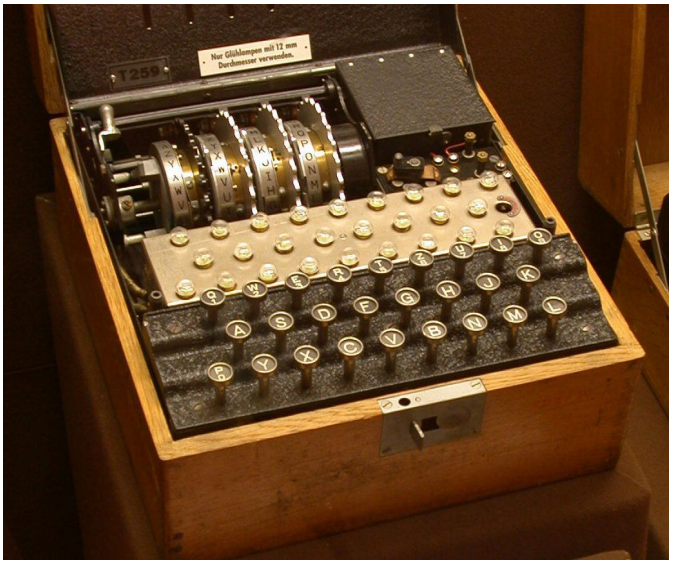
LE INTERCETTAZIONI DELLE COMUNICAZIONI: UTILITÀ ED OPPORTUNITÀ DI STANDARDIZZAZIONE

di Domenico Vulpiani e Carla Izzo

❶ *Introduzione*

L'avvento della rete, ed in particolare il *web* 2.0, ha mutato il modo di comunicare favorendo l'impiego di nuove modalità di crittazione delle comunicazioni *online*, e richiedendo pertanto sistemi sempre più sofisticati per rintracciare e decodificare le tante informazioni che ogni giorno attraversano la rete celate agli occhi dei più. **Se inizialmente l'esigenza di crittografare le informazioni era avvertita prettamente in ambito militare, oggi è una necessità cogente in più settori, da quello economico, commerciale a quello industriale**. Potremmo infatti dire che la sicurezza stessa di un Paese non può prescindere dalla sicurezza dell'infrastruttura di rete e da quella di comunicazione, perché da sempre riuscire a mettere le mani su informazioni strategiche per uno Stato rappresenta per i rivali un vantaggio non di poco conto ed il miglior modo per prevedere le mosse dell'avversario.



ENIGMA a quattro rotori
(fonte: http://pl.wikipedia.org)

A tal proposito, non si può fare a meno di accennare ad uno dei primi esempi di macchina cifratrice elettro-meccanica del secolo scorso, Enigma, ampiamente utilizzata durante la Seconda Guerra Mondiale che, contrariamente a quello che si pensa, non era nata in ambito militare, ma era stata ideata dalla Germania, sin dal 1918, proprio per contrastare fenomeni di spionaggio industriale. In seguito fu però utilizzata durante il Secondo Conflitto Mondiale[(1)]. I polacchi riuscirono a clonare Enigma, realizzando una macchina capace di cifrare i messaggi in maniera analoga e di conseguenza di decifrare quelli prodotti dai nemici, ma i Tedeschi ben presto se ne avvidero, modificarono il sistema di cifratura, rendendo così vano lo sforzo dei polacchi.

Quando la Polonia fu invasa, toccò agli Inglesi provare a capire i messaggi in codice dei nemici. A Bletchley Park, un sito segreto dedicato alla crittoanalisi, fu costituito un team di ingegneri e matematici, tra cui Alan Turing, che lavorò incessantemente per realizzare una macchina similare ad Enigma e riuscire a decodificare le comunicazioni. In particolare Turing svolse un ruolo fondamentale nel forzare il più complesso cifrario dell'Enigma navale, denominato Shark, circostanza resa possibile anche da una fortunata operazione militare.

