence Directive n. 6 del 17 febbraio 1972.

Secondo tale definizione, COMINT significa la registrazione e l'elaborazione delle comunicazioni estere (passed by electromagnetic means) esclusa l'intercettazione e l'elaborazione di comunicazioni scritte, stampa, propaganda non cifrate.

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

5.5.3. Sintesi

1. Già 50 anni fa l'interesse era volto ad informazioni non solo nell'ambito della politica e della sicurezza, ma anche della scienza e dell'economia.
2. I documenti provano che l'NSA collabora con altri servizi nel COMINT.
3. I documenti che forniscono indicazioni sull'organizzazione dell'NSA, sul suo mandato e sulla sua subordinazione gerarchica al ministero della Difesa, non vanno sostanzialmente oltre quanto si può dedurre da fonti accessibili al pubblico, desumibili dalla *homepage* dell'NSA.
4. I cavi possono essere intercettati.
5. Il 544° Intelligence Group e il Distaccamento 2 e 3 dell'Air Intelligence Agency partecipano alla raccolta di informazioni dei servizi.
6. La sigla "ECHELON" appare in diversi contesti.
7. Sugar Grove in West Virginia, la base aerea di Misawa in Giappone, Puerto Rico (ossia Sabana Seca), Guam, Yakima nello Stato di Washington vengono denominate stazioni SIGINT.
8. I documenti forniscono informazioni su come tutelare la vita privata dei cittadini americani.

I documenti non forniscono prove bensì forti indizi, che permettono, congiuntamente ad altri, di formulare ipotesi.

5.6. Indicazioni di autori specializzati e giornalisti

5.6.1. Il libro di Nicky Hager

Nel libro di Nicky Hager pubblicato nel 1996, "Secret Powers – New Zealand's role in the international spy network", si descrive per la prima volta dettagliatamente il sistema ECHELON. Secondo l'autore, le sue origini risalgono all'anno 1947, quando il Regno Unito e gli Stati Uniti, in seguito alla collaborazione bellica, concordarono di proseguire congiuntamente a livello mondiale le attività COMINT. Gli Stati dovevano collaborare alla creazione di un sistema d'intercettazione il più possibile globale, condividendo le strutture specifiche indispensabili a tal fine nonché le spese che vi sono necessariamente connesse e avendo accesso comune ai risultati. In seguito, Canada, Australia e Nuova Zelanda hanno aderito al Patto UKUSA.

Secondo le indicazioni di Hager, l'intercettazione delle comunicazioni via satellite costituisce il fulcro del sistema odierno. Già negli anni Settanta si era iniziato ad intercettare, tramite stazioni di terra, le notizie inviate tramite satelliti Intel, il primo sistema globale di comunicazioni via satellite[55]. In queste notizie si cercano poi, tramite computer, parole chiave o indirizzi ricorrenti, per filtrarne le informazioni chiave. Successivamente, la sorveglianza è stata ampliata ad altri satelliti, ad esempio quelli di Inmarsat[56], che si concentravano sulla comunicazione marittima.

Hager sottolinea nel suo libro che l'intercettazione delle comunicazioni via satellite costituisce solo un elemento, per quanto importante, del sistema d'intercettazione. Inoltre, vi sono numerose

[55] Cfr. al riguardo http://www.intelsat.int/index.htm

[56] Cfr. al riguardo http://www.inmarsat.org/index3.html

altre istituzioni per la sorveglianza di ponti radio e cavi, che tuttavia sono meno documentate e più difficili da dimostrare, in quanto sono meno visibili delle stazioni di terra. "ECHELON" diviene quindi sinonimo di sistema d'intercettazione globale.

5.6.2. Indicazioni di Duncan Campbell

Nello studio STOA 2/5 del 1999, che si occupa in modo approfondito degli aspetti tecnici, Duncan Campbell illustra dettagliatamente che ogni mezzo utilizzato per la trasmissione di comunicazioni può essere intercettato, e spiega con quali modalità. In una delle sue ultime relazioni precisa tuttavia che anche ECHELON ha i suoi limiti, e che l'idea originaria, ossia che fosse possibile una sorveglianza assoluta, si è rivelata erronea. "Né ECHELON né il sistema di spionaggio elettronico, di cui fa parte, lo consentono. Non è neppure disponibile un'attrezzatura che abbia la capacità di elaborare e riconoscere il contenuto di ogni comunicazione verbale o telefonata."[57]

5.6.3. Indicazioni di Jeff Richelson

L'autore Jeffrey Richelson, ex membro dei National Security Archives, ha reso accessibili tramite Internet 16 documenti in passato riservati, che forniscono una panoramica di costituzione, sviluppo, gestione e mandato dell'NSA (National Security Agency)[58].
Egli è inoltre autore di diversi libri ed articoli sulle attività USA in materia di servizi d'informazione. Nel suo libro pubblicato nel 1985, "The Ties That Bind"[59], descrive dettagliatamente come si è giunti al Patto UKUSA e le attività dei servizi segreti che vi hanno partecipato, ossia USA, Gran Bretagna, Canada, Australia e Nuova Zelanda.
Nel suo dettagliatissimo libro "The U.S. Intelligence Community"[60] del 1999, Richelson fornisce una panoramica delle attività dei servizi d'informazione negli USA, e ne descrive la struttura organizzativa nonché i metodi di raccolta ed analisi delle informazioni. Nel capitolo 8 del libro, l'autore esamina nei dettagli le capacità SIGINT dei servizi in questione e descrive alcune stazioni di terra. Nel capitolo 13 descrive i rapporti fra servizi d'informazione degli USA e di altri paesi, e fra l'altro il Patto UKUSA. Cita inoltre la sigla ECHELON quale parola in codice volta ad indicare un sistema di scambio assistito da computer.
Nel suo articolo, pubblicato nel 2000, "Desperately seeking Signals"[61] Richelson descrive brevemente il Patto UKUSA, nomina impianti di intercettazione satellitare per satelliti per comunicazioni e descrive le possibilità ed i limiti dell'intercettazione delle comunicazioni civili.

5.6.4. Indicazioni di Jeff Richelson

verrà inserito successivamente

---

[57] Duncan Campbell, Inside Echelon. Zur Geschichte, Tehnik und Funktion des unter dem Namen Echelon bekannten globalen Abhör- und Filtersystems, 1 (Dentro Echelon. Storia, tecnica e funzione del sistema di ascolto e filtraggio globale conosciuto con il nome di Echelon, 1).

[58] http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html

[59] Jeffrey T. Richelson, Desmond Ball 1985: The Ties That Bind, Boston UNWIN HYMAN, Sydney Wellington London.

[60] Jeffrey T. Richelson 1999 (4th ed.): "The U.S. Intelligence Community", Westview Press.

[61] Jeffrey T. Richelson 2000: "Desperately seeking Signals" The Bulletin of the Atomic Scientists, marzo/aprile 2000, Vol. 56, No. 2, pagg. 47-51.

5.6.5. Indicazioni di Bo Elkjaer e Kenan Seeberg

I giornalisti danesi Bo Elkjaer e Kenan Seeberg hanno indicato al comitato, il 22 gennaio 2001, che già negli anni Ottanta ECHELON era assai progredito, e che dal 1984 la Danimarca collabora con gli USA.

5.7. Affermazioni di ex collaboratori dei servizi d'informazione

5.7.1. Margaret Newsham (ex collaboratrice NSA)

Margaret Newsham[62] è stata impiegata dal 1974 al 1984 presso la Ford e la Lockheed e, in questo periodo, stando alle sue affermazioni, ha lavorato per la NSA. E' stata formata a tale lavoro presso il quartier generale della NSA a Fort George Meade nel Maryland, USA, e dal 1977-1978 è stata assunta a Menwith Hill, la stazione a terra americana su territorio britannico. In tale località ha avuto modo di constatare che veniva intercettata una conversazione del senatore USA Strohm Thurmond. Già nel 1978, ECHELON poteva intercettare le telecomunicazioni di una determinata persona, trasportate via satellite.

Quanto al suo ruolo presso l'NSA, Margaret Newsham afferma di essere stata responsabile dell'elaborazione di sistemi e programmi, della loro configurazione e del loro adattamento ai grandi computer. I programmi software sono stati denominati SILKWORTH e SIRE, e la rete ECHELON.

5.7.2. Wayne Madsen (ex collaboratore NSA)

Wayne Madsen[63], ex collaboratore NSA, conferma a sua volta l'esistenza di ECHELON. A suo avviso, la raccolta di dati economici ha la massima priorità e viene utilizzata a vantaggio delle imprese statunitensi. Egli teme in particolare che ECHELON possa spiare ONG come Amnesty International o Greenpeace. A questo riguardo, egli afferma che l'NSA ha dovuto ammettere di disporre di oltre 1000 pagine d'informazioni sulla Principessa Diana, che, con la sua campagna sulle mine antiuomo, aveva assunto posizioni contrarie alla politica americana.

5.7.3. Mike Frost (ex collaboratore dei servizi segreti canadesi)

Mike Frost è stato dipendente dei servizi segreti canadese CSE[64] per oltre 20 anni. Egli afferma che la stazione d'intercettazione di Ottawa costituiva soltanto una parte di una rete mondiale di stazioni di spionaggio.[65] In un'intervista con la CBS, egli ha dichiarato che "in tutto il mondo, ogni giorno, le conversazioni telefoniche, le e-mail, ed i telefax vengono sorvegliati da ECHELON, una rete segreta governativa di sorveglianza".[66] Ciò riguarda anche le comunicazioni civili. A titolo esemplificativo, in un'intervista con un'emittente australiana egli spiega che di fatto il CSE aveva inserito in una banca dati di terroristi sospetti il nome ed il

[62] Vedasi su quanto segue Bo Elkjaer, Kenan Seeberg, Echelon was my baby – Intervista con Margaret Newsham, Ekstra Bladet, 17.1.1999.

[63] Intervista televisiva dell'NBC "60 Minutes" del 27.2.2000; http://cryptome.org/echelon-60min.htm.

[64] Il Communication Security Establishment, subordinato al Ministero della Difesa canadese, gestisce Sigint.

[65] Intervista televisiva dell'NBC "60 Minutes" del 27.2.2000; http://cryptome.org/echelon-60min.htm.

[66] Rötzer, Die NSA geht wegen Echelon an die Öffentlichkeit;
http://www.heise.de/bin/tp/issue/download.cgi?artikelnr=6633&rub_ordner=special

numero di telefono di una donna che, in un'innocua conversazione telefonica con un amico, aveva utilizzato un'espressione ambigua. Il computer, nell'elaborare la comunicazione, aveva reperito la parola chiave e riprodotto la comunicazione stessa, il responsabile dell'analisi non era sicuro e aveva quindi registrato i dati della persona in questione.[67]

Risulta che i servizi d'informazione degli Stati ECHELON si aiutano reciprocamente spiando l'un per l'altro, in modo perlomeno da non poter rimproverare nulla al servizio interno. Ad esempio, il GCHQ ha incaricato il CSE di spiare per suo conto due ministri britannici, in quanto il Primo Ministro Thatcher voleva sapere se essi condividevano la sua linea politica.[68]

5.7.4. Fred Stock (ex collaboratore dei servizi segreti canadesi)

Fred Stock afferma di essere stato espulso dai servizi segreti canadesi CSE nel 1993 per essersi pronunciato contro il loro nuovo fulcro d'interesse, ossia le informazioni economiche e gli obiettivi civili. Le comunicazioni intercettate contenevano informazioni su transazioni con altri paesi, fra cui i negoziati NAFTA, l'acquisto di cereali dalla Cina e il traffico d'armi francese. Secondo Stock, i servizi ricevevano regolarmente informazioni anche sulle proteste ambientaliste delle navi di Greenpeace in alto mare.[69]

5.8. Informazioni governative

5.8.1. Affermazioni da parte americana

L'ex direttore della CIA James Woolsey ha dichiarato, in una conferenza stampa[70] concessa su richiesta del Dipartimento di Stato degli USA, che gli USA svolgono attività di spionaggio sul continente europeo. La "economic intelligence" viene comunque ottenuta al 95% dall'analisi di fonti d'informazione accessibili al pubblico, e solo nel 5% dei casi si procede alla sottrazione di informazioni segrete. I dati economici di altri paesi sono oggetto di spionaggio nei casi in cui si tratta del rispetto di sanzioni e di beni a duplice uso, nonché di lottare contro la concussione nel conferimento dei pubblici appalti. Queste informazioni non vengono tuttavia trasmesse alle imprese statunitensi. Woolsey sottolinea che, anche se durante lo spionaggio di dati economici ci si dovesse imbattere in informazioni economicamente utilizzabili, sarebbe molto dispendioso in termini di tempo, per un analista, valutare sotto questo profilo l'enorme quantitativo di dati a disposizione, e sarebbe un abuso utilizzare il tempo per spiare partner commerciali alleati. Inoltre, egli fa rilevare che, anche procedendo in tal modo, sarebbe difficile, tenendo conto delle ramificazioni internazionali, valutare quali imprese risultano essere imprese USA, e quindi se far loro pervenire le informazioni.

In un successivo articolo per il Wall Street Journal Europe[71], Woolsey ha ribadito che gli USA spiano l'Europa, ma soltanto per scoprire i casi di corruzione. Egli precisa anche espressamente che gli USA utilizzano computer per reperire le parole chiave dei dati.

---

[67] Intervista televisiva dell'NBC "60 Minutes" del 27.2.2000; http://cryptome.org/echelon-60min.htm.

[68] Intervista dell'emittente australiana Channel 9 del 23..3.1999; http://www.geocities.com/CapitolHill/Senate/8789/sunday1.htm

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

[70] Trascrizione, 7.3.2000, http://cryptome.org/echelon-cia.htm.

[71] James Woolsey, Why America Spies on its Allies, The Wall Street Journal, 22.3.2000, 31.

5.8.2. Affermazioni da parte britannica

Da diverse interrogazioni in seno alla Camera dei Comuni[72] risulta che la stazione RAF di Menwith Hill fa parte del ministero della Difesa britannico, ma viene messa a disposizione del ministero della Difesa statunitense, in particolare dell'NSA[73], che dirige la stazione,[74] quale struttura di comunicazione.[75] Alla metà del 2000 operavano presso la RAF di Menwith Hill 415 membri dell'esercito statunitense e 5 di quello britannico, 989 civili americani e 392 civili britannici, senza contare i collaboratori GCHQ già presenti.[76] La presenza delle truppe USA è disciplinata dal Trattato dell'Atlantico del Nord e da speciali accordi amministrativi segreti[77], ritenuti adeguati per i rapporti esistenti fra i governi di Regno Unito ed USA in vista di una difesa comune.[78] La stazione costituisce parte integrante della rete globale del Ministero della Difesa USA, che appoggia gli interessi britannici, statunitensi e NATO.[79]

Nella relazione annuale 1999/2000 si sottolinea espressamente l'importanza della stretta cooperazione nell'ambito del Patto UKUSA, che si rispecchia nella qualità dei risultati dei servizi d'informazione. In particolare, si fa rilevare che quando, per tre giorni, vennero meno i dispositivi della NSA, il GCHQ servì la clientela americana oltre a quella britannica.[80]

5.8.3. Affermazioni da parte australiana[81]

Martin Brady, direttore del servizio d'informazioni australiano DSD[82], confermò, in una lettera al programma "Sunday" dell'emittente australiana "Channel 9", l'esistenza di una collaborazione fra il DSD e gli altri servizi, nell'ambito dell'accordo UKUSA. Nella stessa lettera si sottolinea che tutte le strutture dei servizi d'informazione australiani vengono gestite da questi ultimi, autonomamente o congiuntamente ai servizi americani. Nei casi in cui gli impianti vengono utilizzati congiuntamente, il governo australiano ha piena conoscenza di tutte le attività e il personale australiano è coinvolto a tutti i livelli.[83]

---

[72] Commons Written Answers, House of Commons Hansard Debares.

[73] 12.7.1995.

[74] 25.10.1994

[75] 3.12.1997

[76] 12.5.2000

[77] 12.7.1995

[78] 8.3.1999, 6.7.1999

[79] 3.12.1997

[80] Intelligence and Security Committee, Annual Report 1999-2000, Z. 14, presentato al Parlamento nel novembre 2000 dal Primo Ministro.

[81] http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp;
http://sunday.ninemsn.com/01_cover_stories/article_335.asp

[82] Defence Signals Directorate, servizio d'informazione australiano che gestisce SIGINT.

[83] Lettera del 16 marzo 1999 di Martin Brady, Direttore del DSD, a Ross Coulthart, Sunday Program; cfr. anche:
http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp;
http://sunday.ninemsn.com/01_cover_stories/article_335.asp.

5.8.4. Affermazioni da parte olandese

Il 19 gennaio 2001 il ministro della Difesa olandese presenta al parlamento una relazione sugli aspetti tecnici e giuridici dell'intercettazione globale nei moderni sistemi di telecomunicazione.[84] Il governo olandese sostiene che, pur non disponendo di conoscenze proprie, sulla scorta delle informazioni messe a disposizione da terzi è altamente probabile che sussista una rete ECHELON, ma che vi siano anche altri sistemi dotati delle stesse possibilità. Il governo olandese è giunto alla conclusione che l'intercettazione globale di sistemi di comunicazione non si limita agli Stati membri del sistema ECHELON, ma si estende a governi di altri paesi.

5.8.5. Affermazioni da parte italiana

Luigi Ramponi, ex direttore del servizio d'informazione italiano, il SISMI, non esprime dubbi sull'esistenza di "ECHELON" nella sua intervista a "Il mondo".[85] Ramponi dichiara espressamente di essere stato al corrente di tale esistenza nella sua veste di capo del SISMI, e di essere stato informato, dal 1992, di una forte attività di intercettazione delle onde a frequenza bassa, media ed elevata. All'inizio della sua attività presso il SISMI nel 1991, si aveva soprattutto a che fare con Gran Bretagna e Stati Uniti.

5.9. Relazioni parlamentari

5.9.1. Relazioni della commissione di controllo belga "Comité Permanent R"

La commissione di controllo belga "Comité Permanent R" si è già pronunciata su ECHELON in due relazioni.

Nel "Rapport d'activités 1999", il terzo capitolo mira ad appurare come reagiscono i servizi d'informazione belgi all'eventualità di un sistema ECHELON di sorveglianza delle comunicazioni. La relazione, di 15 pagine, giunge alla conclusione che entrambi i servizi, Sûreté de l'Etat e Service général du Renseignement (SGR), hanno ottenuto informazioni su ECHELON solo tramite documenti pubblici.

La seconda relazione, "Rapport complémentaire d'activités 1999", si occupa molto più dettagliatamente del sistema ECHELON. Essa si pronuncia sugli studi STOA e dedica parte delle analisi alla descrizione delle condizioni quadro, di carattere tecnico e giuridico, dell'intercettazione delle telecomunicazioni. Essa conclude che ECHELON esiste realmente ed è in grado di intercettare tutte le informazioni trasmesse via satellite (circa l'1% del volume complessivo di telefonate internazionali), procedendo alla ricerca di parole chiave, e che le sue capacità in materia di decodificazione sono notevolmente superiori a quanto presunto da parte americana. Sussistono dubbi circa l'affermazione che non venga gestita un'industria dello spionaggio a Menwith Hill; si sottolinea esplicitamente che è impossibile appurare con certezza cosa fa o meno ECHELON.

[84] Brief aan de Tweede Kamer betreffende "Het grootschalig afluisteren van moderne telecommunicatiesystemen" del 19.1.2001.

[85] Francesco Sorti, Dossier esclusivo. Caso Echelon. parla Luigi Ramponi. Anche i politici sapevano, Il mondo, 17.4.1998.

5.9.2. Relazione della commissione per la difesa nazionale dell'Assemblée Nationale francese

In Francia, la commissione per la difesa nazionale ha presentato all'Assemblée Nationale una relazione sulla tematica dei sistemi d'intercettazione.[86]

Dopo aver esposto nei dettagli i più svariati aspetti, il relatore Arthur Paecht giunge alla conclusione che ECHELON esiste e che si tratta del solo sistema di sorveglianza noto a livello plurinazionale. Le capacità del sistema sono effettive, ma hanno raggiunto il loro limite, non solo perché gli sforzi dispiegati non sono più proporzionali all'esplosione delle comunicazioni, ma anche perché determinati obiettivi hanno appreso a tutelarsi.

Il sistema ECHELON si discosta dagli obiettivi originari legati al contesto della Guerra Fredda, sicché non è improbabile che le informazioni raccolte vengano utilizzate, a fini politici ed economici, contro altri Stati della NATO.

ECHELON potrebbe costituire una minaccia per le libertà fondamentali, e a questo riguardo solleva numerosi problemi che richiedono risposte appropriate. È erroneo supporre che gli Stati membri di ECHELON cessino le proprie attività; vari indizi sembrano piuttosto indicare che è stato costituito un nuovo sistema, con nuovi partner, per spingersi oltre i confini di ECHELON, con l'ausilio di nuovi mezzi.

[86] 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 Assemblöe nationale , enregistré à la Présidence de l'Assemblée nationale le 11 octobre 2000.

6. È possibile che esistano altri sistemi d'intercettazione globali?

6.1. Condizioni necessarie

6.1.1. Requisiti tecnico-geografici

Per l'intercettazione di comunicazioni internazionali trasmesse mediante satelliti di prima generazione, è necessario disporre di stazioni riceventi nella zona dell'Atlantico, nella zona dell'Oceano Indiano e nell'area del Pacifico. Per i satelliti di ultima generazione, che dirigono i segnali verso un'area ristretta, occorre soddisfare ulteriori requisiti relativi alla posizione geografica delle stazioni d'intercettazione, onde coprire tutte le comunicazioni trasmesse via satellite.

Un altro sistema d'intercettazione globale deve necessariamente allestire le proprie stazioni al di fuori dei territori nazionali degli Stati ECHELON.

6.1.2. Requisiti politico-economici

Per allestire un sistema d'intercettazioni mondiale, le autorità che lo controllano devono ritenerlo giustificato dal punto di vista economico e politico. Il beneficiario (o i beneficiari) del sistema devono avere interessi economici, militari o di sicurezza a livello mondiale o perlomeno credere di appartenere al gruppo delle cosiddette potenze mondiali. Ciò riduce la cerchia dei potenziali aspiranti alla Cina ed agli Stati del G-8, esclusi Stati Uniti e Regno Unito.

6.2. Francia

La Francia dispone di propri territori, dipartimenti ed entità territoriali nei tre settori menzionati in precedenza.

Nel settore atlantico, Saint Pierre et Miquelon si trovano ad est del Canada (65° O/47° N), la Guadalupa (61° O/16° N) e la Martinica (60° O/14° N) sono situate a nord-est del Sudamerica e la Guyana Francese occupa parte della costa nordorientale sudamericana (52° O/5° N).

Nel settore dell'Oceano Indiano si trovano, ad est dell'Africa meridionale, le isole di Mayotte (45° O/12° S) e della Riunione (55° O/20° S), nonché, all'estremità meridionale, le Terres Australes et Antarticques Francaises. Nel settore del Pacifico troviamo la Nuova Caledonia (165° O/20° S), Wallis et Futuna (176° O/12° S) e la Polinesia Francese (150° O/16° S).

Scarseggiano le informazioni sull'esistenza di eventuali stazioni del servizio francese di spionaggio DGSE (Direction générale de la sécurité extérieure) in queste regioni d'oltremare. Secondo dichiarazioni di giornalisti francesi[87], esistono stazioni a Kourou nella Guyana Francese e a Mayotte. Non si dispone di dati specifici sulle dimensioni delle stazioni o sul numero di antenne satellitari e relative grandezze. Altre stazioni si troverebbero in Francia, a Domme, presso Bordeaux e a Alluetts-le-Roi nella regione parigina. Jauvert stima un totale di 30. Schmidt-Enboom[88] ritiene che sia operativa una stazione anche in Nuova Caledonia.

Teoricamente, la Francia potrebbe gestire un sistema d'intercettazioni globale. Per una valutazione seria, tuttavia, il relatore non dispone di sufficienti informazioni accessibili al pubblico.

6.3. Russia

Il servizio d'informazione russo FAPSI, responsabile della sicurezza delle comunicazioni e della SIGINT, gestirebbe congiuntamente con i servizi delle forze armate russe stazioni di terra GRU in Lettonia, Vietnam e Cuba.

Nel settore atlantico, secondo dichiarazioni della Federation of American Scientists, si trova la stazione di Lourdes, a Cuba (82°O, 23°N), gestita congiuntamente con i servizi segreti cubani. Nel settore dell'Oceano Indiano esistono stazioni in territorio russo, sulle quali non disponiamo di ulteriori informazioni, oltre alla stazione di Skrunda in Lettonia. Nel settore del Pacifico vi sarebbe una stazione nella Baia di Cam Rank nel Vietnam settentrionale. Si ignorano particolari sulle stazioni, quali numero e grandezza delle antenne.

Tenendo conto delle stazioni ubicate in territorio russo, teoreticamente è possibile realizzare una copertura globale. Anche in questo caso le informazioni disponibili sono insufficienti per una valutazione seria.

6.4. Altri Stati del G-8 e Cina

Gli altri Stati del G-8 e la Cina non dispongono di territori propri o di alleati stretti nei necessari settori del mondo per poter operare un sistema globale di intercettazioni.

---

[87] Jean Guisnel, L'espionage n'est plus un secret, The Tocqueville Connection, 10.7.1998.

Vincent Jauvert, Espionnage comment la France, Le Nouvel Observateur, 5.4.2001, n. 1900, pag. 14 segg.

[88] E.Schmidt-Eenboom, in: Streng Geheim, Museumsstiftung Post und Telekommunikation, Heidelberg 1999, pag. 180.

7. Compatibilità di un sistema d'intercettazione delle comunicazioni del tipo "ECHELON" con il diritto dell'Unione europea

7.1. Approfondimento tematico

Il mandato della commissione prevede, tra l'altro, il compito specifico di determinare la compatibilità di un sistema d'intercettazione delle comunicazioni di tipo "ECHELON" con il diritto comunitario[89], con l'obbligo, in particolare, di valutarne la compatibilità con entrambe le direttive sulla tutela dei dati personali 95/46/CE e 97/66/CE, con l'articolo 286 del trattato che istituisce la Comunità europea e con l'articolo 8 del trattato sull'Unione europea.

Appare necessario abbordare tale determinazione da due punti di vista distinti. Il primo aspetto risulta dalla dimostrazione indiziale contenuta nel capitolo 5, secondo cui il sistema denominato "ECHELON" è stato ideato come sistema per captare le comunicazioni inteso a fornire ai servizi segreti americani, canadesi, australiani, neozelandesi e britannici informazioni su avvenimenti all'estero attraverso la raccolta e la valutazione di dati di comunicazione. Si tratta dunque di un classico strumento di spionaggio dei servizi di informazione esteri[90]. Il primo passo deve quindi servire a determinare la compatibilità di una tale attività del servizio d'informazione con il diritto dell'Unione.

Inoltre, la relazione STOA, presentata da Campbell, accusa questo sistema di essere oggetto di impiego abusivo a fini di spionaggio della concorrenza, arrecando così danni onerosi all'economia dei paesi europei, e cita al riguardo dichiarazioni dell'ex direttore della CIA R. James Woolsey secondo cui gli Stati Uniti effettuerebbero operazioni di spionaggio ai danni di imprese europee unicamente al fine di ristabilire condizioni di uguaglianza di mercato, in quanto gli ordini si ottengono unicamente attraverso la corruzione[91]. In caso di conferma dell'uso dei sistemi a fini di spionaggio della concorrenza, si pone nuovamente la questione della compatibilità con il diritto comunitario. Questo secondo aspetto va quindi studiato separatamente in una seconda fase.

7.2. La compatibilità di un sistema di raccolta di informazioni con il diritto dell'Unione

7.2.1. Compatibilità con il diritto comunitario

Attività e misure al servizio della sicurezza dello Stato e della giustizia penale non rientrano fondamentalmente nella giurisdizione del trattato CE. Poiché la Comunità europea, in ossequio al principio di sussidiarietà, può intervenire unicamente laddove sia titolare di una competenza corrispondente, essa di conseguenza ha escluso questi ambiti dal campo di applicazione delle direttive sulla tutela dei dati di carattere personale fondate sul trattato CE, in particolare

[89] Cfr *supra* capitolo 1, 1.3.

[90] Cfr. capitolo 2.

[91] Cfr. capitolo 5, 5.6. e 5.8.

sull'articolo 95 (ex articolo 100 A). La direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati[92] e la direttiva 97/66/CE sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni[93] non si applicano "comunque ai trattamenti[94]/alle attività[95] riguardanti la pubblica sicurezza, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) e alle attività dello Stato in settori che rientrano nel diritto penale". La proposta di direttiva attualmente all'esame del Parlamento sul trattamento dei dati personali e sulla tutela della vita privata nella comunicazione elettronica[96] riprende la medesima formulazione. L'appartenenza di uno Stato membro ad un sistema d'intercettazione finalizzato alla sicurezza dello Stato non entra pertanto in contraddizione con le direttive per la tutela dei dati personali.

Parimenti, non si ravvisa nessuna violazione dell'articolo 286 del trattato CE, che amplia il campo di applicazione delle direttive sulla tutela dei dati al trattamento dei dati da parte di organi ed istituzioni della Comunità. Lo stesso vale per il regolamento n. 45/2001 concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati[97]. Anche quest'ultimo regolamento è applicabile unicamente all'attività degli organi ricadente nell'ambito del trattato CE[98]. Per evitare malintesi, è utile rilevare esplicitamente che nessuno ha mai supposto che organi ed istituzioni della Comunità partecipino ad un sistema d'intercettazione e il relatore non dispone di nessun indizio in tal senso.

7.2.2. Compatibilità con altri rami del diritto dell'Unione europea

Negli ambiti del titolo V (Politica estera e di sicurezza comune) e del titolo VI (Cooperazione di polizia e giudiziaria in materia penale) non esiste una normativa sulla protezione dei dati paragonabile alle direttive comunitarie. Il Parlamento europeo ha più volte rilevato l'urgente necessità di procedere in tal senso[99].

La protezione dei diritti e delle libertà fondamentali delle persone in questi ambiti è garantita unicamente dagli articoli 6 e 7, in particolare l'articolo 6, paragrafo 2, del trattato sull'Unione

---

[92] GU L 281 del 1995, pag. 31.

[93] GU 1998 L 24/1.

[94] Art. 3 par. 2 dir. 95/46.

[95] Art. 1 par. 3 dir. 97/66.

[96] COM (2000) 385 def., GU C 365 E/223.

[97] Regolamento (CE) n. 45/2001, GU 2001 L 8/1.

[98] Art. 3 par. 1; cfr. altresì il considerando 15 "Qualora tale trattamento venga effettuato dalle istituzioni e organi comunitari per esercitare attività che esulano dall'ambito di applicazione del presente regolamento, e in particolare quelle di cui ai titoli V e VI del trattato sull'Unione europea, la tutela dei diritti e delle libertà fondamentali delle persone è garantita ai sensi dell'articolo 6 del trattato sull'Unione europea. L'accesso ai documenti, anche contenenti dati personali, è soggetto alle disposizioni adottate in base all'articolo 255 TCE, che si applica anche ai titoli V e VI del TUE".

[99] Cfr. ad esempio il punto 25 della risoluzione relativa al piano d'azione del Consiglio e della Commissione concernente la miglior collocazione delle disposizioni del trattato di Amsterdam relative alla realizzazione di uno spazio di libertà, sicurezza e diritto (13844/98 - C4-0692/98 - 98/0923(CNS)), GU C 219 del 30.7.1999, pag. 61 e segg.

europea, in cui l'Unione si impegna a rispettare i diritti fondamentali garantiti dalla CEDU e riconosciuti dalle tradizioni costituzionali degli Stati membri. In aggiunta al carattere obbligatorio dei diritti fondamentali, in particolare della CEDU, per gli Stati membri (cfr. al riguardo il capitolo 8), ne deriva anche un'obbligatorietà dei diritti fondamentali per l'Unione nello svolgimento della sua attività legislativa ed amministrativa. Ma data l'assenza, finora, di una normativa sull'ammissibilità della sorveglianza delle telecomunicazioni a fini di sicurezza o di raccolta di informazioni da parte dei servizi d'informazione[100], non si pone per intanto la questione della violazione dell'articolo 6, paragrafo 2 del trattato UE.

7.3. La questione della compatibilità in caso di impiego abusivo del sistema a fini di spionaggio economico

Qualora uno Stato membro desse il proprio sostegno ad un sistema d'intercettazione che comprendesse tra le proprie attività anche lo spionaggio della concorrenza, consentendo la strumentalizzazione dei propri servizi d'informazione o, rispettivamente, mettendo il proprio territorio a disposizione di servizi d'informazione esteri per tali fini, ci si troverebbe senz'altro in presenza di una violazione del diritto comunitario. Infatti, gli Stati membri, a norma dell'articolo 10 del trattato CE, hanno un obbligo di lealtà totale, che comprende in particolare il divieto di tutte le misure che potrebbero inibire la realizzazione degli obiettivi del trattato. Anche nel caso in cui la captazione di telecomunicazioni non avvantaggiasse l'economia dello Stato membro interessato (eventualità che, tra l'altro, equivarrebbe all'erogazione di un aiuto di Stato, in violazione dell'articolo 87 del trattato CE), bensì quella o quelle di paesi terzi, tale attività risulterebbe in radicale contraddizione con il concetto fondamentale del trattato CE del mercato comune, perché comporterebbe una distorsione del gioco della concorrenza.

Un tale comportamento, a parere del relatore, costituirebbe anche una violazione della direttiva sulla protezione dei dati nel settore delle telecomunicazioni[101], perché la questione dell'applicabilità delle direttive va affrontata mediante interpretazioni funzionali e non organizzative. Ciò non si evince solamente dalla formulazione letterale della norma del campo di applicazione, ma anche dal senso della legge. Se i servizi d'informazione fanno uso delle loro potenzialità a fini di spionaggio economico, allora la loro attività non si svolge a fini di sicurezza o di giustizia penale, bensì esula dai compiti istituzionali dei servizi e ricade pienamente nel campo di applicazione della direttiva. Quest'ultima, però, obbliga gli Stati membri (articolo 5) a garantire la riservatezza delle comunicazioni, vietando in particolare "l'ascolto, l'intercettazione, la memorizzazione o altri generi di intercettazione o di sorveglianza delle comunicazioni ad opera di persone diverse dagli utenti". A norma dell'articolo 14, sono ammesse eccezioni solo se

[100] Nel settore della sorveglianza delle telecomunicazioni attualmente esistono in ambito UE solo due testi legislativi, nessuno dei quali disciplina la questione dell'ammissibilità:

- la risoluzione del Consiglio del 17 gennaio 1995 sull'intercettazione legale delle telecomunicazioni (GU C 329 del 4.11.1996), il cui allegato contiene requisiti tecnici per la realizzazione di misure legali di sorveglianza in sistemi moderni di telecomunicazione e

- l'atto del Consiglio del 29 maggio 2000 che stabilisce, conformemente all'articolo 34 del trattato sull'Unione europea, la convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea (GU C 197 del 12.7.2000, pag. 1, art. 17 f), che definisce le condizioni a cui è possibile l'assistenza giudiziaria in materia penale relativamente all'intercettazione delle telecomunicazione. I diritti degli intercettati non ne risultano assolutamente sminuiti perché lo Stato membro in cui risiede l'intercettato può sempre vietare l'assistenza giudiziaria ove non sia ammissibile a norma del proprio diritto interno.

[101] Direttiva 97/66/CE, GU L 24 del 1998, pag. 1.

sono necessarie per motivi di sicurezza dello Stato, difesa del territorio o giustizia penale. Poiché lo spionaggio economico non è motivo ammissibile di deroga, anche in questo caso si sarebbe in presenza di una violazione del diritto comunitario.

7.4. Conseguenze

In conclusione, possiamo affermare che allo stato attuale del diritto un sistema di raccolta di informazioni del tipo ECHELON non viola il diritto dell'Unione europea, perché non presenta le intersezioni con il diritto dell'Unione necessarie per causare un'incompatibilità. Ciò vale unicamente se il sistema viene utilizzato esclusivamente al servizio della sicurezza dello Stato. Se invece l'impiego che se ne fa esula dai compiti istituzionali e risulta finalizzato ad atti di spionaggio della concorrenza ai danni di imprese estere, allora risulta in violazione del diritto comunitario. Qualora ciò avvenisse con la partecipazione di uno Stato membro, quest'ultimo si troverebbe in violazione del diritto comunitario.

8. La compatibilità della sorveglianza delle comunicazioni da parte di servizi d'informazione con il diritto fondamentale alla vita privata

8.1. Sorveglianza delle comunicazioni quale violazione del diritto fondamentale alla vita privata

Tutte le intercettazioni di comunicazioni, anche solo la raccolta di dati da parte di servizi di informazione al fine di realizzarle[102], costituiscono una profonda violazione della vita privata del singolo cittadino. Solo in uno "Stato di polizia" è consentita l'intercettazione senza restrizioni da parte dello Stato. Per contro, negli Stati membri dell'UE, democrazie mature, è universalmente riconosciuta la necessità del rispetto della vita privata da parte degli organi di Stato - compresi dunque anche i servizi d'informazione -, sancita di norma dalle costituzioni dei singoli Stati. La vita privata gode pertanto di una tutela particolare e le deroghe ad essa sono ammesse unicamente previa considerazione dell'equilibrio giuridico e nel rispetto del principio di proporzionalità.

Anche negli Stati ECHELON esiste la consapevolezza di questa problematica. Le misure di tutela previste riguardano comunque il rispetto della vita privata dei cittadini di quegli stessi Stati e dunque non giovano di norma al cittadino europeo. Secondo le norme statunitensi che disciplinano la sorveglianza elettronica, l'interesse dello Stato di disporre di un servizio d'informazione funzionante non è contrapposto agli interessi di un'efficace tutela generale di un diritto fondamentale, bensì della tutela necessaria della vita privata di "US-Persons".[103]

8.2. La tutela della vita privata in virtù di accordi internazionali

Il rispetto della vita privata quale diritto fondamentale è sancito da numerosi accordi di diritto internazionale[104]. A livello mondiale, occorre citare in particolare il "Patto internazionale sui diritti civili e politici"[105] delle Nazioni Unite del 1966, che garantisce, all'articolo 17, la tutela

[102] Deutsches Bundesverfassungsgericht (BVerfG), 1 BvR 2226/94 del 14.7.1999, Rz 187 "Eingriff ist [...] schon die Erfassung selbst, insofern sie die Kommunikation für den Bundesnachrichtendienst verfügbar macht und die Basis des nachfolgenden Abgleichs mit den Suchbegriffen bildet."

[103] Cfr. la relazione al Congresso americano di fine febbraio 2000 "Legal Standards for the Intelligence Community in Conducting Electronic Surveillance", http://www.fas.org/irp/nsa/standards.html, quella sul Foreign Intelligence Surveillance Act (FISA), riportata al titolo 50, capitolo 36 U.S.C. par. 1801 e segg. e l'Exec. Order No. 12333, 3 C.F.R. 200 (1982), riportato al titolo 50, capitolo 15 U.S.C. par. 401 e segg., http://www4.law.cornell.edu/uscode/50/index.html.

[104] Articolo 12 della Dichiarazione universale dei diritti dell'uomo; articolo 17 del Patto internazionale sui diritti civili e politici delle Nazioni Unite; articolo 7 della Carta dell'Unione europea, articolo 8 della CEDU; raccomandazione del Consiglio dell'OCSE su direttive per la sicurezza dei sistemi di informazione, adottata il 26-27.11.1993 C(92) 188 def.; articolo 7 della Convenzione del Consiglio d'Europa relativa all'elaborazione automatica dei dati personali; cfr. lo studio commissionato dallo STOA "Sviluppo delle tecnologie di sorveglianza e rischio di impiego abusivo di informazioni economiche; volume 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), ottobre 1999, 2.

[105] Patto internazionale sui diritti civili e politici, adottato dall'Assemblea generale delle Nazioni Unite il 16.12.1966.

della vita privata. Tutti gli Stati ECHELON accettano l'arbitrato della Commissione dei diritti umani istituita a norma dell'articolo 41 per statuire sulle violazioni del patto a norma del diritto internazionale, ove si tratti di querele presentate da altri Stati. Il Protocollo addizionale[106], che estende le competenze della commissione dei diritti umani a reclami individuali, non è stato sottoscritto dagli Stati Uniti, con la conseguenza che in caso di violazione del patto da parte di questi ultimi i singoli cittadini non hanno la possibilità di rivolgersi alla Commissione dei diritti umani.

A livello dell'UE, si è cercato di realizzare una tutela fondamentale speciale europea attraverso la redazione di una "Carta dei diritti fondamentali dell'Unione europea". L'articolo 7 della Carta, intitolato "Rispetto della vita privata e della vita familiare", disciplina esplicitamente il diritto al rispetto delle comunicazioni[107]. Inoltre, l'articolo 8 disciplina il diritto fondamentale alla "protezione dei dati di carattere personale". Tale norma avrebbe tutelato il singolo nei casi in cui i suoi dati (in modo automatico o non automatico) fossero stati trattati, come di norma avviene nel caso di intercettazioni e di altre captazioni.

La Carta non è ancora stata integrata nel trattato, e pertanto le disposizioni in essa contenute hanno un effetto vincolante solo per i tre organi che l'hanno accolta nella "Dichiarazione solenne" a margine del Consiglio europeo di Nizza, vale a dire Consiglio, Commissione e Parlamento europeo. Secondo il relatore, detti organi non sono in alcun modo coinvolti in attività di servizi segreti. Anche nel momento in cui la Carta verrà inserita nel trattato ed entrerà pienamente in vigore si dovrà considerare con molta attenzione il suo ristretto ambito di applicazione. Ai sensi dell'articolo 51 le disposizioni della Carta si applicano "… alle istituzioni e agli organi dell'Unione … come pure agli Stati membri esclusivamente nell'attuazione del diritto dell'Unione." Gli effetti della Carta si produrrebbero tutt'al più con il divieto degli aiuti di Stato che creano condizioni perniciose per la concorrenza (cfr. capitolo7, 7.3).

L'unico strumento efficace, a livello internazionale, per la protezione globale della vita privata deriva dalla Convenzione europea dei diritti dell'uomo.

8.3. La normativa della Convenzione europea dei diritti dell'uomo (CEDU)

8.3.1. Importanza della CEDU nellambito dell'UE

La tutela dei diritti fondamentali riconosciuta dalla CEDU assume particolare importanza nella misura in cui la Convenzione è stata ratificata da tutti gli Stati membri dell'UE e pertanto costituisce un livello unitario europeo di tutela. Gli Stati firmatari della Convenzione si sono impegnati, a norma del diritto internazionale, a garantire i diritti sanciti dalla CEDU e hanno accettato di sottostare alle decisioni della Corte europea dei diritti dell'uomo di Strasburgo. Pertanto, la Corte di Strasburgo può controllare che le varie norme nazionali adempiano alla CEDU e, in caso di violazione dei diritti umani, condannare gli Stati a pagare un risarcimento. Inoltre, la CEDU ha acquistato prestigio in seguito alle ripetute istanze in cui la Corte di giustizia

[106] Protocollo addizionale al Patto internazionale sui diritti civili e politici, adottato dall'Assemblea generale delle Nazioni Unite il 16.12.1966.

[107] "Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni."

delle Comunità europee, nell'ambito di cause pregiudiziali, l'ha posta accanto ai principi giuridici generali degli Stati membri considerati per formulare una decisione. Il trattato di Amsterdam, all'articolo 6, paragrafo 2 del trattato UE, ha poi stipulato l'obbligo dell'UE a rispettare i diritti fondamentali garantiti dalla CEDU.

8.3.2. Estensione territoriale e personale della tutela garantita dalla CEDU

I diritti sanciti dalla CEDU stabiliscono diritti umani generali, dunque non vincolati ad una cittadinanza, che devono essere garantiti a tutti coloro che sono soggetti alla giurisdizione degli Stati firmatari. Ciò significa che i diritti umani devono essere sempre riconosciuti su tutto il territorio degli Stati firmatari, in quanto deroghe locali costituirebbero una violazione della Convenzione. Inoltre, tali diritti valgono anche al di fuori del territorio degli Stati firmatari nella misura in cui anche il loro potere politico viene esercitato al di fuori di essi. I diritti garantiti dalla CEDU nei confronti di uno Stato firmatario valgono anche per coloro che si trovano al di fuori del territorio dello Stato stesso, purché quest'ultimo ne abbia violato la vita privata al di fuori di esso[108].