Oggigiorno non si parla più di Enigma e di Bletchley Park , ma rimane comunque alta l'attenzione verso la protezione delle proprie comunicazioni, con l'unica differenza che chi sorveglia ha mezzi di straordinaria capacità, tanto da consentirgli di spostare l'attenzione dal singolo alla massa. Oggi si parla di Echelon, di Prism e del "Utah *Data Center*" .

Echelon è un imponente sistema di controllo delle comunicazioni gestito da cinque Stati firmatari dell'accordo di sicurezza: Australia, Canada, Nuova Zelanda, Regno Unito, e Stati Uniti. L'infrastruttura satellitare è stata installata sin dall'inizio degli anni Sessanta, in piena Guerra Fredda e negli anni '80 il nome in codice Echelon era anche il nome della rete dei *computer* della NSA. A seguito degli attentati dell'11 settembre è stata dedicata maggiore attenzione al traffico dati, alla posta elettronica, ai nuovi strumenti di comunicazione in rete e di telefonia (si veda il Patrioct Act del 26 ottobre del 2001 ed il successivo *Homeland Security Act* del novembre del 2002, nonché l'Irtpa ovvero la riforma dell'*intelligence* e della prevenzione del terrorismo del 2004)[(2)].

In seguito il sistema Echelon è stato sostituito dal programma Prism, gestito dalla *National Security Agency* (NSA) di cui nel dettaglio non si conoscono le potenzialità, ma di sicuro si sa che gestisce le informazioni raccolte da internet e da altri fornitori di servizi elettronici e telematici. Permette di analizzare le comunicazioni dal vivo degli utenti che avvengono via *email*, *chat*, VoIP.

Tutto questo avviene, e non potrebbe essere diversamente da così, mediante la collaborazione tra la NSA ed i giganti della rete, quali Google, Facebook, Microsoft, Twitter, Yahoo, Aol e Apple[(3)], a cui viene richiesto l'accesso a tali informazioni sotto l'approvazione di un mandato Fisa (il controverso *Foreign Intelligence Surveillance Act* rinnovato a dicembre 2012).

Si parla anche con grande insistenza del "Utah *Data Center*", il più grande centro di raccolta di dati del mondo, situato vicino a Camp Williams, una fortezza di 100.000 metri quadrati.

Sarebbe quello il luogo in cui fisicamente vengono ascoltate le conversazioni e monitorate le informazioni che quotidianamente viaggiano in rete, come ad esempio qualsiasi tipo di transazione che avvenga *online*. **Del resto gran parte del traffico mondiale delle comunicazioni fra utenti di nazioni diverse passa per ISP statunitensi e,** quindi per il Patrioct Act, **"per gli Stati Uniti"[(4)]**. Benché il capo della NSA, il generale Keith Alexander abbia rassicurato, dicendo "*non spiamo*

Utah *Data Center*
(fonte: http://www.businessinsider.com)

cittadini onesti, siamo al loro servizio e la nostra attività ha evitato oltre 50 attentati"(5), l'attività perpetrata dagli USA non va esente da dubbi, soprattutto a seguito delle rivelazioni diffuse da Edward Snowden. Tali rivelazioni hanno spinto il Presidente degli Stati Uniti, Barack Obama, ad annunciare una riforma della materia ed una revisione dei poteri della NSA. Il Presidente ha parlato di "*limitazioni nell'utilizzo dei dati dei cittadini ottenuti*", ma non ha aggiunto nulla rispetto alla loro raccolta. Si è anche parlato di permettere maggiore trasparenza, in particolare consentendo ai gestori di pubblicare le informazioni relative alle richieste di dati che ricevono dalle autorità.