Da ultimo, riveste qui particolare importanza, perché la questione dei diritti fondamentali presenta la particolarità, nel settore della sorveglianza delle telecomunicazioni, per cui lo Stato responsabile della sorveglianza, il soggetto sorvegliato e l'effettiva intercettazione possono trovarsi in territori diversi. Ciò vale soprattutto per le comunicazioni internazionali, ma può valere anche per le comunicazioni nazionali ove queste usufruiscano di collegamenti all'estero. Nel caso dell'attività di servizi d'informazione esteri, questa configurazione è il caso più tipico. Non si può nemmeno escludere che le informazioni ottenute con la sorveglianza svolta da un servizio d'informazione possano essere trasmesse ad altri Stati.

8.3.3. Ammissibilità della sorveglianza delle telecomunicazioni a norma dell'articolo 8 della CEDU

Ai sensi dell'articolo 8, paragrafo 1 della CEDU "ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza." La tutela della telefonia o della telecomunicazione non viene nominata esplicitamente, ma secondo la giurisprudenza della Corte europea dei diritti dell'uomo essa rientra nella tutela riconosciuta attraverso i concetti di "vita privata" e "corrispondenza" di cui all'articolo 8 della CEDU[109]. L'estensione della tutela del diritto fondamentale non si limita al contenuto della comunicazione, ma comprende anche la rilevazione di altri dati relativi alla conversazione. Ciò significa che anche quando il servizio d'informazione si limita a rilevare dati quali ora e durata della comunicazione e il numero composto, si ravvisa una violazione della vita privata[110].

---

[108] Cfr. Corte europea dei diritti dell'uomo, Loizidou/Turchia, 23.3.1995, punto 62 con ulteriori rimandi "...the concept of 'jurisidiction' 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" con appunto alla Corte europea dei diritti dell'uomo, Drozd e Janousek, 26.6.1992, punto 91. Cfr. l'esauriente Jacobs, The European Convention on Human Rights (1996), pag. 21 e segg.

[109] Cfr. Corte europea dei diritti dell'uomo, Klass e a., 6.9.1978, punto 41.

[110] Cfr. Corte europea dei diritti dell'uomo, Malone, 2.8.1984, punto 83 e segg.; nonché Davy, B/Davy/U, Aspekte staatlicher Informationssammlung und Art 8 MRK, JBl 1985, pag. 656.

L'articolo 8, paragrafo 2 della CEDU non garantisce questo diritto senza apporvi restrizioni. Violazioni del diritto fondamentale alla vita privata possono essere ammesse ove siano giuridicamente giustificate dalla legge dello Stato interessato[111]. Il diritto deve essere generalmente accessibile e deve avere conseguenze prevedibili.[112]

Gli Stati membri non hanno piena libertà nella definizione di queste violazioni. L'articolo 8 della CEDU le ammette esclusivamente per la realizzazione degli obiettivi elencati al paragrafo 2, in particolare la sicurezza nazionale, l'ordine pubblico, la prevenzione dei reati, ma anche il benessere economico della nazione[113], il che comunque non giustifica lo spionaggio economico, in quanto comprende unicamente violazioni "necessarie in una società democratica". In ciascun caso occorre utilizzare il mezzo più moderato possibile adatto al raggiungimento dello scopo e devono essere costituite garanzie sufficienti contro gli abusi.

8.3.4. Conseguenze dell'articolo 8 della CEDU per l'attività dei servizi di informazione

In base a questi principi generali, per strutturare l'attività dei servizi d'informazione in modo che sia conforme alla legge, occorre considerare quanto segue. Ove il mantenimento della sicurezza nazionale appaia giustificare l'intercettazione o quanto meno la raccolta di dati di connessione da parte dei servizi d'informazione, ciò deve essere previsto dalla legge dello Stato interessato e la norma deve essere accessibile a tutti. Le conseguenze devono essere prevedibili per il singolo, badando però a tutelare le speciali esigenze di segretezza dei servizi. La Corte, in una decisione sulla conformità all'articolo 8 di controlli segreti di dipendenti in settori sensibili per la sicurezza nazionale, ha statuito che l'esigenza di prevedibilità in questo caso specifico non può essere uguale a quella vigente in altri settori[114]. Ma anche in questo caso, la Corte ha posto l'esigenza che la legge debba specificare le circostanze e condizioni in presenza delle quali il potere politico è autorizzato a violare segretamente - con la potenziale pericolosità che questo comporta - la vita privata di un individuo[115].

Affinché l'attività dei servizi d'informazione non risulti lesiva dei diritti umani, occorre badare a che la sicurezza nazionale ne giustifichi l'operato nel rispetto del principio di proporzionalità sancito dall'articolo 8, paragrafo 2 della CEDU: anche la sicurezza nazionale può giustificare violazioni solo se queste sono necessarie in una società democratica. La Corte europea dei diritti dell'uomo ha chiaramente affermato che l'interesse dello Stato di tutelare la propria sicurezza

---

[111] Secondo la giurisprudenza della Corte europea dei diritti dell'uomo (in particolare Sunday Times, 26.4.1979, punto 46 e segg., Silver e a., 25.3.1983, punto 85 e segg.) il concetto "law" (legge) di cui all'articolo 8, paragrafo 2 non comprende solo leggi in senso formale, ma anche disposizioni giuridiche di livello inferiore agli atti legislativi, nonché addirittura il diritto non scritto. La condizione è, in ogni caso, che sia riconoscibile da parte del soggetto in quali circostanze possa avvenire la violazione. Cfr. al riguardo Wessley, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht? ÖJZ 1999, pag. 491 e segg., pag. 495.

[112] Silver e a., 25.3.1983, punto 87 e segg.

[113] La giustificazione del "benessere economico" è stata accolta dalla Corte europea dei diritti dell'uomo in una causa relativa al trasferimento di dati medici significativi per l'assegnazione di risarcimenti pubblici M.S./Svezia, 27.8.1997, punto 38; nonché in una causa relativa all'espulsione dai Paesi Bassi di una persona che viveva della previdenza sociale in seguito al venir meno del motivo per cui le era stato rilasciato un permesso di soggiorno Ciliz/Paesi Bassi, 11.7.2000, punto 65.

[114] Corte europea dei diritti dell'uomo, Leander, 26.3.1987, punto 51.

[115] Corte europea dei diritti dell'uomo, Malone, 2.8.1984, punto 67.

nazionale va bilanciato con la gravità con cui si ledono gli interessi del singolo nel momento in cui se ne viola la vita privata[116]. Tali violazioni non sono limitate ai casi imprescindibili, ma d'altra parte non basta a giustificarle allegarne semplicemente l'utilità o l'auspicabilità[117]. Il punto di vista secondo cui l'intercettazione di tutte le comunicazioni rappresenterebbe la miglior protezione contro la criminalità organizzata sarebbe contrario all'articolo 8 della CEDU anche se fosse ammesso dalla legislazione statale.

Inoltre, considerando il carattere particolare dell'attività dei servizi d'informazione, che richiede la riservatezza e la ricerca di un equilibrio degli interessi in gioco, occorre prevedere possibilità di controllo specialmente rigorose. La Corte di Strasburgo ha chiaramente affermato che un sistema segreto di sorveglianza finalizzato al mantenimento della sicurezza nazionale comporta il rischio di minare o addirittura distruggere la democrazia che presume di difendere, rendendo dunque necessario costituire garanzie adeguate ed efficaci contro gli abusi[118]. L'attività legale dei servizi di sicurezza è dunque giuridicamente giustificata solo se lo Stato firmatario della CEDU ha disposto adeguati sistemi di controllo ed altre garanzie contro gli abusi. Al riguardo, la Corte di Strasburgo ha dichiarato, relativamente all'attività dei servizi d'informazione svedesi, di attribuire particolare importanza alla presenza di deputati in seno all'organo di controllo della polizia, nonché alla sorveglianza svolta dal ministro della Giustizia, dal difensore civico parlamentare e della commissione Giustizia del parlamento. Desta invece preoccupazione il fatto che Francia, Grecia, Irlanda, Lussemburgo e Spagna non dispongano di nessuna commissione parlamentare di controllo specifica per i servizi segreti[119] e di nessun sistema di controllo equivalente al difensore civico parlamentare degli Stati nordici[120]. Il relatore accoglie quindi favorevolmente le iniziative della commissione Difesa dell'Assemblé Nationale francese volte ad istituire una commissione di controllo[121], tanto più che la Francia, per motivi tecnici e geografici, dispone di notevoli capacità nell'attività dei suoi servizi d'informazione.

8.4. L'obbligo di vigilanza sull'attività dei servizi d'informazione esteri

8.4.1. Inammissibilità dell'aggiramento dell'articolo 8 della CEDU attraverso l'intervento di servizi di informazione esteri

Come esaurientemente esposto, gli Stati firmatari devono soddisfare una serie di condizioni affinché l'attività dei loro servizi d'informazione risulti compatibile con l'articolo 8 della CEDU. È evidente che i servizi d'informazione non possono liberarsi da questi obblighi valendosi dell'attività di altri servizi di informazione vincolati da norme meno severe. Altrimenti, il

[116] Corte europea dei diritti dell'uomo, Leander, 26.3.1987, punto 59, Sunday Times, 26.4.1979, punto 46 e segg.

[117] Corte europea dei diritti dell'uomo, Silver e a., 24.10.1983, punto 97.

[118] Corte europea dei diritti dell'uomo, Leander, 26.3.1987, punto 60.

[119] A conoscenza del relatore, Lussemburgo e Irlanda non dispongono di servizi d'informazione competenti per l'estero o di un SIGINT. L'esigenza di un'istanza di controllo speciale si riferisce qui unicamente alle attività del servizio d'informazione nell'ambito del territorio nazionale.

[120] Sulla situazione del controllo dei servizi d'informazione negli Stati membri cfr. il capitolo 9.

[121] Cfr. al riguardo la proposta legislativa "Proposition de loi tendant à la création de délégations parlementaires pour le renseignement", e la relativa relazione del deputato Arthur Paecht, N° 1951 Assemblée nationale, 11a legislatura, registrata il 23 novembre 1999.

principio di legalità, con entrambe le sue componenti di accessibilità e prevedibilità, risulterebbe invalidato e la giurisprudenza della Corte di Strasburgo inficiata nei contenuti.

Ne deriva, da un lato, che lo scambio di dati tra servizi d'informazione è ammissibile solo con restrizioni. Un servizio d'informazione può richiedere dati ad un altro servizio d'informazione solo se i dati in questione sono stati ottenuti in condizioni tali da adempiere alle prescrizioni del diritto nazionale del richiedente. Il campo d'azione previsto dalla legge non può essere ampliato attraverso accordi con altri servizi. Analogamente, un servizio può svolgere attività per conto di un servizio straniero applicandone le istruzioni solo se ne ha verificato la compatibilità con il proprio diritto nazionale. Anche se le informazioni sono destinate ad un altro Stato, ciò nulla toglie all'illegalità di una violazione dalle conseguenze imprevedibili per il soggetto giuridico interessato.

Dall'altro lato, gli Stati firmatari della CEDU non possono autorizzare servizi d'informazione esteri ad operare sul loro territorio ove sussista il dubbio che le loro attività non adempiano alle prescrizioni della CEDU[122].

8.4.2. Conseguenze delle attività tollerate di servizi d'informazione extraeuropei svolte sul territorio degli Stati membri della CEDU

8.4.2.1. La giurisprudenza pertinente della Corte europea dei diritti dell'uomo

Con la ratifica della CEDU, gli Stati firmatari si sono impegnati a subordinare l'esercizio della loro sovranità al controllo costituzionale. Essi non possono liberarsi da quest'obbligo rinunciando alla loro sovranità. Gli Stati rimangono responsabili del loro territorio e pertanto responsabili nei confronti dei soggetti giuridici europei nel caso in cui l'esercizio dell'autorità territoriale sia usurpato dall'attività dei servizi segreti di un altro Stato. La giurisprudenza costante della Corte di Strasburgo afferma inoltre l'obbligo degli Stati firmatari di adottare misure positive a tutela della vita privata onde evitare violazioni dell'articolo 8 della CEDU anche da parte di privati (!), dunque a livello orizzontale, ponendo così il caso in cui il singolo non si trovi contrapposto al potere dello Stato, bensì ad un'altra persona[123]. Se uno Stato consente che un servizio segreto straniero operi sul proprio territorio, l'esigenza di tutela ne risulta sostanzialmente maggiore, perché in questo caso un'altra autorità ne esercita la sovranità territoriale. È dunque logico dedurne che lo Stato debba vigilare sul rispetto dei diritti umani da parte dei servizi segreti attivi sul proprio territorio.

8.4.2.2. Conseguenze per le stazioni

La Germania concede agli Stati Uniti d'America l'uso del proprio territorio, a Bad Aibling, al fine esclusivo di effettuare captazioni satellitari. A Menwith Hill, in Gran Bretagna, esiste una situazione di uso comune del territorio per lo stesso scopo. Se in queste stazioni un servizio segreto americano intercettasse comunicazioni non militari di privati o imprese originanti in uno Stato firmatario della CEDU, entra in gioco l'obbligo di sorveglianza ai sensi della CEDU. All'atto pratico, ciò significa che la Germania e il Regno Unito, quali firmatari della CEDU,

[122] Cfr. al riguardo anche Yernault, "Echelon" et l'Europe. La protection de la vie privée face à l'espionnage des communications, Journal des tribunaux, Droit Européen 2000, pagg. 187 e segg.

[123] Corte europea dei diritti dell'uomo, Abdulaziz, Cabales e Balkandali, 28.5.1985, punto 67; X e Y/Paesi Bassi, 26.3.1985, punto 23; Gaskin/Regno Unito 7.7.1989, punto 38; Powell e Rayner, 21.2.1990, punto 41.

hanno l'obbligo di verificare la costituzionalità dell'operato dei servizi segreti americani. Tanto più che rappresentanti della NRO e della stampa hanno ripetutamente espresso dubbi sull'attività della NSA.

8.4.2.3. Conseguenze per le intercettazioni eseguite per incarico estero

A Morwenstow, in Gran Bretagna, secondo informazioni in nostro possesso, il GCHQ in collaborazione con la NSA e su istruzioni di quest'ultima capta comunicazioni civili e le trasmette agli USA in forma di materiale grezzo. Anche in caso di attività svolte per incarico di terzi vale l'obbligo di verificare la costituzionalità della richiesta.

8.4.2.4. Obbligo particolare di cautela nei confronti di paesi terzi

Gli Stati firmatari della CEDU possono, entro certi limiti, ritenere reciprocamente che ambe le parti osservano quanto prescritto dalla Convenzione, a meno che risulti di uno Stato firmatario che viola la CEDU in modo sistematico e permanente. Nel caso degli Stati Uniti, si tratta di uno Stato che non è Parte della CEDU e non si è assoggettato a nessun sistema di controllo equivalente. L'attività dei suoi servizi d'informazione è meticolosamente regolamentata ove riguardi cittadini americani o residenti legali degli Stati Uniti, ma l'attività della NSA all'estero è disciplinata da altre norme di cui molte sono coperte da segreto e pertanto inaccessibili. Desta poi ulteriore preoccupazione il fatto che nonostante i servizi d'informazione americani siano sottoposti al controllo di commissioni del Congresso e del Senato, tali commissioni parlamentari mostrano scarso interesse per l'attività della NSA all'estero.

Appare quindi opportuno fare appello alla Germania e al Regno Unito affinché prendano sul serio gli obblighi derivanti dalla CEDU e subordinino l'autorizzazione di ulteriori attività di servizio d'informazione della NSA sui loro territori alla loro compatibilità con la CEDU. A tal fine, occorre prendere in considerazione tre aspetti principali.

1. A norma della CEDU le violazioni della vita privata sono lecite solo se fondate su norme di diritto generalmente accessibili e le cui conseguenze per il singolo sono prevedibili. Questo requisito è adempiuto solo se gli Stati Uniti rendono pubblico ai cittadini europei come e in che circostanze vengono eseguite le investigazioni. Fintanto che esistono incompatibilità con la CEDU, occorre adeguare le norme al livello europeo di tutela.

2. A norma della CEDU, le violazioni non possono essere sproporzionate ed occorre porre in atto il mezzo più moderato possibile. Dal punto di vista del cittadino europeo, una violazione commessa da parte europea è meno grave di una commessa da parte americana, in quanto ha la possibilità di adire le istanze giuridiche solo nel primo caso[124]. Pertanto, nella misura del possibile, le violazioni devono essere commesse da parte tedesca e inglese, e in ogni caso quelle che rientrano nel campo di applicazione della procedura penale. La parte americana ha tentato più volte di giustificare l'intercettazione di telecomunicazioni con l'accusa di corruzione ed estorsione da parte europea[125]. Occorre ricordare agli Stati Uniti che tutti gli Stati dell'UE dispongono di sistemi penali funzionanti. In caso di circostanze sospette, gli USA devono lasciare che gli Stati interessati si occupino del procedimento penale. In assenza di tali

[124] Ne deriva anche la conformità con l'articolo 13 della CEDU, che conferisce alla parte lesa il diritto di adire le istanze nazionali.

[125] Woolsey (ex direttore della CIA), Why America Spies on its Allies, The Wall Street Journal Europe, 22.3.2000, 31.

circostanze, la sorveglianza risulta sproporzionata e pertanto lesiva dei diritti umani e come tale inammissibile. La compatibilità con la CEDU si ravvisa dunque unicamente se gli Stati Uniti si limitano ad adottare misure di sorveglianza finalizzate alla loro sicurezza nazionale, astenendosi dall'intervenire a fini della giustizia penale.

3. Come si è detto, la giurisprudenza della Corte di Strasburgo relativa alla costituzionalità esige l'esistenza di sistemi di controllo e garanzie contro gli abusi. Ne consegue che la sorveglianza delle telecomunicazioni sul territorio europeo da parte degli Stati Uniti è compatibile con i diritti umani solo se gli USA, nei casi in cui captano dal loro territorio comunicazioni ai fini di mantenere la loro sicurezza nazionale, mettono in atto controlli efficaci o, rispettivamente, se la NSA subordina la propria attività sul territorio europeo alle istituzioni di controllo dello Stato ospitante (rispettivamente Germania o Regno Unito).

Affinché l'attività di captazione di telecomunicazioni da parte degli Stati Uniti risulti compatibile con la CEDU devono essere osservate le condizioni esposte nei tre punti precedenti ed occorre garantire il rispetto del livello integrale di tutela in Europa stipulato dalla CEDU.

9. I cittadini dell'UE sono sufficientemente tutelati rispetto all'attività dei servizi d'informazione?

9.1. Tutela dall'attività dei servizi d'informazione: un compito dei parlamenti nazionali

L'attività dei servizi d'informazione potrà costituire un aspetto futuro della politica estera e di sicurezza comune, ma poiché attualmente non esiste a livello dell'UE nessuna normativa in tal senso[126], la configurazione della tutela dall'attività dei servizi d'informazione dipende esclusivamente dagli ordinamenti giuridici nazionali.

I parlamenti nazionali svolgono una doppia funzione: nella loro veste legislativa decidono sia sull'entità e sulle attribuzioni delle agenzie di spionaggio, che sulla struttura del controllo delle loro attività. Come discusso esaurientemente nel capitolo precedente, i Parlamenti, nell'elaborare le norme che disciplinano l'ammissibilità della sorveglianza delle telecomunicazioni, devono attenersi alle restrizioni stipulate dall'articolo 8 della CEDU, vale a dire che le norme adottate devono essere necessarie, proporzionate e tali da avere conseguenze prevedibili per i singoli interessati, oltre a prevedere meccanismi di controllo adeguati ed efficaci relativi alle attribuzioni delle autorità di controllo.

Inoltre, i Parlamenti nazionali hanno, nella maggior parte degli Stati, un ruolo attivo di controllo, poiché il controllo dell'esecutivo (e quindi dei servizi di spionaggio) costituisce, accanto alla funzione legislativa, la seconda funzione "classica" di un parlamento. La configurazione di questi aspetti, tuttavia, presenta notevoli differenze da uno Stato membro all'altro dell'UE e spesso si verifica la coesistenza di organi parlamentari e non parlamentari.

9.2. Attribuzioni delle autorità nazionali relativamente all'attuazione di misure di sorveglianza

Le misure di sorveglianza attuate dallo Stato sono ammesse, di norma, ai fini della giustizia penale, del mantenimento dell'ordine pubblico e della sicurezza dello Stato[127] (contro minacce esterne).

Ai fini della giustizia penale, in tutti gli Stati membri è ammesso derogare alla riservatezza delle telecomunicazioni ove sussista sufficiente sospetto della perpetrazione di un reato (talvolta specificamente qualificato, ovvero di maggior gravità rispetto ad altri) da parte di una persona in concreto. In considerazione della gravità della violazione derogata, di norma è necessaria l'autorizzazione di un giudice[128] ed esistono norme precise relative alla durata consentita della sorveglianza, ai controlli ed alla cancellazione dei dati.

---

[126] Cfr. al riguardo anche il capitolo 7.

[127] Questi scopi sono riconosciuti anche dall'art. 8, par. 2 della CEDU quali motivi giustificati per violare la *privacy*. Cfr. al riguardo *supra* 8.3.2.

[128] Ma dispone altrimenti il diritto britannico, che conferisce la decisione dell'autorizzazione al Secretary of State (Regulation of Investigatory Powers Act 2000, Section 5 (1) e (3) (b)).

Per garantire la sicurezza interna e l'ordine pubblico, la raccolta di informazioni da parte dello Stato viene ampliata in indagini individuali in caso di concreti sospetti di attività criminale. Ai fini del riconoscimento tempestivo di movimenti estremisti o sovversivi, il legislatore nazionale autorizza l'ottenimento di ulteriori informazioni su determinate persone o gruppi. La raccolta di dati pertinenti e l'analisi degli stessi sono competenza di speciali servizi di informazione interni.

Da ultimo, le misure di sorveglianza attuate ai fini della sicurezza dello Stato rappresentano una quota considerevole delle attività di questo tipo. Il trattamento, la valutazione e la presentazione di informazioni rilevanti su paesi stranieri è di norma competenza di un apposito servizio segreto competente per l'estero[129]. Generalmente la sorveglianza non riguarda individui specifici, bensì particolari settori o frequenze. A seconda dei mezzi a disposizione del servizio segreto competente per l'estero e delle sue attribuzioni legali, è possibile avere un ampio spettro, dal semplice ascolto di comunicazioni radio militari di onda corta alla sorveglianza di tutti i tipi di connessioni di telecomunicazione verso l'estero. In alcuni Stati membri la sorveglianza delle telecomunicazioni a fini di spionaggio è vietata[130], mentre in altri essa - in alcuni casi previa autorizzazione di una commissione indipendente[131] - è autorizzata mediante ordinanza ministeriale[132] e per alcune forme di comunicazione può avvenire senza restrizioni[133]. Le attribuzioni proporzionalmente ampie di taluni servizi segreti derivano dal fatto che essi si dedicano alla sorveglianza di comunicazioni effettuate all'estero, che quindi riguardano solo in piccola misura i cittadini del paese cui appartiene il servizio, destando per questo motivo ben pochi scrupoli.

9.3. Il controllo dei servizi d'informazione

È particolarmente importante effettuare controlli efficaci e completi perché da un lato i servizi d'informazione operano in condizioni di segretezza, svolgono attività di lunga durata e le persone interessate spesso non hanno riscontri della sorveglianza di cui sono oggetto per lungo tempo o (secondo quale sia la legge vigente) mai, e dall'altro lato perché le misure di sorveglianza spesso riguardano ampi gruppi mal definiti di persone, per cui lo Stato può entrare in possesso in brevissimo tempo di un'ingente quantità di dati personali.

Naturalmente tutti gli organismi di controllo - indipendentemente dalla loro struttura - si trovano ad affrontare il problema per cui, a causa del particolare carattere dei servizi segreti, spesso è quasi impossibile determinare se tutte le informazioni raccolte siano poi messe a disposizione o se una parte di esse venga occultata. È questo un ulteriore incentivo ad adottare una normativa rigorosa. Fondamentalmente si può ritenere che un'elevata efficienza dei controlli e di conseguenza una garanzia durevole della legalità delle violazioni sono possibili se il potere di

[129] Riguardo all'attività dei servizi di spionaggio all'estero cfr. l'esposizione completa al capitolo 2.

[130] Come in Austria e in Belgio.

[131] Come avviene in Germania, a norma del Gesetz zur Beschränkung des Brief-, Post-, und Fernmeldegeheimnisses (Gesetz zu Artikel 10 Grundgesetz). Ai sensi del par. 9, la commissione (salvo in caso di urgenza) deve essere informata prima dell'esecuzione.

[132] Così in Gran Bretagna (Regulation of Investigatory Powers Act, Section 1) e in Francia per comunicazioni via cavo (Art. 3, 4 Loi 91-646 du 10 Juillet 1991, loi relative au secret des correspondances émises par la voie des télécommunications).

[133] Così avviene per le comunicazioni via etere in Francia (art. 20 Loi 91-646 du 10 Juillet 1991, loi relative au secret des correspondances émises par la voie des télécommunications).

autorizzazione della sorveglianza delle telecomunicazioni è riservata al livello amministrativo più alto, se è necessaria la autorizzazione preventiva di un giudice per poter procedere e se un organo indipendente vigila anche sull'esecuzione delle misure. Inoltre, la democrazia politica e lo Stato di diritto sono considerazioni che portano ad auspicare che l'operato dei servizi segreti, compatibilmente con il principio della divisione dei poteri, sia integralmente sottoposto al controllo di un organo parlamentare. Ciò si verifica pienamente in Germania, dove le misure di sorveglianza delle telecomunicazioni sono decise dal ministro federale competente. Salvo in casi in cui un ritardo sarebbe pericoloso occorre, prima di procedere, informare dell'azione una commissione indipendente e non vincolata ("G10-Kommission"[134]), che delibera sulla necessità e sull'ammissibilità delle misure proposte. Nei casi in cui il servizio segreto tedesco per l'estero BND sia giustificato a procedere alla sorveglianza di telecomunicazioni via etere con l'ausilio di filtri attraverso termini chiave di ricerca, la commissione delibera anche sull'ammissibilità dei termini chiave. La "G-10 Kommission" esercita anche i controlli sulla comunicazione, obbligatoria per legge, agli interessati, nonché sulla distruzione dei dati ottenuti da parte della BND.

Esiste anche un organo parlamentare di controllo (PKGr)[135], composto da 9 deputati del Parlamento nazionale, che vigila sull'attività dei tre servizi d'informazione tedeschi. Il PKGr ha diritto di accesso ai documenti, di ascolto degli addetti ai servizi d'informazione e di visita dei servizi e indagine; quest'ultimo diritto può essergli negato solo per gravi motivi di accesso alle informazioni o di tutela dei diritti personali di terzi, oppure se è in gioco il cuore della responsabilità specifica dell'esecutivo. Le deliberazioni del PKGr sono segrete ed i suoi membri sono tenuti alla riservatezza anche dopo la fine dell'incarico. A metà e alla fine della legislatura il PKGr trasmette al Bundestag tedesco una relazione sull'attività di controllo.

Un controllo così completo, praticamente a tenuta stagna, dei servizi segreti è comunque l'eccezione negli Stati membri.

In Francia[136], per esempio, richiedono l'autorizzazione del Primo Ministro solo le misure di sorveglianza che comportano l'intercettazione da cavi. Solo queste ultime sono sottoposte al controllo di un'apposita commissione (Commission nationale de contrôle des interceptions de sécurité), cui appartengono un deputato e un senatore. L'autorizzazione di un'intercettazione da parte di un ministro o di un suo delegato passa al vaglio del presidente della commissione, che in caso di dubbio sull'ammissibilità può presentarla all'esame della commissione, la quale emana poi raccomandazioni e, ove ritenga essere in presenza di un'infrazione rilevante, ne informa il pubblico ministero. Intercettazioni finalizzate alla difesa di interessi nazionali che comportano l'ascolto di comunicazioni via etere - dunque anche via satellite - non sono sottoposte a nessuna restrizione ed esulano pertanto dal controllo di una commissione.

Inoltre, l'operato dei servizi segreti francesi non è sottoposto al controllo di una commissione parlamentare specifica, sebbene siano in corso iniziative in tal senso. La commissione Difesa

---

[134] Cfr. al riguardo il completo: Die Parlamentarische Kontrolle der Nachrichtendienste in Deutschland, Stand 9.9.2000, edito dal Deutscher Bundestag, Sekretariat des PKGr.

[135] Gesetz über die Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (PKGrG) vom 17. Juni 1999 BGBl I 1334 idgF.

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

dell'Assemblea nazionale ha adottato una proposta in tal senso[137], ma la discussione in plenaria non ha ancora avuto luogo.

Nel Regno Unito ogni sorveglianza di comunicazioni su territorio britannico richiede l'autorizzazione ministeriale ("Secretary of State"). La formulazione della legge, tuttavia, non chiarisce se la captazione generica di un ampio spettro di comunicazioni, successivamente vagliate in base a parole chiave, rientri anch'essa nel concetto di "interception" quale è impiegato nella "Regulation of Investigatory Powers Act 2000" (RIP) qualora il vaglio non avvenga su territorio britannico, bensì il "materiale grezzo" venga inviato all'estero prima di essere esaminato. Il controllo dell'osservanza di quanto disposto dal RIP 2000 è affidato (ex post) a "Commissioner", giudici di alta istanza in servizio o in pensione nominati dal Primo Ministro. Il "Commissioner" responsabile delle misure di intercettazione ("Interception Commissioner") esercita il controllo sulla concessione di autorizzazioni di intercettazione ed appoggia l'investigazione di reclami relativi ad intercettazioni. L'"Intelligence Service Commissioner" vigila sulle autorizzazioni per attività dei servizi segreti e di sicurezza ed appoggia l'investigazione di reclami relativi a questi servizi. L'"Investigatory Powers Tribunal", presieduto da un giudice di alta istanza, indaga su tutti i reclami relativi alle intercettazioni e all'attività dei servizi.

Il controllo parlamentare è svolto dall'"Intelligence and Security Committee" (ISC)[138], che vigila su tutti e tre i servizi d'informazione civili (MI5, MI6 e GCHQ) ed è responsabile, in particolare, della verifica dell'emissione dei risultati e dell'amministrazione, nonché del controllo delle procedure del servizio di sicurezza, del servizio segreto e del GCHQ. La commissione si compone di 9 membri della Camera bassa e della Camera alta, di cui nessuno può ricoprire l'incarico di ministro. A differenza delle commissioni di controllo di altri Stati, che generalmente sono prescelte o nominate dal parlamento o dal presidente del parlamento, i membri di questa commissione sono nominati dal Primo Ministro previa consultazione con i capi dell'opposizione.

Questi esempi bastano per vedere quanto il livello di tutela differisca da uno Stato all'altro. Per quanto riguarda il controllo parlamentare, il relatore desidera rilevare che l'esistenza di una commissione specifica di controllo per la sorveglianza dei servizi d'informazione è molto importante. Tali commissioni presentano il vantaggio, rispetto a commissioni generiche, di godere di maggiore fiducia da parte dei servizi d'informazione, poiché i loro membri sono tenuti alla riservatezza e le loro riunioni non sono pubbliche. Inoltre, esse dispongono di diritti particolari, conferiti per consentire loro di svolgere il loro speciale compito, circostanza che risulta imprescindibile per la sorveglianza di attività segrete.

Fortunatamente, la maggior parte degli Stati membri dell'UE ha istituito commissioni parlamentari specifiche di controllo. In Belgio[139], Danimarca[140], Germania[141], Italia[142], Paesi

[137] Cfr. al riguardo la proposta di legge "Proposition de loi tendant à la création de délégations parlementaires pour le renseignement", e la relativa relazione del deputato Arthur Paecht, N° 1951 Assemblée nationale, 11a Legislatura, registrato il 23 novembre 1999.

[138] Intelligence services act 1994, Section 10.

[139] 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.

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

Bassi[143] e Portogallo[144] esistono commissioni parlamentari di controllo responsabili di controllare i servizi segreti militari e civili. Nel Regno Unito[145] la commissione speciale di controllo sorveglia unicamente i servizi d'informazione civili (che tuttavia sono di gran lunga i più importanti), mentre i servizi militari sono sottoposti al controllo della generica commissione di difesa. In Austria[146] i due rami del servizio segreto sono competenza di due diverse commissioni di controllo, organizzate nello stesso modo e dotate degli stessi diritti. Negli Stati nordici di Finlandia[147] e Svezia[148], sono incaricati del controllo parlamentare difensori civici indipendenti nominati dal Parlamento. In Francia, Grecia, Irlanda, Lussemburgo e Spagna non esiste nessuna commissione parlamentare specifica e l'attività di controllo è svolta unicamente dalle commissioni generiche nel contesto dell'attività generale del Parlamento.

9.4. Valutazione della situazione per il cittadino europeo

La situazione in Europa per il cittadino europeo appare poco soddisfacente. Le attribuzioni dei servizi d'informazione nel settore della sorveglianza delle telecomunicazioni sono assai diverse tra loro in quanto alla portata e lo stesso vale per le commissioni di controllo. Non tutti gli Stati membri che dispongono di un servizio d'informazione si sono dotati di organi parlamentari di controllo indipendenti muniti delle necessarie attribuzioni di controllo. Siamo molto lontani dall'avere un livello uniforme di protezione.

Dal punto di vista dell'Europa questa situazione è tanto più deplorevole in quanto essa non incide particolarmente sui cittadini degli Stati interessati, i quali attraverso l'esercizio democratico del voto potrebbero influire sul grado di protezione esistente. Le conseguenze negative riguardano principalmente cittadini di altri Stati, poiché il campo di azione dei servizi d'informazione si trova prevalentemente fuori dei confini nazionali. Il singolo cittadino si trova relativamente indifeso di fronte all'azione di sistemi stranieri, nei confronti dei quali vi è quindi una maggiore esigenza di tutela. Non bisogna poi dimenticare che a motivo del carattere particolare dei servizi segreti, i cittadini dell'UE possono essere interessati contemporaneamente dall'attività di più

---

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

[142] 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.

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

[144] Conselho de Fiscalização dos Serviços de Informações (CFSI), legge 30/84 del 5 settembre 1984, modificata dalla legge 4/95 del 21 febbraio 1995, legge 15/96 del 30 aprile 1996 e legge 75-A/97 del 22 luglio 1997.

[145] Intelligence and Security Committee (ISC), intelligence services act 1994, Section 10.

[146] Ständigen Unterausschuss des Landesverteidigungsausschusses zur Überprüfung von nachrichtendienstlichen Maßnahmen zur Sicherung der militärischen Landesverteidigung und dem Ständigen 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.

[147] Mediatore parlamentare, fondamento giuridico per il controllo per la polizia (SUPO): Poliisilaki 493/1995 §33 e Laki pakkokeinolain 5 a luvun muuttamisesta 366/1999 §15, per le forze armate: Poliisilaki 493/1995 §33 e Laki poliisin tehtävien suorittamisesta puolustusvoimissa 1251/1995 §5.

[148] Rikspolisstyrelsens ledning, Förordning (1989:773) med instruktion för Rikspolisstyrelsen (Ordinanza (1989:773) sull'autorità nazionale di polizia).

servizi di spionaggio. Un livello uniforme di protezione adeguato ai principi democratici sarebbe auspicabile in questo caso. In questo contesto, occorre anche riflettere sulla fattibilità di promulgare in questo campo direttive di protezione dei dati a livello dell'UE.

Inoltre, la questione della tutela del cittadino europeo si porrà nuovamente allorché, nell'ambito della politica di sicurezza comune, si inizierà una collaborazione tra servizi d'informazione degli Stati membri. Al riguardo, si invitano le istituzioni europee a promulgare norme di tutela adeguate. Sarà compito del Parlamento europeo, quale difensore dei principi dello Stato di diritto, premere per svolgere la funzione di controllo che gli corrisponde in qualità di organo democraticamente legittimato. Si coglie anche l'occasione per invitare il Parlamento europeo a realizzare le condizioni affinché il trattamento riservato di dati sensibili e di altri documenti segreti sia affidato ad una commissione appositamente istituita i cui membri siano tenuti alla riservatezza. Solo soddisfacendo queste condizioni diventerà realistico e, in considerazione di una collaborazione funzionante dei servizi d'informazione - collaborazione assolutamente indispensabile ai fini di una politica di sicurezza comune credibile - responsabile esigere questi diritti di controllo.

10. La tutela contro lo spionaggio economico

10.1. Gli obiettivi dello spionaggio economico

In un'impresa economica rispetto alla segretezza si possono delineare tre categorie di informazioni. In primo luogo vi sono informazioni a cui viene data di proposito **la più ampia diffusione possibile**. Si tratta di informazioni specifiche relative ai prodotti dell'impresa (ad esempio caratteristiche del prodotto, prezzi, e così via) e di informazioni pubblicitarie che influenzano l'immagine dell'impresa.

In secondo luogo vi sono informazioni **che vengono protette e diffuse attivamente**, in quanto non riguardano la posizione concorrenziale dell'impresa. Tra queste si annoverano ad esempio la data della gita aziendale, il menu della mensa o la marca del fax utilizzato.

Infine vi sono informazioni che vengono **protette dalla conoscenza da parte di terzi**. Tali informazioni sono tutelate contro la concorrenza, ma anche nei confronti dello Stato se un'impresa non intende rispettare le leggi (fisco, regole sull'embargo, e così via) Al riguardo esistono gradi diversi di protezione fino alla segretezza assoluta, ad esempio rispetto ai risultati della ricerca in caso di domanda di brevetto o in merito alla produzione di armamenti[149].

Nel caso in questione lo spionaggio ha come obiettivo ottenere le informazioni tenute segrete da un'impresa. Se il mandante è un'impresa concorrente, si parla di **spionaggio della concorrenza** (nonché di spionaggio aziendale, spionaggio industriale). Se invece il mandante è un servizio di informazione statale si parla di **spionaggio economico.**

10.1.1. Gli obiettivi dello spionaggio nel dettaglio

I dati strategici rilevanti per lo spionaggio economico si possono classificare per categorie o settori aziendali.

10.1.1.1. Categorie

È evidente che le informazioni relative ai seguenti settori rivestono grande interesse: biotecnologia, tecnologia genetica, tecnologia relativa al settore medico e ambientale, computer ad alto rendimento, software, optoelettronica, tecnica dell'immagine, dei sensori e dei segnali, memorizzazione dati, ceramica tecnica, leghe ad alto rendimento, nanotecnologia. L'elenco non è completo e si modifica del resto al passo con lo sviluppo tecnologico. In questi settori lo spionaggio riguarda soprattutto il furto di risultati della ricerca o a specifiche tecniche di produzione.

10.1.1.2. Settori aziendali

Gli obiettivi dello spionaggio riguardano logicamente i settori relativi a ricerca e sviluppo, acquisti, personale, produzione, distribuzione, vendita, commercializzazione, linee di produzione e finanze. Spesso si sottovalutano il significato e l'importanza di tali dati (cfr. *infra* 10.1.4).

[149] Informationen für geheimschutzbetreute Unternehmen, BMWI 1997.

10.1.2. Spionaggio della concorrenza

La posizione strategica di un'impresa sul mercato dipende dalla sua situazione nei settori ricerca e sviluppo, processi di produzione, linee di produzione, finanziamento, commercializzazione, vendita, distribuzione, acquisti e forze lavoro[150]. Le informazioni in materia sono di grande interesse per ogni concorrente sul mercato, perché offrono indicazioni in merito ai piani e ai punti deboli e consentono quindi di adottare contromisure strategiche.

Una parte di queste informazioni è pubblicamente accessibile. Vi sono aziende di consulenza altamente specializzate che operando in piena legalità conducono studi sulla concorrenza, tra cui si annoverano imprese rinomate, quali ad esempio Roland & Berger in Germania. Del resto negli Stati Uniti la "competitive intelligence" fa parte dei normali strumenti della gestione[151]. Dall'insieme di singole informazioni tramite un'analisi professionale è possibile ricavare un quadro chiaro della situazione.

Il passaggio dalla legalità allo spionaggio illegale della concorrenza è determinato dalla scelta dei mezzi con cui vengono raccolte le informazioni. Soltanto se gli strumenti utilizzati sono illegali secondo lo specifico ordinamento giuridico, l'azione diventa un reato, mentre lo svolgimento di analisi in sé non è perseguibile. L'accesso alle informazioni che rivestono particolare interesse per la concorrenza è naturalmente protetto e si può ottenere soltanto violando la legge. Le tecniche utilizzate a tal fine non si differenziano in alcun modo dai metodi generali di spionaggio descritti nel capitolo 2.

Non esistono dati precisi in merito all'entità dello spionaggio della concorrenza. Le cifre ufficiose, come nel caso dello spionaggio tradizionale, sono molto elevate. Entrambe le parti interessate (esecutori e vittime) non hanno alcun interesse che la cosa sia resa di pubblico dominio. Per le imprese coinvolte questo significa sempre un danno a livello di immagine e naturalmente neanche i colpevoli hanno interesse a pubblicizzare le loro attività. Per questo soltanto pochi casi sono portati dinanzi al tribunale.

Ciononostante sempre più spesso la stampa riporta informazioni relative allo spionaggio della concorrenza. Il relatore ha inoltre discusso di tale questione con alcuni responsabili della sicurezza di importanti imprese tedesche[152] e con dirigneti di società americane ed europee. In generale si può constatare che lo spionaggio della concorrenza continua ad esistere, anche se non rappresenta una pratica quotidiana.

10.2. I danni arrecati dallo spionaggio economico

A causa delle elevate cifre ufficiose non si riesce a definire con esattezza l'entità del danno arrecato dallo spionaggio della concorrenza e dallo spionaggio economico. Questa situazione è imputabile al fatto che una parte delle cifre citate sono alte per ragioni di interesse. Aziende che si occupano della sicurezza e servizi di controspionaggio hanno un comprensibile interesse a collocare il danno al massimo grado della scala realisticamente possibile. Ciononostante le cifre forniscono una certa idea.

---

[150] M. F. Porter, Competitive Strategy.

[151] Hummelt, Roman, Wirtschaftsspionage auf dem Datenhighway, Hanserverlag, Monaco 1997.

[152] Nomi e dettagli sono riservati.

Già nel 1988 il Max Planck Institut ha stimato che i danni arrecati dallo spionaggio economico in Germania sono equivalenti almeno a 8 miliardi di marchi[153].Il presidente della federazione tedesca delle aziende di consulenza in materia di sicurezza indica sulla base delle valutazioni di esperti un importo pari a 15 miliardi di marchi l'anno. Hermann Lutz, presidente del sindacato europeo di polizia, ritienne che il danno sia di 20 miliardi di marchi l'anno. L'FBI[154] calcola per il 1992/1993 un danno di 1,7 miliardi di dollari arrecato all'economia americana dallo spionaggio della concorrenza ed economico. L'ex presidente della commissione di controllo dei servizi segreti dell'House of Representatives degli Stati Uniti parla di una perdita pari a 100 miliardi di dollari, legata alle commesse perse e agli ulteriori costi per la ricerca e lo sviluppo. Tra il 1990 e il 1996 questo ha comportato una perdita di 6 milioni di posti di lavoro.[155]

In sostanza non è necessario conoscere con precisione l'entità del danno. A prescindere dall'entità del danno economico è compito dello Stato agire tramite polizia e servizi segreti contro lo spionaggio della concorrenza ed economico. Anche per quanto riguarda le decisioni in seno alle imprese in merito alla protezione delle informazioni e all'adozione di proprie misure di controspionaggio le cifre del danno complessivo non costituiscono una base necessaria. Ogni impresa deve valutare il massimo danno possibile che è in grado di sostenere per la sottrazione di informazioni, calcolare le previsioni di entrate e confrontare gli importi risultanti con i costi per la sicurezza. Il vero problema non riguarda la mancanza di cifre precise relative al danno complessivo. Accade piuttosto che ad eccezione delle grandi imprese non si effettuano quasi mai simili valutazioni del rapporto costi/vantaggi con un conseguente danno per la sicurezza.