❷ *Alcuni esempi concreti*

Le intercettazioni costituiscono da sempre uno strumento investigativo di estrema rilevanza e larga diffusione nel contesto delle indagini di Polizia Giudiziaria. **Ne sono un esempio gli innumerevoli casi risolti nel corso degli anni grazie al loro impiego**.
Negli anni Novanta, quando ancora internet non era così diffusione capillarmente, né tantomeno i telefoni cellulari erano così comuni, fu avviata un'indagine della Polizia di Stato, su un'organizzazione criminale presente a Roma e dedita al traffico dei sostanze stupefacenti dai Balcani in Italia.
Tale organizzazione, per poter comunicare con la Macedonia e con l'Albania, non poteva fare altro che utilizzare le cabine telefoniche pubbliche. Dopo mesi di pedinamenti e di appostamenti, si riuscì a risalire con l'ausilio del gestore telefonico ai due numeri telefonici chiamati più frequentemente dai malviventi. Tenuto conto che tutte le telefonate da qualsiasi parte provenienti ed indirizzate a tali utenze venivano convogliate verso un'unica centrale telefonica situata vicino a Fontana di Trevi, si poté intraprendere una serrata attività di intercettazione, monitorando e registrando tutte le chiamate verso i numeri in questione, indipendentemente dal punto in cui venivano effettuate. L'attività portò all'arresto di un'intera organizzazione criminale che aveva affiliati ben oltre i confini nazionali.
È utile ricordare anche un'altra indagine più vicina ai nostri giorni e realizzata soprattutto attraverso intercettazioni ambientali, telefoniche e telematiche. Si tratta dell'Operazione Hammam condotta in Umbria dalla Polizia Postale e dal servizio Antiterrorismo. Nell'ambito di tale operazione sono stati arrestati affiliati di una pericolosissima cellula terroristica specializzata nell'addestramento alle tecniche di guerriglia utilizzate dai fondamentalisti islamici, nonché molto attiva nella realizzazione di esplosivi, silenziatori per armi da fuoco. A seguito di accertamenti è emerso che l'*Imam* nel tempo aveva istruito molti integralisti islamici alla preparazione e all'uso di esplosivi, armi, sostanze chimiche nocive per avvelenare acquedotti.
Si è scoperto che gli arrestati avevano scaricato da Internet veri e propri manuali con le indicazioni per realizzare ordigni artigianali, con un ritmo che è arrivato fino a 20.000 documenti in una sola settimana.

❸ *La competenza giurisdizionale*

I fenomeni criminali che direttamente o indirettamente coinvolgono le tecnologie informatiche e telematiche, come già si è avuto modo di sottolineare in precedenza, hanno un carattere transnazionale che **impone di considerare in questo contesto la delicata questione della competenza giurisdizionale**. Tale aspetto, che ha sempre avuto un'elevata importanza alla luce della natura intrinsecamente globale della rete Internet, negli ultimi anni ha assunto una rilevanza ancora maggiore in ragione dello sviluppo e della diffusione di servizi basati sul *cloud computing*.
In questo caso, i *server* preposti all'erogazione del servizio possono essere fisicamente collocati in aree geografiche diverse da quelle dei soggetti giuridicamente responsabili degli stessi e/o da quelle degli utenti che ne fruiscono. Di conseguenza è molto frequente la circostanza in cui si debbano intercettare comunicazioni presso fornitori di servizi di comunicazione che hanno una sede fisica e/o legale esterna ai confini nazionali, nell'ambito dei quali l'Autorità Giudiziaria titolare dell'indagine ha la competenza territoriale. **Pertanto è fondamentale che gli Stati si prestino una reciproca assistenza giudiziaria nella repressione dei crimini informatici o perpetrati a mezzo informatico**. Lo strumento giuridico principe per condurre queste forme di collaborazione è costituito dalla rogatoria internazionale.
In considerazione del fatto che i sistemi giuridici e giudiziari sono diversi da uno Stato all'altro, per consentire la cooperazione in tale settore, molti Stati hanno stipulato convenzioni e accordi bilaterali volti a facilitare l'assistenza e la cooperazione giudiziaria tra le autorità nazionali coinvolte, detti *Mutual Legal Assistance Treaty* (MLAT), soprattutto con l'intento di ottenere una maggiore efficacia e celerità delle procedure.
A livello europeo, la norma capostipite è la Convenzione Europea di Assistenza Giudiziaria, firmata a Strasburgo il 20 aprile 1959. Inoltre, il Trattato sull'Unione Europea dedica il Titolo VI alle disposizioni sulle cooperazione di Polizia Giudiziaria in materia penale. In considerazione del fatto che molti fornitori di servizi hanno sede negli USA, particolare valore riveste in questo contesto anche il vigente Accordo sulla Mutua Assistenza Giudiziaria tra l'Unione Europea e gli Stati Uniti d'America.