10.3. Chi pratica lo spionaggio?

Secondo uno studio della Società di analisi economica Ernest Young[156] i principali committenti dello spionaggio nei confronti delle imprese sono per il 39% concorrenti, per il 19% clienti, per il 9% fornitori e per il 7% servizi segreti. Lo spionaggio è ad opera di propri collaboratori, agenzie private di spionaggio, hacker pagati e professionisti dei servizi segreti[157].

10.3.1. Propri collaboratori (reati interni)

La letteratura consultata, le indicazioni in merito fornite dagli esperti in seno alla commissione e i colloqui del relatore con responsabili della sicurezza ed autorità di controspionaggio concordano nell'indicare che il maggior rischio a livello di spionaggio è imputabile a collaboratori delusi o insoddisfatti. In qualità di impiegati dell'impresa hanno accesso diretto alle informazioni, si fanno corrompere con offerte di denaro e sottraggono a beneficio dei loro committenti segreti aziendali.

Si corrono rischi notevoli anche in caso di cambio di lavoro. Oggi non è più necessario copiare montagne di documenti per sottrarre alle imprese informazioni importanti. Si possono registrare di nascosto su dischetto e una volta cambiato posto di lavoro fornirle al nuovo datore.

---

[153] IMPULSE, 3/97, pag.13 e segg.

[154] Congressional Statement, L. J. Freech, direttore dell'FBI, 9.5.1996.

[155] Robert Lyle, Radio Liberty/Radio free Europe, 10 febbraio 1999.

[156] Computerzeitung, 30.11.1995, pag. 2.

[157] R. Hummelt, Spionage auf dem Datenhighway, Monaco 1997, pag. 49 e segg.

10.3.2. Agenzie private di spionaggio

Il numero delle agenzie specializzate nello spionaggio di dati continua a crescere. Talvolta vi lavorano ex collaboratori di servizi di informazione. Tali agenzie svolgono spesso sia attività di consulenza in materia di sicurezza che attività di investigazione con lo scopo di sottrarre informazioni su commissione. Di solito vengono impiegati mezzi legali, ma vi sono anche agenzie che ricorrono a metodi illegali.

10.3.3. Hacker

Gli "hacker" sono esperti informatici che grazie alle loro competenze possono accedere dall'esterno a reti informatiche. All'inizio gli hacker erano appassionati di computer che si divertivano a superare le misure di sicurezza di sistemi informatici. Oggi vi sono hacker che lavorano su commissione sia nei servizi sia sul mercato.

10.3.4. Servizi d'informazione

Con la fine della guerra fredda i compiti dei servizi di informazione sono cambiati. I loro nuovi campi di azione sono la criminalità organizzata e il settore economico (maggiori informazioni nel capitolo 10, 10.5).

10.4. Come si effettua lo spionaggio?

Secondo le indicazioni delle autorità di controspionaggio e dei responsabili della sicurezza di grandi imprese, nello spionaggio economico vengono impiegati tutti i metodi e gli strumenti sperimentati dai servizi di informazione (cfr. capitolo 2, 2.4). Le imprese dispongono tuttavia di strutture più aperte rispetto alle istituzioni militari, ai servizi di informazione o agli uffici governativi. Rispetto allo spionaggio economico si aggiungono pertanto alcuni rischi:

- il reclutamento dei collaboratori è più facile perché le possibilità in materia di sicurezza di un'impresa non sono paragonabili a quelle delle autorità di controspionaggio;
- la mobilità dei posti di lavoro implica che molte informazioni siano registrate su computer portatili. Rubare computer portatili o copiare furtivamente il disco fisso dopo essersi introdotti nella camera d'albergo fa parte pertanto delle tecniche normali utilizzate dallo spionaggio economico;
- l'accesso alle reti informatiche è più semplice che nel caso di istituzioni di sicurezza statali perché proprio nelle piccole e medie imprese la consapevolezza e le precauzioni in materia di sicurezza sono molto meno diffuse;
- per gli stessi motivi è molto più semplice carpire informazioni ascoltandole in loco (cfr. capitolo 3, 3.2).

La valutazione delle informazioni raccolte in proposito dimostra che lo spionaggio economico avviene per lo più in loco o in caso di trasferte, perché è possibile con meno eccezioni (cfr. *infra* 10.6) reperire le informazioni cercate senza ricorrere alle reti internazionali di telecomunicazione.

10.5. Spionaggio economico da parte degli Stati

10.5.1. Spionaggio economico strategico da parte dei servizi di informazione

Con la fine della Guerra Fredda si sono rese disponibili capacità dei servizi d'informazioni, oggi impiegate in altri settori. Gli USA dichiarano apertamente che una parte delle attività dei loro servizi di informazione riguardano anche l'economia. Tra queste si annoverano, ad esempio, la sorveglianza sul rispetto delle sanzioni economiche, delle regole sul traffico di armi e sui cosiddetti beni a duplice uso, il controllo degli sviluppi sui mercati delle materie prime e dell'andamento dei mercati finanziari internazionali. Secondo le informazioni del relatore non sono soltanto i servizi statunitensi ad occuparsi di questo settore e al riguardo non vi sono critiche rilevanti.

10.5.2. I servizi d'informazione quali agenti dello spionaggio della concorrenza

Le critiche si levano quando i servizi di informazione statali vengono impiegati in modo abusivo per procurare tramite lo spionaggio vantaggi a livello di concorrenza internazionale ad imprese del territorio nazionale. Al riguardo occorre distinguere due casi[158].

10.5.2.1. Stati hightech

Stati industriali altamente sviluppati possono trarre ampio vantaggio dallo spionaggio industriale. Grazie allo spionaggio sullo sviluppo di un settore si possono adottare misure specifiche in materia di economia estera e di politica delle sovvenzioni che rendono più competitiva la propria industria o consentono di risparmiare a livello di sovvenzioni. Un altro punto chiave può consistere nel reperire informazioni dettagliate in caso di commesse di alto valore (cfr. *infra* 10.6).

10.5.2.2. Stati meno sviluppati a livello tecnologico

Per alcuni di questi Stati si tratta di procurarsi il know-how tecnico che consenta di ovviare all'arretratezza della propria industria senza dover affrontare costi di sviluppo e tasse di concessione. Un altro obiettivo consiste nell'impossessarsi di documenti relativi a prodotti e a tecniche di produzione, al fine di diventare competitivi sul mercato mondiale tramite copie realizzate a basso costo (retribuzioni!). È dimostrato che i servizi russi hanno ricevuto espressamente tale incarico. La legge n. 5 della federazione russa sull'informazione estera contempla espressamente tra i compiti dei servizi di informazione il reperimento di informazioni economiche e tecnico-scientifiche.
Per altri Stati (ad esempio Iran, Irak, Siria, Libia, Corea del Nord, India e Pakistan) si tratta di carpire informazioni per i loro programmi nazionali di armamento soprattutto nel settore nucleare e in quello delle armi biologiche e chimiche. Un altro aspetto dell'attività dei servizi di questi Stati consiste nella gestione di imprese fittizie per l'acquisto non sospetto di beni a duplice uso.

10.6. ECHELON si presta allo spionaggio industriale?

Lo spionaggio della concorrenza può ottenere solo in modo fortuito informazioni importanti con il controllo strategico delle telecomunicazioni a livello internazionale. Di fatto, soprattutto all'interno delle imprese stesse si trovano dati aziendali sensibili, **e pertanto lo spionaggio della**

[158] Colloquio privato del relatore con un addetto del servizio di controspionaggio, fonte riservata.

concorrenza si traduce soprattutto nel tentativo di ottenere informazioni dai dipendenti o tramite soggeti introdotti clandestinamente oppure cercando di inserirsi nelle reti informatiche interne. Solo nel caso in cui i dati sensibili vengono trasmessi all'esterno via cavo o via radio (satellite) si può impiegare un sistema di sorveglianza delle comunicazioni a fini di spionaggio della concorrenza. Tale situazione si verifica in modo sistematico nei seguenti tre casi:

- imprese che operano in tre aree geografiche con fuso orario diverso, i cui risultati intermedi vengono inviati dall'Europa verso l'America e quindi trasmessi in Asia;

- videoconferenze di multinazionali trasmesse tramite sistemi V-sat o via cavo;

- ordini importanti le cui trattative si svolgono in loco (ad esempio installazione di impianti, costruzione di infrastrutture delle telecomunicazioni, costruzione di nuovi sistemi di trasporto, e così via), e da lì devono essere definiti con la sede centrale.

Se in questi casi le imprese non proteggono le loro comunicazioni, la loro intercettazione fornisce dati importanti per lo spionaggio della concorrenza.

10.7. Casi pubblicati

La stampa e la letteratura specializzata hanno riportato alcuni casi di spionaggio economico e della concorrenza. La tabella di seguito illustrata riassume una parte delle fonti analizzate e indica brevemente il soggetto coinvolto, il periodo in cui è avvenuto il fatto, il caso nello specifico, l'obiettivo e le conseguenze.

La particolarità è che talvolta le informazioni in merito ad uno stesso caso non sono omogenee, come per quanto riguarda, ad esempio, Enercon, per il quale si indica come "colpevole" l'NSA, oppure il ministero dell'Economia statunitense o ancora il concorrente autore delle fotografie.

Caso	Chi	Quando	Cosa	Come	Obiettivo	Conseguenze	Fonte
Air France	DGSE	fino al 1994	Conversazioni di uomini d'affari in viaggio	Nelle cabine di prima classe di Air France sono nascoste alcune comici – La compagnia aerea ha presentato pubblicamente le proprie scuse	Raccogliere informazioni	Non comunicate	"Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?" di Arno Schütze, 1/
Airbus	NSA	1994	Informazioni sugli affari tra Airbus e la linea aerea arabo-saudita	Intercettazione di fax e telefonate tra i partner	Passare informazioni ai concorrenti amercani Boeing e Mc-Donnell-Douglas	Gli americani concludono l'affare da 6 miliardi di dollari	"Antennen gedreht", Wirtschaftswoche Nr.46/9 novembre 2000
Airbus	NSA	1994	Contratto di oltre 6 miliardi di dollari con l'Arabia Saudita Corruzione del gruppo europeo Airbus.	Intercettazione di fax e telefonate tra il gruppo europeo Airbus e la compagnia aerea/il governo sauditi tramite satelliti per le comunicazioni	Scoprire casi di corruzione	McDonnel-Douglas, il concorrente americano di airbus, conclude l'affare	"Sviluppo delle tecnologie di sorveglianza e rischio di impeigo abusivo di informazioni economiche", Vol 2/5 10 1999 STOA, di Duncan Campbell
BASF	Vertriebsman n	Non comunic ato	Descrizione di processi per la produzione di materie prime per creme per la pelle della società BASF (settore della cosmesi)	Non comunicato	Non comunicato	Nessuna, perché tentativo sventato	"Nicht gerade zimperlich", Wirtschaftswoche Nr.43 / 16. Ottobre 1992
Ministero federale dell'Economi a (Germania)	CIA	1997	Informazioni su prodotti di alta tecnologia nel ministero federale dell'Economia	Impiego di un agente	Raccogliere informazioni	L'agente viene scoperto nel tentativo di agire ed espulso	"Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?" di Arno Schütze, 1/98
Ministero federale dell'Economi a (Germania)	CIA	1997	Retroscena del processo "Mykonos" di Berlino, finanziamenti della Hermes per esportazioni in Iran, creazione di imprese tedesche fornitrici di prodotti di alta tecnologia all'Iran	Un agente della CIA sotto mentite spoglie di ambasciatore statunitense ha avuto colloqui in via amichevole con il direttore del dipartimento competente per la regione araba (punto focale: l'Iran) in seno al ministero federale dell'Economia	Raccogliere informazioni	Non comunicate Il funzionario si è rivolto alle autorità tedesche competenti per la sicurezza, che hanno fatto presente agli uffici americani di non gradire l'operazione della CIA. L'agente della CIA è stato quindi "allontanato".	"Wirtschaftsspionage. Die gewerbliche Wirtschaft im Visier fremder Nachrichtendienste", Landesamt für Verfassungsschutz Baden-Württemberg, Stoccarda, Edizione: 1998
Dasa	Servizi d'informazion e russi	1996 – 1999	Vendita e trasmissione di documenti sulla tecnologia degli armamenti di un'impresa di Monaco del settore (SZ / 30.05.2000: gruppo Dasa nel settore degli armamenti a	Incarico affidato a 2 tedeschi	Raccogliere informazioni su missili teleguidati, sistemi d'arma (anticarro e antiaerei)	SZ / 30.05.2000: "(...) Tradimento sotto il profilo militare " non particolarmente grave". Il tribunale si è pronunciato negli stessi termini anche per quanto riguardava i	"Anmerkungen zur Sicherheitslage der deutschen Wirtschaft", ASW; Bonn, aprile 2001 "Haftstrafe wegen Spionage

			Ottobrunn)			danni economici.”	für Russland”, SDZ / 30 maggio 2000
Embargo	BND	circa il 1990	Ripristino delle esportazioni verso la Libia di tecnologia soggetta ad embargo (tra l’atro da parte di Siemens)	Intercettazione delle telecomunicazioni	Scoprire il trasferimento ilelgale di tecnologie ed armi	Nessuna particolare conseguenza, forniture non ostacolate in alcun modo	“Maulwürfe in Nadelstreifen”, Andreas Förster, pag. 110

Caso	Chi	Quando	Cosa	Come	Obiettivo	Conseguenze	Fonte
Enercon	Esperti in energia eolica di Oldenburg e una dipendente di Kenetech	Non comunicato	Impianti di energia eolica della società Enercon	Non comunicato	Non comunicato	Non comunicate	“Anmerkungen zur Sicherheitslage der deutschen Wirtschaft”, ASW; Bonn, aprile 2001
Enercon	NSA	Non comunicato	Ruota eolica per produrre energia elettrica, progettata dall’ingegnere Aloys Wobben della Frisia orientale	Non comunicato	Passare informazioni tecniche di Wobben alla società statunitense	La società statunitense anticipa Wobben nella presentazione della domanda di brevetto per la ruota eolica; Wobben viene accusato dalla cancelleria statunitense (violazione del diritto di brevetto)	“Aktenkrieger”, SZ, 29 marzo 2001
Enercon	Società statunitense Kenetech Windpower Corp	1994	Importanti dettagli di un impianto eolico ad alta tecnologia (dai sezionatori fino alle schede)	Fotografie	Riuscire ad ottenere il brevetto negli USA	La Enercon GmbH presenta alcuni progetti per aprire il mercato americano al ghiaccio	“Sicherheit muss künftig zur Chefsache werden”, HB / 29 agosto 1996
Enercon	Ingegnere W. di Oldenburg e società statunitense Kenetech	marzo 1994	Aerogeneratore tipo E-40 di Enercon	L’ingegnere W. trasmette informazioni, una dipendente di Kenetech fotografa l’impianto + dettagli in campo elettrico	Kenetech: tenta di reperire prove per poter accusare successivamente (1995) Enercon di violazione di brevetto Enercon: raccogliere illegalmente informazioni su segreti aziendali Un ex collaboratore dell’NSA deve aver dichiarato ad un giornalista televiso che gli americani hanno trasmesso a Kenetech tramite Echelon le informazioni raccolte su Enercon.	Non comunicate	“Klettern für die Konkurrenz”, SZ 13 ottobre 2000
Enercon	Kenetech Windpower	prima del 1996	Dati per l’impianto di energia eolica di Enercon	Fotografie dell’impianto scattate dai tecnici di Kenetech	Riprodurre l’impianto presso Kenetech	A Enercon viene data ragione; le spie vengono denunciate; perdita stimata: varie centinaia	“Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?” di Arno

						di milioni di marchi	Schütze, 1/98
Ministero del Commercio del Giappone	CIA	1996	Trattative sui contingenti d'importazione delle autovetture statunitense sul mercato giapponese	Violazione del sistema informatico del ministero del Commercio del Giappone violato ad opera di hacker	Il negoziatore statunitense Mickey Kantor deve accettare l'offerta più bassa	Kantor accetta l'offerta più bassa	"Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?" di Arno Schütze, 1/98
Autovetture giapponesi	Governo statunitense	Non comunicato	Trattative sull'importazione di vetture di lusso giapponesi Informazioni sui livelli normali di emissioni delle vetture giapponesi.	COMINT, nessuna indicazione più precisa	Raccogliere informazioni	Nessuna indicazione	"Sviluppo delle tecnologie di sorvweglianza e rischio di impiego abusivo di informazioni economiche", Vol 2/5 10 1999 STOA, di Duncan Campbell

Caso	Chi	Quando	Cosa	Come	Obiettivo	Conseguenze	Fonte
López	NSA	Non comunicato	Videoconferenza di VW e López	Intercettazione di Bad Aibling	Trasmettere informazioni alla General Motors e alla Opel	Grazie alle intercettazioni il pubblico ministero avrebbe ottenuto "prove molto precise" ai fini dell'indagine	Il comandante delle forze armate Erich Schmidt-Eenboom in "Wenn Freunde spionieren" www.zdf.msnbc.de/news/54637.asp?cp1=1
López	López e tre suoi collaboratori	1992 - 1993	Documenti e dati relativi ai settori di ricerca, pianificazione, lavorazione e acquisti (documentazioni per uno stabilimento in Spagna, costi di varie serie di modelli, studi di progetti, strategie di acquisto e risparmio)	Raccolta di materiale	La VW intende avvalersi della documentazione della General Motors	Dopo il procedimento penale, i due gruppi pervengono ad un accordo extragiudiziale. Nel 1996 López viene reintegrato nella VW come dirigente, nel 1997 la VW interrompe i rapporti con gli altri tre collaboratori del gruppo di López, versa 100 milioni di dollari a GM/Opel (presumibilmente le spese legali) e acquista per 7 anni pezzi di ricambio da GM/Opel per un totale di 1 miliardo di dollari	"Wirtschaftsspionage. Die gewerbliche Wirtschaft im Visier fremder Nachrichtendienste", Landesamt für Verfassungsschutz Baden-Württemberg, Stoccarda, Edizione: 1998
López	NSA	1993	Videoconferenza tra José Ignacio López e il responsabile della VW Ferdinand Piëch	Registrazione della videoconferenza e consegna del nastro alla General Motors (GM)	Proteggere i segreti aziendali della GM americana che López intendeva passare alla VW (listini prezzi, piani segreti su nuove marche di vetture e utilitarie)	López sparisce, nel 1998 inzia un procedimento penale contro pagamento di un'ammenda; nessuna azione nei confronti dell'NSA	"Antennen gedreht", Wirtschaftswoche Nr.46 / 9 novembre 2000 "Abgehört", Berliner Zeitung, 22 gennaio 1996 "Die Affäre López ist beendet", Wirtschaftsspiegel, 28 luglio 1998 "Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?"di Arno Schütze, 1/98
Los Alamos	Israele	1988	Due collaboratori del programma di ricerca nucleare di Israele si inseriscono nel server del laboratorio di armi atomiche di Los Alamos	Pirateria informatica	Raccogliere informazioni sulla nuovo spoletta per armi nucleari degli USA	Nessuna particolare conseguenza, poiché gli hacker fuggono in Israele, dove uno di loro viene temporaneamente messo agli	"Maulwürfe in Nadelstreifen", Andreas Förster, pag. 137

						arresti; non vi è alcuna voce ufficiale che confermi il collegamento con i servizi segreti isrealiani	
Contrabbando	BND	anni ‘70	Contrabbando di computer nella DDR	Non comunicato	Scoprire il trasferimento di tecnologia nel blocco orientale	Nessuna particolare conseguenza, nessun ostacolo alle forniture	“Maulwürfe in Nadelstreifen”, Andreas Förster, pag. 113

Caso	Chi	Quando	Cosa	Come	Obiettivo	Conseguenze	Fonte
TGV	DGSE	1993	Calcolo dei costi di Siemens Contratto per la fornitura alla Corea del Sud di treni ad alta velocità	Non comunicato	Offrire prezzi inferiori	Alcatel-Alsthom si aggiudica l'appalto ai danni del costruttore ICE	"Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?" di Arno Schütze, 1/98
TGV	Sconosciuto	1993	Calcolo dei costi di AEG e Siemens per l'appalto pubblico nella Corea del Sud relativo alla fornitura di treni ad alta velocità	Accusa mossa da Siemens che sostiene che le linee telefoniche e fax della filiale di Seul vengano intercettate	Creare condizioni vantaggiose nelle trattative a favore del concorrente franco-britannico GEC Alsthom	Il committente sceglie GEC Alsthom, sebbene l'offerta tedesca fosse migliore	"Abgehört", Berliner Zeitung, 22 gennaio 1996
Thomson-Alcatel contro Raytheon	CIA/ NSA	1994	Assegnazione alla società francese Thomson-Alcatel di un contratto brasiliano del valore di miliardi (1,4 miliardi di dollari) per la sorveglianza via satellite dell'Amazzonia	Intercettazione delle comunicazioni del vincitore dell'appalto (Thomson-Alcatel, FR)	Scoprire casi di corruzione (pagamento di tangenti)	Il Presidente Clinton reclama presso il governo brasiliano; in seguito alle insistenze del governo statunitense, l'appalto viene assegnato alla società americana "Raytheon"	"Maulwürfe in Nadelstreifen", Andreas Förster, pag. 91
Thomson-Alcatel contro Raytheon	Il ministero statunitense dell'Economia "si è scomodato"	1994	Trattative per un progetto del valore di miliardi sulla sorveglianza via radar della foresta tropicale brasiliana	Non comunicato	Aggiudicarsi l'appalto	Il gruppo francese Thomson CSF e Alcatel perdono l'appalto che viene aggiudicato alla società americana Raytheon	"Antennen gedreht", Wirtschaftswoche Nr.46 / 9 novembre 2000
Thomson-Alcatel contro Raytheon	NSA Ministero per il Commercio	Ministero per il Commercio	Trattative per un progetto del valore di miliardi (1,4 miliardi di dollari) sulla sorveglianza dell'Amazzonia (SIVA) Scoprire casi di corruzione presso il "Selection Panel" (commissione di selezione) brasiliano. Osservazione di Campbell: la Rayethon ha installato una stazione d'intercettazione a Sugar Grove	Intercettazione della trattativa tra la Thomson-CSF e il Brasile e consegna dei risultati alla Raytheon Corp.	Scoprire casi di corruzione Aggiudicarsi l'appalto	La Raytheon si aggiudica l'appalto	"Sviluppo delle tecnologie di sorveglianza e rischio di impiego abusivo di informazioni economiche", Vol 2/5 10 1999 STOA, di Duncan Campbell http://www:rayethon:com/sivam/contract:html
Thyssen	BP	1990	Appalto del valore di milioni per la fornitura di gas e petrolio nel Mare del Nord	Intercettazione di fax del vincitore dell'appalto (Thyssen)	Scoprire casi di corruzione	BP cita Thyssen per il risarcimento dei danni	"Maulwürfe in Nadelstreifen", Andreas Förster, pag. 92
VW	Sconosciuto	"negli anni	Non comunicato	Tra l'altro, videocamera a raggi infrarossi nascosta sotto terra	Raccogliere informazioni su nuovi sviluppi	VW denuncia perdite di utili dell'ordine di 1 miliardo	"Sicherheit muss künftig zur Chefsache werden", HB / 29

		scorsi“		che trasmette immagini via radio			agosto 1996
VW	Sconosciuto	1996	Linea di prova a Ehra-Lessien di VW	Videocamera nascosta	Informazioni su nuovi modelli della VW	Non comunicate	“Auf Schritt und Tritt” Wirtschaftswoche Nr. 25, 11 giugno 1998

10.8. Tutela rispetto allo spionaggio economico

10.8.1. Tutela giuridica

In tutte gli ordinamenti giuridici degli Stati industrializzati il furto di segreti aziendali è punito penalmente. Come per tutti gli altri aspetti del diritto penale anche il livello di tutela varia notevolmente tra i vari paesi. Si può tuttavia affermare che in linea di principio la gravità della pena è chiaramente inferiore rispetto a quella prevista per i casi di spionaggio connessi alla sicurezza militare. Non di rado lo spionaggio della concorrenza è vietato solo nei confronti delle imprese su territorio nazionale e non di quelle all'estero, situazione, questa, cui non si sottraggono neanche gli Stati Uniti.

Le leggi in materia vietano sostanzialmente solo le attività di spionaggio tra imprese del settore industriale, mentre non è certo che impongano limitazioni anche all'operato dei servizi d'informazione dello Stato, in quanto questi ultimi sono autorizzati a sottrarre informazioni in virtù delle normative che li istituiscono.

Si delineerebbe un caso limite qualora i servizi segreti mettessero a disposizione di singole imprese le informazioni ottenute tramite lo spionaggio, poiché di regola le leggi che attribuiscono ai servizi d'informazione particolari poteri non contemplerebbero la fattispecie. In particolare, nell'ambito dell'Unione europea si configurerebbe una violazione del trattato CE (cfr. capitolo…).

A prescindere da tale aspetto, sarebbe tuttavia molto difficile nella pratica formulare una tutela giuridica per un'impresa rivolgendosi ai tribunale, perché l'intercettazione non lascia tracce e non produce alcuna prova che abbia valore legale.

10.8.2. Altri ostacoli per lo spionaggio economico

Gli Stati accettano il fatto che i servizi d'informazione operino anche nel contesto dell'economia per ottenere informazioni strategiche generali. Il cosiddetto "gentlemen agreement" viene tuttavia pesantemente violato a causa dello spionaggio della concorrenza a favore della propria industria. Qualora si possa dimostrare che uno Stato ha agito in tal senso, ne risulta danneggiata non poco la sua immagine politica. Questo vale soprattutto se si tratta di una potenza mondiale quale gli Stati Uniti, che vedrebbero enormemente pregiudicato il loro diritto alla guida politica mondiale. Potenze di media grandezza potrebbero cedere alla tentazione di mettersi in mostra, una potenza mondiale non può.

Oltre ai problemi di natura politica emerge anche una questione di carattere pratico, vale a dire quale singola impresa dovrebbe essere messa a conoscenza dei risultati dello spionaggio della concorrenza. Nel settore delle costruzioni aeronautiche è facile trovare la risposta, perché complessivamente esistono solo due grandi offerenti, mentre in tutti gli altri casi in cui ve ne sono in numero maggiore, inoltre non di proprietà dello Stato, è oltremodo difficile scegliere una singola impresa. Nel caso di informazioni dettagliate sulle offerte dei concorrenti e passate a singole imprese nell'ambito di appalti pubblici internazionali si potrebbe anche ipotizzare di trasmettere informazioni di spionaggio a tutti i concorrenti del proprio paese. Ciò vale in particolare nel caso in cui esista una struttura di sostegno del governo accessibile a tutti i concorrenti nazionali a condizioni di parità, come nel caso del cosiddetto Advocacy Center negli

Stati Uniti. Nel caso di furto di tecnologia, che dovrebbe inevitabilmente tradursi in una domanda di brevetto, non sarebbe logicamente più possibile riservare un trattamento uguale alle imprese.

Tale situazione sarebbe particolarmente problematica per il sistema politico americano. I finanziamenti delle campagne elettorali dei politici americani dipendono in larga misura dalle donazioni delle industrie dei rispettivi collegi elettorali. Se anche solo in un caso si palesasse in modo esemplare che i servizi d'informazione hanno riservato un trattamento privilegiato a singole imprese, si abbatterebbero sul sistema politico enormi accuse. Come ha affermato l'ex direttore della CIA Woolsey in occasione di un incontro con in rappresentanti della commissione "In questo caso la collina (vale a dire il Congresso degli Stati Uniti) impazzirebbe!". Quando ha ragione, ha ragione!

10.9. Gli USA e lo spionaggio economico

10.9.1. La posizione ufficiale degli americani riguardo allo spionaggio economico

La posizione degli americani che l'ex direttore della CIA Woolsey e Porter Gross, presidente della commissione di controllo dei servizi segreti in seno alla House of Representatives, hanno delineato in occasione di alcuni incontri può essere sintetizzata come di seguito riportato.

1. Gli USA sorvegliano le telecomunicazioni internazionali per ottenere informazioni generali sugli sviluppi economici, sulle forniture di beni a duplice uso e sul rispetto degli embarghi.

2. Gli USA sorvegliano le comunicazioni mirate di imprese singole nell'ambito di gare d'appalto al fine di impedire distorsioni del mercato dovute a corruzione ai danni delle imprese statunitensi.

La legge vieta alle società americane di compiere atti di corruzione e i revisori dei conti sono tenuti a comunicare gli eventuali casi di pagamento di tangenti di cui sono venuti a conoscenza. Qualora grazie alla sorveglianza delle comunicazioni si dovessero scoprire casi di corruzione nell'ambito di appalti pubblici, l'ambasciatore britannico interverrebbe presso il governo del rispettivo Stato. Per contro, le società statunitensi candidate non verrebbero direttamente informate.

10.9.2. Il ruolo dell'Advocacy Center nella promozione delle esportazioni statunitensi

10.9.2.1. Funzioni dell'Advocacy Center

L'Advocacy Center in seno al ministero per il Commercio degli Stati Uniti è il fulcro della strategia nazionale per le esportazioni iniziata dal Presidente Clinton e proseguita dall'amministrazione Bush. Il Centro è stato istituito nel 1993 e da allora ha aiutato centinaia di imprese americane ad aggiudicarsi appalti pubblici all'estero. Riunisce le risorse competenti del governo degli Stati Uniti, dagli esperti nei singoli settori agli addetti all'economia delle ambasciate fino a comprendere la Casa Bianca.

10.9.2.2. Attività del Centro

All'interno del centro stesso lavora solo un ristretto gruppo formato da 12 persone (dati al 6.2.2001). Il Centro funge da primo contatto per le imprese nei rapporti con le diverse autorità dell'amministrazione statunitense che si occupano di promuovere le esportazioni. Le imprese non sono soggette ad alcuna discriminazione, tuttavia il Centro sostiene, sulla base di chiare regole, solo progetti nell'interesse nazionale degli USA. I prodotti forniti, ad esempio, devono provenire dagli USA per almeno il 50% del valore.

10.9.2.3. Questioni aperte connesse al Centro

Il governo americano non ha autorizzato che si svolgesse l'incontro programmato tra i membri della commissione e il Centro, e quindi non è stato possibile discutere in modo approfondito due questioni che davano adito a dubbi:

a, la commissione è in possesso di documenti che dimostrano il coinvolgimento della CIA nelle attività del Centro;

b, tra le informazioni messe a disposizione su Internet, il Centro dichiara di raggruppare le risorse di 19 "U.S. government agencies". In un altro punto vengono tuttavia indicati i nomi di sole 14 agenzie. Ci si domanda pertanto il motivo per cui 5 agenzie non vengano espressamente citate.

10.10.La sicurezza delle reti informatiche

verrà inserito successivamente

10.11.Sottovalutare i rischi

verrà inserito successivamente

10.11.1. Grandi imprese

10.11.2. Piccole e medie imprese

10.11.3. Istituzioni europee

10.11.4. Istituzioni di ricerca

11. Autotutela tramite la crittografia

11.1. Finalità e funzionamento della cifratura

11.1.1. Finalità della cifratura

In ogni trasmissione di informazioni esiste il rischio che l'informazione venga intercettata da un estraneo. Se si vuole escludere il rischio che terzi vengano a conoscenza del contenuto della comunicazione, occorre renderla illeggibile o indecifrabile per gli estranei, ovvero occorre cifrarla. Per questo nel settore militare e diplomatico sono state introdotte già da tempo tecniche di cifratura[159].

Negli ultimi vent'anni l'importanza della cifratura è cresciuta, poiché una percentuale sempre maggiore di comunicazioni è stata trasmessa all'estero, e il singolo Stato non poteva più garantire il segreto epistolare e delle telecomunicazioni. Inoltre le possibilità tecniche più avanzate a disposizione di ogni Stato per intercettare o registrare legalmente le comunicazioni hanno comportato una maggiore esigenza di protezione da parte dei cittadini interessati. Ed infine l'accresciuto interesse da parte della criminalità per l'accesso illegale ad informazioni e la loro falsificazione ha reso indispensabile l'adozione di misure di protezione (ad esempio nel settore bancario).

Con l'invenzione della comunicazione elettrica ed elettronica (telegrafo, telefono, radio, telescrivente, fax e Internet) la comunicazione di informazioni è diventata molto più facile e incomparabilmente più rapida. Lo svantaggio è stato l'assenza di qualsiasi forma di protezione **tecnica** che impedisse l'intercettazione o la registrazione, per cui chiunque disponesse di un apparecchio adeguato, riuscendo ad accedere allo strumento che veicolava la comunicazione, era in grado di intercettare la comunicazione. L'intercettazione, se svolta in modo professionale, non lascia praticamente tracce. Pertanto la cifratura ha acquisito un'importanza del tutto nuova. È stato il settore bancario che con l'introduzione dei movimenti finanziari elettronici ha iniziato per primo a proteggere regolarmente con la cifratura la relativa comunicazione. Con la progressiva internazionalizzazione dell'economia si è reso talvolta necessario proteggere la comunicazione anche con la crittografia. In seguito all'ampia diffusione della comunicazione via Internet priva di qualsiasi protezione è sorta l'esigenza anche per i privati di proteggere la comunicazione da possibili intercettazioni.

Nel quadro di questa relazione ci si chiede quindi se esistano metodi di cifratura della comunicazione economici, legali, sufficientemente sicuri e facili da usare che consentano di autotutelarsi contro le intercettazioni.

11.1.2. Funzionamento della cifratura

Il principio della cifratura consiste nel trasformare un testo in chiaro in un testo in codice, in modo tale che venga privato di significato o ne abbia uno diverso. Gli addetti ai lavori possono

[159] Le notizie al riguardo risalgono fino all'antichità, gli Spartani nel V secolo d.C. utilizzavano per esempio lo scitale.

tuttavia riportare il testo alla forma originale. La cifratura trasforma, ad esempio, una sequenza sensata di lettere in una priva di senso che nessuno dall'esterno può comprendere.

Questo è possibile tramite un determinato metodo (algoritmo della cifratura) che si basa sulla traslazione delle lettere (metodo della trasposizione ideale) e/o sulla sostituzione (metodo della sostituzione). Oggi **il metodo della cifratura** (algoritmo) non è tenuto segreto. Al contrario: è stato di recente pubblicato a livello mondiale il nuovo standard globale di cifratura ad uso dell'economia. Questo vale anche per la realizzazione di un determinato algoritmo di cifratura come hardware in un apparecchio, ad esempio in un fax predisposto per la crittografia.

Il **vero segreto** è la cosiddetta **chiave.** Il modo migliore per spiegare questo meccanismo è ricorrere ad un esempio pratico. Di norma il funzionamento delle serrature delle porte è conosciuto, perché sono oggetto di un brevetto. La protezione specifica di una porta dipende dal fatto che per un determinato tipo di serratura possono esistere molti tipi diversi di chiave. Lo stesso accade per la cifratura di informazioni: con **un metodo pubblicamente conosciuto** di cifratura (algoritmo) si possono tenere segrete **molte** informazioni diverse grazie a differenti chiavi specifiche **tenute segrete** dagli interessati.

Per chiarire i concetti sopracitati può essere utile l'esempio del cosiddetto "cifrario di Cesare". Il condottiero romano cifrava le informazioni, sostituendo semplicemente ogni lettera con quella che la seguiva di tre posizioni nell'alfabeto, ovvero A con D, B con E, eccetera. La parola **ECHELON** diventa in questo modo **HFKHORQ.** Quindi, in questo caso, l'**algoritmo di cifratura** consiste in uno **spostamento di lettere** all'interno dell'alfabeto, la **chiave** concreta è l'indicazione di spostarsi di **tre posizione nell'alfabeto!** Sia la cifratura che la decrittazione avvengono nello stesso modo: con lo scorrimento delle lettere di tre posti. Si tratta quindi di un sistema simmetrico. Oggi una protezione di questo tipo non durerebbe più di un secondo!

Nel caso di una buona cifratura il metodo può essere conosciuto pubblicamente e ciononostante la cifratura può essere considerata sicura. È tuttavia necessario che il numero delle chiavi sia talmente alto da rendere impossibile provarle tutte in un determinato periodo di tempo (il cosiddetto **brute force attack - attacco di forza bruta**) anche ricorrendo all'ausilio del computer. D'altro canto la sola presenza di molte chiavi non è indice di sicurezza crittologica, se il metodo della cifratura veicola un testo in codice che contiene spunti per una decrittazione (ad esempio lo spostamento di determinate lettere)[160]. La cifratura di Cesare non è sicura sotto entrambi gli aspetti. Con la semplice sostituzione il metodo può essere decifrato in fretta attraverso le diverse possibilità di spostamento delle lettere in una lingua, dal momento che esistono soltanto 25 possibilità, ovvero 25 chiavi, poiché l'alfabeto consiste soltanto di 26 lettere. Un avversario può scoprire in fretta la chiave: gli è sufficiente fare alcuni tentativi e quindi decifrare il testo.

In seguito si valuteranno i requisiti che un sistema dovrebbe avere per essere sicuro.

[160] Al riguardo cfr. anche Leiberich, Vom diplomatischen Code zur Falltürfunktion - Hundert Jahre Kryptographie in Deutschland, Spektrum der Wissenschaft, giugno 1999, pag. 26 e segg.

11.2. La sicurezza dei sistemi di cifratura

11.2.1. Il concetto di sicurezza della cifratura in generale

Quando si afferma che un sistema di cifratura deve essere "sicuro", si possono intendere due situazioni diverse. Da un lato si può richiedere che esso sia assolutamente sicuro, ovvero che senza conoscere la chiave sia impossibile decifrare il messaggio e che questa impossibilità sia matematicamente certa. Dall'altro lato ci si può accontentare che allo stato attuale della tecnica il codice non possa essere manomesso, il che garantisce la sicurezza per un periodo ampiamente superiore al "periodo critico" entro il quale una notizia dev'essere mantenuta segreta.

11.2.2. La sicurezza assoluta: la chiave infinita o one-time pad

Al momento soltanto l'one-time pad rappresenta un sistema del tutto sicuro. Tale sistema è stato sviluppato verso la fine della prima guerra mondiale[161], ma è stato utilizzato anche in seguito per le telescriventi nelle situazioni di crisi tra Mosca e Washington. Il principio consiste in una chiave che dispone le lettere in modo del tutto casuale, senza ripetere mai lo stesso ordine. Mittente e destinatario comunicano in modo cifrato tramite queste sequenze di lettere e distruggono la chiave non appena è stata usata la prima volta. Poiché non esiste alcuna regola interna alla chiave, è impossibile per un crittoanalista violare il codice. Questo è dimostrato con matematica certezza.[162]

Lo svantaggio di questo sistema è che non è facile creare grandi quantità di chiavi casuali di questo tipo,[163] e che è difficile e poco pratico comunicare per via sicura la chiave. Tale metodo non viene pertanto usato per gli scambi commerciali in generale.

11.2.3. Sicurezza relativa allo stato attuale della tecnica

11.2.3.1. L'impiego di macchine per la cifratura e la decrittazione

Già prima dell'invenzione dell'one-time pad sono state sviluppate procedure crittografiche che mettevano a disposizione un elevato numero di chiavi in grado di elaborare testi in codice contenenti il minor numero possibile di elementi regolari e quindi di punti di riferimento per una crittoanalisi. Al fine di rendere tali metodi applicabili nella pratica con sufficiente rapidità sono state elaborate macchine per la cifratura e la decrittazione. La più spettacolare di questo genere era di certo l'ENIGMA[164], impiegata dalla Germania durante la Seconda guerra mondiale. L'esercito di esperti di decrittazione impegnato a Bletchley Park in Inghilterra riuscì a violare la cifratura dell'ENIGMA con l'aiuto di macchine speciali, le cosiddette "bombe". Sia l'ENIGMA che le "bombe" erano sistemi meccanici.

---

[161] Tale procedura è stata introdotta dal maggiore Joseph Mauborgne, responsabile della sezione di ricerca crittografica dell'esercito americano. Cfr. al riguardo Singh, Geheime Botschaften (1999), pag. 151.

[162] Cfr. al riguardo Singh, Geheime Botschaften (1999), pag. 151 e segg.

[163] Cfr. al riguardo Wobst, Abenteuer Kryptologie^2 (1998), pag. 60.

[164] L'Enigma è stato elaborato da Arthur Scherbius e brevettato nel 1928. Assomigliava in un certo modo ad una macchina per scrivere, poiché era dotato di una tastiera sulla quale veniva digitato il testo in chiaro. Mediante una serie di contatti elettrici e cilindri rotanti il testo veniva codificato in base ad una determinata disposizione e quindi decodificato con la stessa macchina sulla base di dizionari.

11.2.3.2. L'impiego del computer nella crittologia

L'invenzione del computer ha rappresentato un evento pionieristico per la crittografia, poiché la sua efficienza consente l'impiego di sistemi sempre più complessi. Sebbene i principi fondamentali della cifratura non siano cambiati, sono subentrate alcune novità. In primo luogo è aumentato di molto il grado di complessità possibile dei sistemi di cifratura, dal momento che l'aspetto meccanico non costituiva più un limite alle possibilità di realizzazione, in secondo luogo è cresciuta drasticamente la velocità del processo di cifratura.

L'informazione viene rielaborata a livello digitale dai computer con numeri binari. Ciò significa che l'informazione viene trasformata nella sequenza di due segnali, ovvero 0 e 1. 1 corrisponde nel linguaggio fisico ad una tensione elettrica ovvero ad una magnetizzazione ("luce accesa"), 0 alla soppressione della tensione o della magnetizzazione ("luce spenta"). In questo modo è stato creato il codice ASCII[165] che rappresenta ogni lettera con una combinazione a sette posizioni di 0 e 1[166]. Un testo assume quindi la forma di una serie di 0 e 1, invece delle lettere vengono cifrati i numeri.

Al riguardo può essere usata sia la forma della trasposizione (metodo della traslazione), sia quella della sostituzione (metodo della sostituzione). La sostituzione può avvenire per esempio sommando una chiave nella forma di una sequenza qualsiasi di cifre. Secondo le regole della matematica binaria, sommando due numeri uguali si ottiene 0 (quindi 0+0=0 e 1+1=0), mentre sommando due numeri diversi si ottiene 1 (0+1=1). La nuova serie cifrata che risulta dall'addizione è quindi una successione binaria che può essere rielaborata con un sistema digitale o resa di nuovo leggibile sottraendo la chiave sommata.

L'utilizzo del computer ha consentito di realizzare, con l'introduzione di algoritmi di cifratura più complessi, testi in codice che non offrono praticamente nessun punto di riferimento per una crittoanalisi. Un tentativo di decrittazione è possibile soltanto provando tutte le chiavi possibili. Maggiore è la lunghezza della chiave più si estendono i tempi della procedura anche ricorrendo a computer ad alto rendimento. Vi sono quindi procedure che allo stato attuale della tecnica possono essere considerate sicure.

11.2.4. Standardizzazione e limitazione deliberata della sicurezza

Con la diffusione del computer negli anni Settanta si è resa necessaria con sempre maggior urgenza la standardizzazione dei sistemi di cifratura, perché soltanto in questo modo diventava possibile per le imprese una comunicazione sicura con i partner commerciali senza un eccessivo dispendio. I primi tentativi in tal senso sono stati effettuati negli Stati Uniti.
Una cifratura potente può essere utilizzata anche per scopi illeciti o da potenziali avversari militari; può inoltre rendere più difficile o impossibile lo spionaggio elettronico. Per questo la National Security Agency (NSA) ha ritenuto opportuno che si scegliesse uno standard di cifratura abbastanza sicuro per l'economia, che tuttavia rimanesse decifrabile con la sua specifica dotazione tecnica. A tal fine la lunghezza della chiave è stata limitata a 56 bit. Questo riduce il numero delle chiavi possibili a 100 000 000 000 000 000 blocchi[167]. Di fatto il 23 novembre

[165] American Standard Code for Information Interchange.

[166] A = 1000001, B= 1000010, C= 1000011, D= 1000100, E = 1000101, ecc.

[167] Tale cifra, rappresentata su base binaria, consiste in una successione di 56 zero e uno. Cfr. al riguardo Singh, Geheime Botschaften (1999), pag. 3.