Inoltre la legge n. 48/2008 ha ratificato la Convenzione del Consiglio dell'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001. **Con tale disposizione normativa (art.16) è stato introdotto anche l'innovativo istituto del "congelamento dei dati"** che prevede il mantenimento delle informazioni per un periodo massimo di novanta giorni, prorogabile fino a sei mesi, su richiesta del Ministero dell'Interno o, in sua delega, dei propri organi centrali specialistici in materia di informatica e telematica, come il Servizio Polizia Postale e delle

Comunicazioni. Tale previsione è stata concepita primariamente per adempiere alle richieste da parte di Autorità straniere, in modo da evitare di giungere alla scadenza dei tempi di conservazione previsti prima che si completi il complesso e lungo *iter* delle procedure di rogatoria. Si osserva, comunque, che la norma in questione non estende i limiti temporali massimi, ma **si limita a richiedere la conservazione di dati già acquisiti entro i termini previsti**.

❹ *Modello di utilizzo e opportunità di standardizzazione*

È chiaro che per la buona riuscita di operazioni come quelle descritte in precedenza è fondamentale che vi sia una stretta sinergia tra le forze di Polizia, i gestori telefonici e coloro che forniscono sistemi sempre più sofisticati d'intercettazione (c.d. *Vendors*), che studiano soluzioni rispondenti alle esigenze della Polizia italiana e soprattutto rispettose delle disposizioni emanate dal Garante della privacy in fatto di tutela della riservatezza dei dati. A fronte di un'indubbia efficacia, che costituisce la ragione del suo crescente utilizzo, questo mezzo di ricerca della prova è infatti caratterizzato da un elevato grado di invasività della *privacy* degli individui, consentendo di accedere in modo profondo alla sfera personale dei soggetti intercettati. A causa di questo effetto collaterale, quella delle intercettazioni è una tematica molto sensibile, caratterizzata da rilevanti implicazioni giuridiche, politiche e sociali.

Vale la pena sottolineare che l'attività di intercettazione, sebbene possa apparire simile a quella dell'acquisizione delle informazioni conservate dai fornitori dei servizi di comunicazione, affinità spesso foriera di confusione negli organi di informazione, in realtà incarna un approccio concettualmente complementare. Infatti, **le intercettazioni consentono di ottenere le informazioni di contenuto delle comunicazioni correnti e non si limitano, dunque, alla mera acquisizione delle informazioni riportate nei tabulati di traffico**, che caratterizzano solo gli attributi principali delle comunicazioni passate. Si può pertanto affermare che l'intercettazione costituisce lo strumento di indagine più incisivo a disposizione nel contesto delle reti di comunicazione.

In materia di intercettazioni sussistono rilevanti obblighi di legge per i fornitori dei servizi di comunicazione, che assumono la qualifica di operatori ai sensi del Codice delle Comunicazioni Elettroniche. Infatti, ai sensi dell'articolo 96 del predetto codice, questi sono tenuti ad assicurare una serie di prestazioni a fini di giustizia, c.d. "prestazioni obbligatorie". L'esecuzione delle richieste di intercettazione è infatti obbligatoria per tutti gli operatori. **In generale, anche le prestazioni relative alle richieste di intercettazione devono essere individuate in un apposito Repertorio, al momento non ancora disponibile**, che stabilisca le modalità ed i tempi di effettuazione delle prestazioni stesse, gli obblighi specifici, nonché le forme di rimborso dei costi sostenuti, la cui entità è specificata in un apposito listino.