1976 è stata introdotta ufficialmente con il nome Data Encryption Standard (DES) il cosiddetto algoritmo Lucifer di Horst Feistel nella **versione a 56 bit**, che ha rappresentato per venticinque anni lo standard ufficiale di cifratura americano[168]. Anche in Europa e in Giappone è stato introdotto questo metodo soprattutto nel settore bancario. Contro le previsioni di numerosi media, per molto tempo l'algoritmo di DES non è stato decodificato, tuttavia nel frattempo è stato elaborato un hardware sufficientemente potente da provare tutte le chiavi ("brute force attack"). Il triplo DES che ha una chiave a 112 bit, continua invece ad essere considerato sicuro. Il successore di DES, l'AES (Advanced Encryption Standard) è una procedura europea[169] progettata a Lovanio in Belgio sotto il nome di Rijndael. **È rapida e viene considerata sicura, poiché si è rinunciato a limitare la lunghezza della chiave.** Questo è da ricondurre ad una modificata politica americana in materia di crittografia (cfr. *supra* 11.1.4).

La standardizzazione ha rappresentato per le imprese una sostanziale semplificazione della cifratura. Permane tuttavia il problema della comunicazione della chiave.

11.3. Il problema della comunicazione/trasmissione sicura della chiave

11.3.1. Cifratura asimmetrica: il sistema a public key

Finché un sistema opera con una chiave sola con la quale si procede sia alla cifratura che alla decrittazione (cifratura simmetrica) è difficile che possa essere utilizzato da **molti** partner. La chiave deve essere infatti comunicata ad ogni nuovo partner prima di procedere alla trasmissione in modo da evitare che un terzo possa venirne a conoscenza. Si tratta di una procedura di difficile attuazione nella pratica per il mondo economico e possibile solo in alcuni casi per i privati.

La cifratura asimmetrica offre una soluzione a questo problema: per la cifratura e la decrittazione non viene utilizzata la stessa chiave. L'informazione viene cifrata con una chiave che può essere conosciuta da chiunque, la cosiddetta **chiave pubblica**. Il sistema opera tuttavia in una sola direzione, come un'autostrada, e quindi con la chiave pubblica non è più possibile tornare al testo in chiaro. Pertanto chiunque voglia mantenere riservata un'informazione può inviare al proprio interlocutore la chiave pubblica per la cifratura dell'informazione anche attraverso una via poco sicura. Per la decrittazione del messaggio occorre un'altra chiave, la **chiave privata**, che è mantenuta segreta e non viene inviata.[170] Il paragone più illuminante per capire tale sistema è quello con un lucchetto: chiunque è in grado di far scattare un lucchetto e chiudere quindi in modo sicuro un contenitore, tuttavia può aprirlo soltanto chi possiede la chiave giusta.[171] La chiave pubblica e quella privata sono collegate l'una all'altra; tuttavia dalla chiave pubblica non si può dedurre quella privata.

Ron Rivest, Adi Shamir e Leonard Adleman hanno inventato un sistema di cifratura asimmetrica, il cosiddetto sistema RSA, che prende il nome dalle iniziali dei loro cognomi. In

[168] Cfr. al riguardo Singh, Geheime Botschaften (1999), pag. 302 e segg.

[169] È stato ideato da due crittografi belgi all'Università Cattolica di Lovanio, Joan Daemen e Vincent Rijmen.

[170] L'idea della cifratura asimmetrica nella forma di sistema a public key è stata di Whitfield Diffie e Martin Hellmann.

[171] Singh, Geheime Botschaften (1999), pag. 327.

una funzione unidirezionale (una cosiddetta funzione one-way) si inserisce come parte della chiave pubblica il risultato della moltiplicazione di due grandi numeri primi. In questo modo il testo in chiaro viene cifrato. La decrittazione è possibile soltanto per chi conosce il valore di entrambi i numeri primi utilizzati. Non esiste tuttavia alcuna operazione matematica che consenta a partire dalla moltiplicazione di due numeri primi di calcolare dal risultato quali sono i numeri di partenza. Finora è possibile soltanto procedere per tentativi sistematici. Pertanto allo stato attuale della scienza il sistema è sicuro, se vengono scelti numeri primi abbastanza elevati. L'unico rischio consiste nella possibilità che un giorno un brillante matematico scopra un'operazione più rapida per la scomposizione dei fattori. Per il momento, nonostante numerosi tentativi, nessuno vi è ancora riuscito.[172] Si è più volte sostenuto addirittura che il problema sia irrisolvibile, tuttavia fino ad oggi non si è raggiunta alcuna indicazione esatta in merito.[173]

In confronto al sistema simmetrico (ad esempio DES), la cifratura a public key richiede sul PC un tempo di calcolo molto più lungo o l'impiego di sistemi rapidi.

11.3.2. La cifratura a public key per i privati

Per rendere accessibile in generale il sistema a public key Phil Zimmerman ha ideato un sistema che collega la dispendiosa procedura di calcolo della cifratura a public key con un sistema simmetrico più rapido. L'informazione stessa deve essere cifrata con un sistema simmetrico, il sistema IDEA elaborato a Zurigo, mentre la chiave per la cifratura simmetrica viene comunicata allo stesso tempo con il sistema a public key. Zimmerman ha inventato un programma di facile uso, chiamato Pretty Good Privacy, che ad un comando da tastiera (o da mouse) crea la chiave necessaria e avvia la cifratura. Il programma è stato messo in Internet, dove chiunque poteva scaricarlo. Il PGP è stato successivamente acquistato dall'impresa americana NAI, ma continua ad essere messo gratuitamente a disposizione dei privati.[174] Della versione precedente è stato pubblicato il testo sorgente in modo da dimostrare che vi è alcun sotterfugio. I testi sorgente della versione più recente PGP 7, che erano corredati di una veste grafica espressamente creata per agevolare gli utenti, purtroppo non sono più stati pubblicati.
Esiste tuttavia anche un'altra realizzazione dello standard OpenPGP, lo GnuPG. Lo GnuPG offre gli stessi metodi di cifratura del PGP con il quale è inoltre compatibile. Si tratta tuttavia di software liberi, il cui codice sorgente è conosciuto e che chiunque può utilizzare e trasmettere. Il ministero tedesco dell'Economia e la tecnologia ha promosso il portale dello GnuPG su Windows e l'elaborazione di una veste grafica, ma purtroppo al momento il progetto non è ancora stato completato. Secondo le informazioni del relatore i lavori procedono.

Esistono inoltre standard concorrenti di OpenPGP, quali l'S/MIME, che è supportato da molti programmi di posta elettronica. Il relatore non dispone tuttavia di informazioni sulla realizzazione libera.

[172] Cfr. al riguardo Buchmann, Faktorisierung großer Zahlen, Spektrum der Wissenschft 2 1999, pag. 6 e segg.

[173] Cfr. al riguardo Singh, Geheime Botschaften (1999), pag. 335 e segg.

[174] Informazioni sul software si trovano all'indirizzo www.pgpi.com.

11.3.3. Procedure future

Soluzioni del tutto nuove per la trasmissione sicura della chiave potrebbero emergere in futuro dalla crittografia quantistica. Essa consente di individuare un'eventuale intercettazione durante la trasmissione di una chiave. Se si inviano fotoni polarizzati, non è possibile individuarne la polarizzazione senza modificare i fotoni stessi. In questo modo eventuali interferenze sulla linea potrebbero essere individuate con certezza. Verrebbe quindi utilizzata soltanto una chiave non intercettata. Nelle prove finora condotte è già riuscita una trasmissione su una distanza di oltre 48 km con cavo in fibra di vetro e di oltre 500 km per via aerea.[175]

11.4. Sicurezza dei prodotti di cifratura

Nel contesto del dibattito incentrato sull'effettiva sicurezza dei sistemi di cifratura i prodotti americani e le scappatoie che li caratterizzano sono di nuovo stati messi sotto accusa. La stampa ha dedicato caratteri cubitali, ad esempio, al caso di Excel, nella cui versione per l'Europa spesso non risulta, stando a quanto si afferma, la metà del codice del record di intestazione del file. Microsoft si è anche irritata per l'attenzione che la stampa ha riservato alla notizia secondo cui un hacker avrebbe scoperto una "chiave NSA" nascosta nel programma, fatto, questo, che la società americana ha seccamente smentito. Dal momento che Microsoft non ha comunicato il suo codice sorgente, qualsiasi opinione in merito è oggetto di speculazione. Nondimento per le versioni precedenti di PGP e GnuPG la possibilità di ricorrere a una simile scappatoia si può escludere con certezza, in quanto il corrispondente testo sorgente è stato reso noto.

11.5. Cifratura in conflitto con gli interessi dello Stato

11.5.1. I tentativi di imporre limitazioni alla cifratura

In alcuni Stati è innanzitutto vietato utilizzare software di cifratura o apparecchiatura per la crittografia e le eventuali eccezioni sono subordinate ad un'autorizzazione. Questa situazione non è propria solo di dittature quali la Cina, l'Iran o l'Irak, ma anche di paesi democratici in cui l'uso o la vendita di programmi o apparecchiature per la cifratura è stata limitata in forza di leggi in materia. Le comunicazioni dovebbero pertanto essere protette contro l'accesso da parte di persone non autorizzate, lasciando tuttavia impregiudicata la possibilità per lo Stato di effettuare intercettazioni legali come in precedenza. La perdita di superiorità sul versante tecnico da parte delle autorità dovrebbe essere bilanciata con divieti legali. Ad esempio, fino a poco tempo fa la Francia ha vietato l'utilizzo della crittografia in generale e l'ha condizionato alla concessione di una singola autorizzazione. Alcuni anni fa anche in Germania è stato sollevato un dibattito sulle limitazioni alla cifratura e sulla necessità di depositare i codici. In passato gli Stati Uniti hanno invece limitato la lunghezza dei codici.

11.5.2. L'importanza di una cifratura sicura per il commercio elettronico

Nel frattempo questi tentativi dovrebbero essere definitivamente naufragati. L'interesse dello Stato a poter accedere alla decrittazione e di conseguenza ai testi in chiaro non si contrappone cioè solo al diritto alla tutela dei singoli, ma anche a interessi economici consolidati. Infatti il commercio elettronico e l'electronic banking (automazione dei servizi bancari) dipendono da una comunicazione sicura via Internet. Se non è possibile garantire tale aspetto, queste tecniche sono

[175] In merito alla crittografia quantistica cfr. Wobst, Abenteuer Kryptographie[2] (1998), pag. 234 e segg.

condannate al fallimento, perché verrebbe a mancare la fiducia dei clienti. È un siffatto contesto che spiega l'inversione di tendenza assunta da statunitensi o americani sul versante della politica di materia di crittografia.

A questo punto è emerso che il commercio elettronico necessita di procedure di cifratura sicure per un duplice motivo: non solo per cifrare le informazioni, ma anche per poter comprovare in modo inequivocabile l'identità dei partner commerciali. Per la firma elettronica si può infatti ricorrere ad un uso inverso della chiave pubblica: la chiave privata viene utilizzata per la cifratura, quella pubblica per la decodifica. Questa forma di cifratura conferma l'origine della firma. Chiunque utilizzando la chiave pubblica di una persona può accertarsi della sua autenticità, ma non può contraffarne la firma. Nel PGP è stata inserita anche questa funzione di facile impiego.

11.5.3. I problemi di chi viaggia per lavoro

In alcuni Stati a coloro che viaggiano per lavoro non è consentito utilizzare programmi di cifratura sui propri portatili. Questo impedisce di proteggere in qualche modo le comunicazioni con la propria impresa o di tutelare i dati inseriti contro l'accesso indebito.

11.6. Domande di carattere pratico sulla cifratura

Volendo rispondere alla domanda che riguarda per chi e in quali casi sia opportuno ricorrere alla cifratura, sembra giusto operare una distinzione tra privati e imprese.
Spesso si sostiene che per i privati la codificazione di fax e conversazioni telefoniche tramite telefoni predisposti per la crittografia o fax dotati di sistemi di cifratura non è una soluzione attuabile nella pratica, non solo in quanto i costi da sostenere per la realizzazione di tali apparecchiature sono relativamente elevati, ma anche perché la loro applicabilità presuppone che l'interlocutore disponga a propria volta di apparecchi di questo genere, condizione, questa, che si presenta solo in rarissimi casi.

Per contro, chiunque può e deve crittare i messaggi di posta elettronica. All'affermazione spesso avanzata secondo cui non si hanno segreti e quindi non c'è alcuna necessità di ricorrere alla cifratura, si deve controbattere che non è usuale inviare le comunicazioni scritte su cartolina, e che si deve considerare che un messaggio di posta elettronica non è niente altro che una lettera senza busta. La cifratura di messaggi di posta elettronica è sicura e non presenta quasi nessuna difficoltà, in Internet i privati possono già reperire sistemi di facile uso e gratuiti, quali PGP e GnuPGP. Purtroppo manca ancora la necessaria diffusione. Sarebbe auspicale che il potere pubblico desse il buon esempio e si impegnasse in un processo di standardizzazione della cifratura onde demistificarla.

Per quanto attiene alle imprese, si dovrebbe vigilare con particolare rigore che la trasmissione di informazioni sensibili avvenga solo su percorsi sicuri di comunicazione. Sembra ovvio che sia un principio che ben si applica alle grandi imprese, ma è proprio nelle piccole e medie imprese che spesso le informazioni di carattere interno vengono trasmesse per posta elettronica senza essere crittate, perché manca un'adeguata sensibilizzazione nei confronti del problema. In questo caso si deve sperare che le associazioni industriali e le camere di commercio si impegnino più a fondo per fornire spiegazioni in merito. Naturalmente la crittazione di messaggi di posta elettronica è solo una delle tante sfaccettatura della sicurezza, e soprattutto risulta inutile se all'informazione hanno avuto accesso altri ancora prima che questa venisse cifrata. Questo

significa che si deve rendere sicuro l'intero ambiente di lavoro, che si deve garantire la sicurezza dei locali utilizzati e controllare l'accesso fisico a uffici e computer. Si deve tuttavia anche impedire l'accesso non autorizzato alle informazioni tramite rete utilizzando le adeguate protezioni. Il collegamento tra la rete interna e Internet presenta particolari rischi. Se si considera la sicurezza con la dovuta serietà si devono altresì usare solo sistemi operativi il cui codice sorgente è noto e verificato, poiché solo la sicurezza consente di determinare cosa avviene con i dati. Il settore della sicurezza offre altresì una gamma di attività alle imprese. Sul mercato sono presenti già numerose aziende che prestano servizi di consulenza e riconversione nel campo della sicurezza a prezzi accessibili e la cui offerta registra una crescita costante per effetto della domanda. Inoltre c'è da augurarsi che le organizzazioni industriali e le camere di commercio si occupino di questi aspetti soprattutto per richiamare l'attenzione delle piccole imprese sulla questione della sicurezza e per sostenere il progetto e l'attuazione di un concetto di protezione di ampia portata.

12. Le relazioni esterne dell'Unione europea e la raccolta di informazioni

12.1. Introduzione

Con l'adozione del Trattato di Maastricht nel 1991 è stata definita la politica estera e di sicurezza comune (PESC) nella sua forma più elementare, quale nuovo strumento strategico per l'Unione europea. Sei anni dopo, il Trattato di Amsterdam ha ulteriormente strutturato la PESC e ha creato la possibilità di iniziative di difesa comuni nell'ambito dell'Unione europea, pur preservando le alleanze esistenti. Sulla base del Trattato di Amsterdam e alla luce dell'esperienza maturata nel Kosovo, nel dicembre 1999 il Consiglio europeo di Helsinki ha lanciato l'iniziativa europea in materia di sicurezza e di difesa. L'iniziativa mira a creare una forza multinazionale costituita da circa 50.000-60.000 effettivi entro la seconda metà del 2003. L'esistenza di tale forza multinazionale renderà inevitabile lo sviluppo di una capacità di intelligence autonoma. La semplice integrazione dell'attuale capacità di intelligence dell'UEO non sarà sufficiente a realizzare tale obiettivo. È inevitabile prevedere una maggiore cooperazione tra le agenzie di intelligence degli Stati membri, che vada ben oltre le forme di cooperazione attuali.

Nondimeno, l'ulteriore sviluppo della PESC non è l'unico elemento a comportare una maggiore cooperazione dei servizi di informazione dell'Unione. Anche la maggiore integrazione economica nell'ambito dell'Unione europea renderà necessario intensificare la cooperazione nel campo della raccolta di informazioni. Una politica europea comune richiede una percezione comune della realtà economica nel mondo esterno all'Unione europea. Una posizione comune nei negoziati commerciali in seno all'OMC o con i paesi terzi comporta la tutela comune della posizione negoziale. Forti industrie europee hanno bisogno di una protezione comune contro lo spionaggio economico dall'esterno dell'Unione europea.

Si deve infine sottolineare che l'ulteriore sviluppo del secondo pilastro dell'Unione e delle attività dell'Unione nel settore degli affari interni e della giustizia deve anche portare ad una maggiore cooperazione tra i servizi di informazione. In particolare, la lotta comune contro il terrorismo, il commercio illegale di armi, il traffico di esseri umani e il riciclaggio di denaro non si può attuare senza una stretta cooperazione tra i servizi di informazione.

12.2. Possibilità di cooperazione nell'ambito dell'Unione europea

12.2.1 Cooperazione attuale

Sebbene tradizionalmente i servizi di informazione si fidino solo delle informazioni raccolte da essi stessi e forse sussista persino una certa diffidenza tra i diversi servizi di informazione all'interno dell'Unione europea, la cooperazione tra i servizi sta già registrando una progressiva intensificazione. Vi sono frequenti contatti in seno alla NATO, all'UEO e nell'ambito dell'Unione europea. Inoltre, mentre i servizi di informazione in seno alla NATO dipendono ancora in larga misura dai contributi di gran lunga più sofisticati degli Stati Uniti, la creazione del centro satellitare dell'UEO a Torrejon (Spagna) e l'istituzione di un ufficio di intelligence presso la sede dell'UEO hanno contribuito ad un'azione europea più autonoma in questo campo.

12.2.2. Vantaggi di una politica europea comune in materia di intelligence

A parte gli sviluppi che si stanno già verificando, è bene rilevare che una politica comune europea in materia di intelligence di fatto presenta vantaggi oggettivi. Tali vantaggi si possono descrivere come segue.

12.2.2.1. Vantaggi professionali

Innanzitutto il materiale riservato e non riservato da raccogliere, analizzare e valutare da parte di una sola agenzia o nell'ambito di accordi bilaterali in seno all'Europa occidentale è semplicemente troppo. Le richieste di servizi di informazione variano dalle informazioni in materia di difesa, alle informazioni riguardanti le politiche economiche interne ed internazionali dei paesi terzi, alle informazioni a sostegno della lotta contro il crimine organizzato e il traffico di droga. Anche se la cooperazione esistesse solo al livello più elementare, cioè per quanto riguarda la raccolta di open-source intelligence (OSINT), tale cooperazione darebbe già risultati di grande importanza per le politiche dell'Unione europea.

12.2.2.2. Vantaggi in termini di bilancio

Nel passato recente le dotazioni di bilancio per la raccolta di informazioni sono state ridotte e, in alcuni casi, continuano a subire tagli. Nel contempo, le richieste di informazioni e quindi di intelligence sono aumentate. I bilanci ridotti non solo rendono possibile tale cooperazione ma, nel lungo termine, essa risulterà anche redditizia. In particolare, nel caso di istituzione e mantenimento di infrastrutture tecniche, le operazioni comuni risultano interessanti in presenza di una scarsità di fondi, ma anche nell'ambito della valutazione delle informazioni raccolte. Una maggiore cooperazione rafforzerà l'efficacia della raccolta di informazioni.

12.2.2.3. Vantaggi politici

In linea di principio, le informazioni raccolte sono usate per consentire ai governi di adottare decisioni migliori su basi migliori. L'ulteriore integrazione politica ed economica a livello di Unione europea significa che le informazioni devono essere disponibili a livello europeo e deve inoltre basarsi su più di una fonte.

12.2.3. Osservazioni conclusive

Questi vantaggi oggettivi illustrano solo la crescente importanza della cooperazione nell'ambito dell'Unione europea. In passato, gli Stati-nazioni erano abituati a garantire la sicurezza esterna, l'ordine interno, la prosperità nazionale e l'identità culturale ciascuno per proprio conto. Oggigiorno, l'Unione europea sta assumendo in molti campi un ruolo almeno complementare a quello dello Stato-nazione. È impossibile che i servizi di informazione rimangano l'ultimo e unico campo non influenzato dal processo di integrazione europea.

12.3. Cooperazione oltre il livello dell'Unione europea

In seguito alla seconda guerra mondiale la cooperazione nel campo della raccolta di informazioni inizialmente non avveniva a livello europeo, ma molto più a livello transatlantico. Si è già rilevato in precedenza che sono stati instaurati stretti rapporti nel campo della raccolta di informazioni tra il Regno Unito e gli Stati Uniti. Tuttavia, anche nel campo dell'intelligence in materia di difesa in seno alla NATO e non solo, gli Stati Uniti erano e continuano ad essere il partner assolutamente dominante. La questione principale è quindi: l'intensificazione della cooperazione europea nel campo della raccolta di informazioni perturberà seriamente i rapporti

con gli Stati Uniti o può invece portare a un rafforzamento di tali rapporti? In che modo si svilupperanno le relazioni UE-USA sotto la nuova amministrazione Bush? In particolare, in che modo sarà mantenuto il rapporto speciale tra Stati Uniti e Regno Unito in questo contesto?
Alcuni sono del parere che non sussista necessariamente una contraddizione tra i rapporti speciali UK-USA e l'ulteriore sviluppo della PESC. Altri ritengono che proprio il settore della raccolta di informazioni possa essere la questione per cui il Regno Unito si vedrà obbligato a decidere se il suo destino sia europeo o transatlantico. I profondi legami tra Regno Unito e Stati Uniti (e gli altri partner dell'accordo UK-USA) possono ostacolare la condivisione dell'intelligence tra gli altri Stati dell'Unione europea, in quanto il governo britannico potrebbe essere meno interessato alla condivisione intraeuropea ed i partner nell'Unione europea potrebbero fidarsi meno del Regno Unito. Del pari, se gli Stati Uniti ritengono che il Regno Unito abbia sviluppato contatti speciali con i suoi partner dell'Unione, e che ciò rientri in uno speciale accordo europeo, essi potrebbero dimostrarsi restii a continuare a condividere la propria intelligence con il Regno Unito. Promuovere la cooperazione europea nel campo dell'intelligence può quindi costituire un test importante per le ambizioni europee del Regno Unito e per la capacità d'integrazione dell'Unione europea.

Nelle circostanze attuali, tuttavia, è ben poco probabile che persino progressi estremamente rapidi nella cooperazione tra i partner europei possano, nel breve e persino nel lungo periodo, accorciare le distanze con gli Stati Uniti in termini di vantaggio tecnologico. L'Unione europea non sarà in grado di creare una rete sofisticata di satelliti SIGINT, satelliti per l'acquisizione di immagini e stazioni di terra. L'Unione europea non sarà in grado di sviluppare, nel breve periodo, la rete informatica altamente sofisticata indispensabile per la selezione e la valutazione del materiale raccolto. L'Unione europea non sarà disposta a rendere disponibili le risorse di bilancio necessarie per costituire un'alternativa reale alle attività di intelligence degli Stati Uniti. Pertanto, già dal punto di vista tecnologico e di bilancio sarà nell'interesse dell'Unione europea mantenere stretti rapporti con gli Stati Uniti nel campo della raccolta di informazioni. Nondimeno, anche sotto il profilo politico sarà importante mantenere e, se necessario, rafforzare le relazioni con gli Stati Uniti, in particolare per quanto riguarda la lotta comune contro il crimine organizzato, il terrorismo, il traffico di armi e droga e il riciclaggio di denaro. Operazioni comuni di intelligence sono indispensabili per sostenere una lotta comune. Le iniziative comuni di mantenimento della pace, come nell'ex Yugoslavia, richiedono un maggiore contributo europeo in tutti i settori di intervento.

D'altro canto, una maggiore consapevolezza europea dev'essere accompagnata da una maggiore responsabilità europea. L'Unione europea dovrebbe diventare un partner a livello più paritario, non solo in ambito economico, ma anche nel settore della difesa e quindi nel campo della raccolta di informazioni. Una capacità europea di intelligence più autonoma non va quindi considerata come un elemento destinato ad indebolire le relazioni transatlantiche, ma andrebbe usata come strumento di rafforzamento, facendo sì che l'Unione europea sia riconosciuta come partner più paritario e dotato di maggiore capacità. Nel contempo, l'Unione europea deve compiere sforzi autonomi per proteggere la sua economia e la sua industria contro minacce illegali e indesiderate, quali lo spionaggio economico, il cybercrimine e gli attacchi terroristici. È inoltre necessaria un'intesa transatlantica nel campo dello spionaggio industriale. L'Unione europea e gli Stati Uniti dovrebbero definire un insieme di norme su ciò che è consentito e ciò che non è consentito in detto campo. Per rafforzare la cooperazione transatlantica in questo ambito, si potrebbe lanciare un'iniziativa comune a livello di OMC, al fine di usare i meccanismi di questa organizzazione per salvaguardare un equo sviluppo economico a livello mondiale.

12.4. Osservazioni finali

Fermo restando il principio fondamentale della tutela della vita privata dei cittadini europei, un ulteriore sviluppo di una capacità comune di intelligence a livello di Unione europea dev'essere considerato necessario e inevitabile. La cooperazione con i paesi terzi, in particolare con gli Stati Uniti, dev'essere salvaguardata e, con ogni possibilità, rafforzata. Ciò non significa necessariamente che le attività SIGINT europee debbano essere automaticamente integrate in un sistema ECHELON autonomo dell'Unione europea o che l'Unione europea debba diventare un partner a pieno titolo dell'attuale accordo UK-USA. Tuttavia, la promozione di un'adeguata responsabilità europea nel campo della raccolta di informazioni dev'essere valutata con efficacia. Una capacità di intelligence europea integrata comporta, al tempo stesso, un sistema di controllo politico europeo sulle attività delle agenzie competenti. Si dovranno adottare decisioni sugli strumenti per la valutazione dell'intelligence e per l'assunzione delle decisioni politiche, sulla base di un'analisi dei rapporti di intelligence. L'assenza di un sistema di controllo politico, e quindi di consapevolezza e responsabilità politica per il processo di raccolta di informazioni, sarebbe pregiudizievole per il processo di integrazione europea.

13. Conclusioni e raccomandazioni

13.1. Premessa

Il presente capitolo fornisce informazioni e riporta conclusioni possibili. Non lo si deve considerare definitivo, anzi il relatore gradirebbe che fosse assunto come base per il dibattito politico da condurre adesso in seno alla commissione. Il testo dovrà essere ancora oggetto di modifiche, in modo da poter inserire gli elementi emersi in occasione di questo confronto.

13.2. Conclusioni

Sull'esistenza di un sistema di intercettazione globale per comunicazioni private ed economiche (sistema di intercettazione ECHELON)

Non si può nutrire più alcun dubbio in merito all'esistenza di un sistema di intercettazione delle comunicazioni a livello mondiale, cui cooperano in proporzione gli Stati Uniti, il Regno Unito, il Canada, l'Australia e la Nuova Zelanda nel quadro del Patto UKUSA. Il fatto che sulla base degli attuali indizi sembri verosimile che il suo nome in codice sia effettivamente "ECHELON" è un aspetto che comunque rivesta un'importanza secondaria.

Dall'analisi condotta è emerso che questo sistema non può di certo essere così potente come sostenuto da una parte dei media.

Sui limiti del sistema di intercettazione

Il sistema di sorveglianza si basa sull'intercettazione globale delle comunicazioni via satellite, tuttavia nelle aree ad elevata densità di comunicazioni solo un volume estremamente ridotto di queste viene trasmesso tramite satellite. Questo significa che la maggior parte di esse non può essere intercettata dalle stazioni di terra, bensì solo inserendosi nei cavi o captando le trasmissioni via radio. Dalle ricerche è tuttavia emerso che gli Stati ECHELON hanno accesso solo ad una parte molto esigua delle comunicazioni via cavo e via radio e a causa del personale necessario sono in grado di analizzare solo una percentuale ridotta delle comunicazioni.

Sulla possibile esistenza di altri sistemi di intercettazione

Poiché l'intercettazione di comunicazioni costituisce un usuale strumento di spionaggio impiegato nell'ambito dei servizi di informazione, anche altri Stati potrebbero gestire un simile sistema, nella misura in cui dispongano delle corrispondenti risorse finanziarie e delle circostanze geografiche adeguate. La Francia sarebbe - o perlomeno era per quanto riguarda le circostanze geografiche - l'unico Stato membro dell'Unione europea in grado di istituire da solo un sistema di intercettazione globale, in considerazione dei suoi territori d'oltremare. Inoltre vi sono elementi che consentono di supporre che anche la Russia potrebbe gestire un sistema di questo genere.

Sulla compatibilità con il diritto dell'Unione europea

La questione attinente alla compatibilità di un sistema del tipo ECHELON con il diritto dell'Unione europea richiede di operare una distinzione: se il sistema viene impiegato solo nell'ambito dei servizi di informazione, non si pone alcun elemento di contrasto con la normativa europea, in quanto le attività di sicurezza degli Stati non sono contemplate dal trattato CE, ma rientrerebbero nel titolo V del trattato sull'Unione europea (PESC), benché al momento non sia prevista ancora alcuna regolamentazione pertinente e quindi manchino punti di contatto. Per converso, se l'impiego del sistema è abusivo, quest'ultimo è in contrasto con l'obbligo di lealtà

degli Stati membri e con il concetto di un mercato comune caratterizzato dalla libera concorrenza, e quindi uno Stato membro che vi partecipi agisce in violazione del diritto dell'Unione europea.

Sulla compatibilità con il diritto fondamentale alla vita privata (articolo 8 della CEDU)

Tutte le intercettazioni di comunicazioni rappresentano una profonda ingerenza nella vita privata del singolo. L'articolo 8 della CEDU tutela la vita privata e ammette queste interferenze solo se sono necessarie per salvaguardare la sicurezza nazionale, nella misura in cui le disposizioni in materia siano previste dalla legge nazionale e accessibili in generale, e stabiliscano in quali circostanze e a quali condizioni l'autorità pubblica può ricorrervi. Inoltre le ingerenze nella vita privata devono essere proporzionate rispetto all'interesse da tutelare, e quindi conformemente a quanto sancito dalla CEDU non è sufficiente che siano meramente utili o auspicabili.

Un sistema del servizio di informazione che captasse qualsiasi comunicazione senza garantire il rispetto del principio di proporzionalità non sarebbe compatibile con la CEDU. Parimenti si sarebbe in presenza di una violazione della CEDU nel caso in cui la normativa che disciplina la sorveglianza delle comunicazioni non preveda alcuna base giuridica, non sia accessibile in generale o sia formulata in maniera tale da non poter ipotizzare quali siano le eventuale conseguenze per i singoli. Poiché le norme che disciplinano l'attività dei servizi di informazione americani all'estero sono in gran parte riservate, vi è ragione almeno di dubitare che il principio di proporzionalità venga rispettato e di sostenere che si è in presenza di una violazione dei principi di accessibilità del diritto e di prevedibilità del suo rispetto sanciti dalla CEDU.

Sebbene gli Stati Uniti non siano una parte contraente della CEDU, gli Stati membri si devono comportare in conformità della CEDU. Essi non si possono sottrarre agli obblighi che incombono loro in virtù della CEDU, in quanto consentono di operare sul loro territorio ai servizi di informazione di altri Stati che prevedono normative meno rigide, poiché altrimenti il principio di legalità verrebbe privato delle sue due componenti, l'accessibilità e la prevedibilità del suo rispetto, e quanto sancito dalla CEDU svuotato di contenuto.

La compatibilità con i diritti fondamentali dell'attività dei servizi di informazione legittimata in virtù di una legislazione in materia richiede la presenza di sistemi di controllo adeguati, in modo da controbilanciare il pericolo insito nell'azione segreta di una parte dell'apparato amministrativo. Considerato che la Corte europea dei diritti dell'uomo ha sottolineato espressamente la necessità di avvalersi di un sistema di controllo efficiente nell'ambito dell'attività dei servizi di informazione, desta preoccupazioni il fatto che alcuni Stati membri non dispongano di alcun proprio organo parlamentare di controllo che si occupi dei servizi segreti.

Sulla questione se i cittadini dell'Unione europea sono tutelati in modo adeguato nei confronti dei servizi di informazione

La tutela dei cittadini dell'Unione europea dipende dalla situazione giuridica propria dei singoli Stati membri, i quali sono tuttavia strutturati in modo diverso, e a volte non dispongono di alcun organo parlamentare di controllo, tanto da rendere quasi impossibile sostenere che sia garantita una tutela sufficiente. I cittadini europei hanno un interesse fondamentale a che i rispettivi parlamenti nazionali siano dotati di una commissione di controllo speciale strutturata formalmente, che sorvegli e controlli le attività dei servizi di informazione. Tuttavia persino laddove un organo di controllo è presente questo è più interessato ad occuparsi dell'attività dei servizi di informazione nazionali che non di quelli esteri, in quanto normalmente i cittadini del proprio Stato rientrano solo nel primo caso.

Qualora i servizi di informazione cooperino nel quadro della PESC si chiede alle istituzioni di creare condizioni di protezione sufficienti a favore dei cittadini europei.

Sullo spionaggio economico

Rientra nell'attività dei servizi di informazione esteri occuparsi di dati economici, quali sviluppi settoriali, andamento dei mercati delle materie prime, rispetto di embarghi economici, rispetto delle regole di fornitura di beni a duplice uso, e così via. Questi elementi spiegano il motivo per cui spesso le imprese pertinenti vengano sorvegliate. Non è in alcun caso tollerabile che i servizi di informazione, nello svolgimento di indagini su imprese estere, vengano sfruttati per lo spionaggio economico al fine di avvantaggiare la concorrenza sul territorio nazionale. Tuttavia non vi è alcun elemento a sostegno del fatto che il sistema d'intercettazione globale sia stato creato a tale scopo, benché sia stato affermato più volte.

Spesso i dati aziendali sensibili si trovano all'interno delle stesse imprese, e pertanto lo spionaggio della concorrenza si traduce principalmente nel tentativo di ottenere informazioni dai dipendenti o tramite soggetti introdotti clandestinamente oppure cercando di inserirsi nelle reti informatiche interne. Solo nel caso in cui i dati sensibili vengano trasmessi all'esterno via cavo o via radio (satellite) si può impiegare un sistema di sorveglianza delle comunicazioni a fini di spionaggio della concorrenza e che tale situazione si verifica in modo sistematico solo nei seguenti tre casi:

- imprese che operano in tre aree geografiche con fuso orario diverso, i cui risultati intermedi vengono inviati dall'Europa verso l'America e quindi trasmessi in Asia;
- videoconferenze di gruppi multinazionali trasmesse tramite sistemi V-sat o via cavo;
- ordini importanti le cui trattative si svolgono in loco (ad esempio costruzione di impianti, installazione di infrastrutture delle telecomunicazioni, costruzione di nuovi sistemi di trasporto e così via) e da lì devono essere definiti con la sede centrale.

Sulle possibilità di autotutelarsi

La sicurezza delle imprese si può conseguire solo rendendo sicuro l'intero ambiente di lavoro e proteggendo tutte le vie di comunicazione attraverso le quali vengono trasmesse le informazioni sensibili. Il mercato europeo offre sistemi di cifratura sufficientemente sicuri e a prezzi convenienti. Anche i privati devono ricorrere con urgenza alla crittazione dei messaggi di posta elettronica, poiché un messaggio non crittato è alla stregua di una lettera senza busta. In Internet sono disponibili gratuitamente per gli utenti privati sistemi di uso relativamente facile.

Sulla cooperazione dei servizi di informazione nell'ambito dell'Unione europea

L'Unione europea ha comunicato la propria intenzione di coordinare la raccolta di informazione da parte dei servizi di informazione nel quadro di una propria politica di sicurezza e di difesa, senza tuttavia interrompere la cooperazione in questi settori con altri partner. Una cooperazione dei servizi di informazione nell'ambito dell'Unione europea sarebbe anche auspicabile, poiché, da un lato, una politica di sicurezza comune che escluda la partecipazione dei servizi segreti non sarebbe sensata, e, dall'altro, vi sarebbero collegati non pochi vantaggi sotto il profilo professionale, finanziario e politico. Essa corrisponderebbe più adeguatamente al concetto di un partner che si pone di fronte agli USA su un piano di parità e potrebbe riunire tutti gli Stati membri in un sistema pienamente compatibile con quanto sancito dalla CEDU. Ovviamente il controllo di tale cooperazione deve essere affidato al Parlamento europeo. Il Parlamento europeo ha in programma di elaborare propri regolamenti in merito all'accesso a informazioni e documenti confidenziali e sensibili.

13.3. Raccomandazioni

Sulla conclusione e modifica di accordi internazionali sulla tutela dei cittadini e delle imprese

1. Si invita il Segretario generale del Consiglio d'Europa a chiedere al comitato dei ministri di valutare se sia opportuno adeguare la tutela della vita privata garantita ai sensi dell'articolo 8 della CEDU ai moderni metodi di comunicazione e alle possibilità di intercettazione

inserendola in un protocollo addizionale o considerandola insieme alla normativa sulla tutela dei dati nel quadro di una revisione della convenzione sulla tutela dei dati, a condizione di non ridurre il livello di protezione giuridica conseguito attraverso il tribunale né di diminuire il grado di flessibilità necessaria per gli adeguamenti agli sviluppi futuri;

2. si esortano gli Stati membri a istituire una piattaforma europea allo scopo di esaminare le disposizioni di legge per quanto riguarda il rispetto del segreto epistolare e delle comunicazioni, e ad accordarsi su un testo comune, che garantisca a tutti i cittadini europei la tutela della vita privata sull'intero territorio degli Stati membri in conformità di quanto stabilito all'articolo 7 della Carta dei diritti fondamentali dell'Unione europea, e che garantisca altresì che l'attività dei servizi di informazione sia compatibile con i diritti fondamentali, nonché esercitata in base alle condizioni di cui all'articolo 8 della CEDU, indicate al capitolo 8 della relazione, in particolare al punto 8.3.4;

3. si invitano gli Stati membri ad approvare un protocollo addizionale che consenta alle Comunità europee di aderire alla CEDU, oppure a riflettere su altre eventuali misure intese ad ovviare ai conflitti giurisprudenziali tra la Corte di Strasburgo e la Corte di Lussemburgo;

4. si invita il Segretario generale dell'ONU ad incaricare la commissione responsabile di presentare proposte intese ad adeguare alle innovazioni tecniche l'articolo 17 del Patto internazionale sui diritti civili e politici che garantisce la tutela della vita privata;

5. si esortano gli Stati Uniti a firmare il protocollo addizionale al Patto internazionale sui diritti civili e politici, affinché, in caso di sua violazione, sia possibile presentare ricorsi individuali contro gli Stati Uniti dinanzi alla tradizionale commissione per i diritti umani; si sollecitano le ONG americane di pertinenza, in particolare l'ACLU (American Civil Liberties Union) e l'EPIC (Electronic Privacy Information Center) ad esercitare la dovuta pressione sul governo americano;

Sulle misure legislative nazionali intese a tutelare cittadini e imprese

6. si invitano gli Stati membri a verificare che la legislazione nazionale in materia di attività dei servizi di informazione sia compatibile con i diritti fondamentali;

7. si sollecitano gli Stati membri ad adoperarsi per conseguire l'obiettivo, riguardo all'attività dei servizi di informazione, di una tutela comune il cui livello corrisponda al più elevato tra quelli garantiti dagli Stati dell'Unione europea, poiché i soggetti interessati dall'attività di un servizio di informazione estero sono di solito i cittadini di paesi terzi e pertanto anche di altri Stati membri;

8. si invitano le istituzioni dell'Unione europea a creare condizioni di protezione sufficienti a favore dei cittadini europei nel caso in cui i servizi di informazione cooperino nel quadro della PESC. Il Parlamento europeo in qualità di logico organo di controllo deve, dal canto proprio, predisporre le circostanze necessarie per la sorveglianza di questo settore altamente sensibile, in modo da esigere in modo realistico ma anche fondato i dovuti diritti attinenti al controllo;

Sulle misure legislative speciali volte alla lotta contro lo spionaggio industriale

9. si esortano gli Stati membri a riflettere sul modo in cui sia possibile in forza di normative del diritto europeo e di quello internazionale lottare contro lo spionaggio economico e la corruzione come mezzo per assicurarsi appalti, in particolare valutare se sia possibile elaborare una regolamentazione nel quadro dell'OMC che tenga conto delle distorsioni della concorrenza imputabili a un tale comportamento, ad esempio considerando nulli simili accordi;

10. si sollecitano gli Stati membri ad impegnarsi in una esplicita dichiarazione comune a non condurre alcuna attività di spionaggio economico gli uni nei confronti degli altri, e a dimostrare di conseguenza di essere in armonia con lo spirito e le disposizioni del trattato CE;

Sulle misure intese all'applicazione del diritto e loro controllo

11. si esortano i parlamenti nazionali che non dispongono di un proprio organo di controllo incaricato di sorvegliare i servizi d'informazione a istituirne uno;

12. si invitano gli organi di controllo nazionali dei servizi segreti ad attribuire grande peso alla tutela della vita privata nell'esercizio dell'attività di controllo a loro affidata, a prescindere dal fatto che si tratti di sorvegliare i cittadini del proprio Stato, di un altro Stato membro o di paesi terzi;

13. si sollecitano i servizi di informazione degli Stati membri ad accettare i dati forniti da altri servizi di informazione solo nel caso in cui la raccolta di tali dati possa avvenire nelle circorstanze previste dal proprio diritto nazionale, poiché gli Stati membri non possono non adempiere gli obblighi derivanti dalla CEDU solo perché richiedono l'intervento di altri servizi di informazione;

14. si sollecitano la Germania e l'Inghilterra a subordinare l'ulteriore autorizzazione sul loro territorio di intercettazioni di comunicazioni ad opera dei servizi di informazione degli USA alla compatibilità con la CEDU, vale a dire tali attività devono soddisfare il principio di proporzionalità, avere base giuridica accessibile e conseguenze prevedibili per il singolo, e si esortano altresì i due Stati ad esercitare un controllo efficiente, poiché sono responsabili sul loro territorio della compatibilità dell'attività dei servizi di informazione, sia essa autorizzata o anche solo tollerata;

Sulle misure intese a promuovere l'autotutela di cittadini e imprese

15. si invitano la Commissione e gli Stati membri a sviluppare programmi volti a promuovere la sensibilizzazione di cittadini e imprese in merito alla questione della sicurezza e intesi al contempo ad offrire un sostegno pratico all'elaborazione e all'attuazione di concetti di protezione di ampia portata;

16. si esortano la Commissione e gli Stati membri ad elaborare misure adeguate intese a promuovere, sviluppare e realizzare tecnologie e software di cifratura europei e volte soprattutto a sostenere i progetti incentrati sullo studio di software di crittazione di facile uso il cui testo sorgente sia noto;

17. si sollecitano la Commissione e gli Stati membri a sviluppare software di cui sia reso pubblico il testo sorgente, in modo da poter garantire l'assenza di eventuali "backdoor" (cosiddetti "open-source software" o "software liberi");

18. si invita le istituzioni europee e le amministrazioni pubbliche degli Stati membri a ricorrere in modo sistematico alla cifratura dei messaggi di posta elettronica, in modo che nel lungo periodo la crittazione diventi un procedimento consueto;

Su altre misure

19. si sollecitano le imprese a rafforzare la cooperazione con i servizi di controspionaggio e a informarli in merito a particolari attacchi dall'esterno a fini di spionaggio industriale, in modo da potenziare l'efficienza di detti servizi;

20. si esorta la Commissione a presentare una proposta in merito all'istituzione di un servizio di consulenza europeo nel settore della sicurezza delle informazioni delle imprese, volto non solo ad accrescere la sensibilizzazione in tale ambito, ma anche ad offrire un sostegno pratico;

21. si invita il Parlamento europeo a organizzare un congresso transeuropeo sulla tutela della vita privata contro la sorveglianza delle telecomunicazioni, affinché ONG europee, statunitensi e di altri Stati creino una piattaforma che consenta di confrontarsi su aspetti transfrontalieri e internazionali e di coordinare i settori di attività e gli interventi.