Nello specifico, le intercettazioni avvengono oggi mediante una struttura tecnologica nella quale le linee captate, che trasportano voce o dati, vengono duplicate verso i centri di ascolto delle Procure della Repubblica che ne fanno richiesta. In tale contesto, l'ETSI, organizzazione europea che definisce raccomandazioni tecniche nel campo delle telecomunicazioni, raccomanda uno standard anche per le intercettazioni. **La standardizzazione delle procedure ha dei risvolti importanti sia per quanto concerne la cooperazione tra le forze di polizia** (vista la natura transnazionale di alcuni reati: frodi *online*, immigrazione clandestina, traffico di esseri umani, pedofilia) **sia sotto l'aspetto economico**. **Si ritiene opportuno sottolineare che sarebbe molto importante che gli organi istituzionali competenti (Ministero dello Sviluppo Economico, Ministero della Giustizia, e Ministero dell'Interno) condividessero pienamente il modello ETSI per le intercettazioni**, in particolare:

- il principio di separazione delle funzionalità dedicate ad erogare il "servizio", come ad esempio la chiamata telefonica o la connessione Internet, e quelle d'intercettazione dello stesso "servizio";
- il principio di standardizzazione delle modalità d'invio dei risultati delle intercettazioni verso le Procure, indipendentemente dall'operatore e dal "servizio" interessati.

Questo approccio determinerebbe una netta discontinuità con il passato, con sistemi di intercettazione strettamente dipendenti dalle specifiche tecnologie (spesso eterogenee e di tipo proprietario) degli apparati utilizzati dai *provider*. La piena conformità al modello ETSI sia da parte dei *provider* che da parte dei *Vendors*, prima citati, consentirebbe infatti di scegliere le soluzioni ritenute più idonee, senza essere assoggettati a possibili vincoli di carattere tecnologico indotti dalle reti di comunicazione. **La separazione delle funzionalità, inoltre, produrrebbe l'effetto di omogeneizzare il mercato, scongiurando possibili abusi dovuti a posizioni di dominanza e favorendo così la diminuzione dei costi sostenuti dalla Procure e dalla Polizia Giudiziaria**. In effetti, negli anni si è assistito ad un decremento dei costi unitari per il singolo obiettivo. Si ritiene, inoltre, che il modello ETSI favorirebbe in tale contesto una più chiara definizione dei ruoli, delle funzioni e delle responsabilità.

Tale obiettivo risulta di particolare importanza in relazione anche al soddisfacimento dei rilevanti bisogni di *privacy* dei cittadini. In Italia tale aspetto è stato accuratamente affrontato dal Garante per la Protezione dei Dati Personali, il quale con un recentissimo provvedimento datato 18 luglio 2013, ha prescritto alle Procure della Repubblica, misure e accorgimenti per incrementare la sicurezza delle informazioni raccolte ed usate nello svolgimento delle intercettazioni. Dai riscontri ottenuti è emerso un quadro variegato e disomogeneo, che ha posto l'esigenza di compiere interventi volti all'innalzamento del livello di sicurezza dei dati e dei sistemi usati per gestirli, nonché di estendere tali interventi alla generalità degli Organi Giudiziari.©

NOTE

1. Cfr. http://www.docente.unicas.it/useruploads/000789/files/04-enigma.pdf.
2. Cfr. "*Spionaggio Usa. In principio fu Echelon*" di Michele di Salvo (Rif. http://www.unita.it/mondo/spionaggio-tecnologico-una-br-tutto-inizio-da-echelon-1.508756).
3. Cfr. http://www.polisblog.it/post/166863/che-cose-prism-il-programma-di-sorveglianza-dellnsa.
4. Vedi "Sicurezza e Giustizia" n.III/MMXI, "*Il Patriot Act che permette agli USA di accedere ai dati degli utenti europei*" di C. Rogialli.
5. Cfr. http://ricerca.repubblica.it/repubblica/archivio/repubblica/2013/10/27/utah-viaggio-nella-fortezza-dove-lamerica-cela.html.◊