



## **Il nemico vi ascolta. Tacete!**

Chiaramente non alludiamo allo slogan fascista, né al film del 1943 con Stanlio e Ollio «Il nemico ci ascolta»

(  
*Air Raid Wardens*  
)

, ma a qualcosa di più serio: allo spionaggio informativo dilagante e, per finire, alle telecamere cinesi per come appresso illustreremo. Invero, si desidera far notare nel prosieguo come nel tempo, per un motivo o per un altro, il citato motto di avvertimento sia rimasto pur sempre valido e attuale.

Da che mondo è mondo lo spionaggio è sempre esistito. Gli antichi egizi elaborarono sapientemente un sistema per l'acquisizione di informazioni, a danno degli Ittiti, dopo la Battaglia di Qadeš (1296 a.C.) e per conseguire il controllo della Nubia, ma senza andare molto in là nel tempo ci ricordiamo di Pio V, fondatore dei servizi segreti vaticani nel 1566. Essi ricevettero la denominazione di 'Santa Alleanza', ma vennero meglio conosciuti con il nome de 'L'Entità'. Il compito di detti Servizi era quello di difendere in primis la cristianità e quindi, di riverbero, il potere del Vaticano. Ecco però che, a questo riguardo, all'attento osservatore non può sfuggire una situazione da *guinness*: un piccolo Stato, il più piccolo al mondo, con l'intelligence più antica dello spionaggio moderno!

Ma come la Danza Cosmica di Shiva, tutto però si evolve in un divenire che non permette più lo

staticismo scientifico. Col passar degli anni, infatti, tutti i governi si dotano di valide strutture spionistiche destinate ad ottenere la conoscenza di segreti, generalmente di rivali o nemici, al fine di proteggersi da minacce interne o esterne, nonché per conseguire vantaggi militari, politici o economici. Fioriscono gli 007, le super spie alla James Bond e nel contempo si fa a gara tra gli Stati per poter vantare il migliore apparato di Servizi anche perché questi ultimi rappresentano l'ostentazione della forza e della potenza di un paese nei confronti degli altri.

Lo spionaggio in realtà ormai non ha più limiti: si spiano i nemici, i concorrenti, gli amici, i propri cittadini e puranco i coniugi... infedeli. Invero, se con riguardo al primo soggetto lo spionaggio è sotto certi aspetti comprensibile, lo è molto meno allorché esso viene effettuato negli altri casi. Basti ricordare la situazione d'impaccio in cui gli USA si sono venuti a trovare con i governi amici di quasi mezzo mondo dopo le rivelazioni di Edward Joseph Snowden, sulla rete di spionaggio internazionale della NSA.

**In punto di diritto:** non esiste una norma sulla *intelligence*; non c'è mai stato nessuno che abbia pensato di stipulare una convenzione internazionale sullo spionaggio in tempo di pace e in particolare in nessun momento è stata presa in considerazione la fattispecie di spionaggio tra alleati. In quest'ultimo caso vien da chiedersi se esistano almeno delle regole, seppure non scritte, in materia, in quanto la trasgressione delle stesse sarebbe aggravata dalla violazione del rapporto di fiducia, che dovrebbe legare i Paesi amici.

Per lo spionaggio in tempo di pace, allo stato, è soltanto possibile pensare ad una normazione sull'estrazione non autorizzata di dati dalla rete, supportata dal diritto alla privacy e pertanto incriminare i *big* dell'Internet, che ne facciano indebito utilizzo.

In sostanza, solo dello spionaggio in tempo di guerra incontriamo una certa regolamentazione nel diritto internazionale: secondo la disciplina del Protocollo aggiuntivo alle Convenzioni di Ginevra, se una spia agente di una forza armata viene catturata dal nemico, sarà trattata da spia e non da prigioniero di guerra.

**In punto di fatto:** In questo stato di cose, in ambito internazionale e in tempo di pace «vale tutto»: ognuno dunque spia quanto più può e come meglio può!

**Le App ci spiano**

Ma puntiamo adesso l'attenzione sui comuni mortali, su di noi. Secondo le ormai diffuse informazioni la nostra privacy va a farsi friggere a causa delle moltissime App (applicazioni software dedicate ai dispositivi di tipo mobile, quali smartphone o tablet), che spiano la nostra vita nel Web trasmettendo dati, a nostra insaputa. Si è appurato, infatti, che gli hacker, tra i tanti mezzi fraudolenti, da tempo ci spiano con una nuova app che può essere utilizzata sugli smartphone; si chiama PlaceRaider ("malware visivo") e consente un utilizzo inizialmente limitato ai telefoni dotati del sistema Android, ma l'estensione ad altri smartphone, assicurano, sarebbe solo questione di tempo. Molto poco tempo, diremmo, per come corre la rivoluzione tecnologica.

Ma come tutto ciò può avvenire? Parrebbe che la PlaceRaider riesca ad acquisire immagini dal cellulare controllato in quanto ha la capacità di mettere in funzione la fotocamera, a distanza e senza che l'interessato se ne accorga. Attraverso le immagini rubate si potrebbero persino riprodurre modelli 3D che permetterebbero di ricostruire i movimenti del malcapitato hackerato o addirittura importanti documenti. È chiaro che la nostra vita ormai è controllata e registrata in un poderoso database alloggiato in chissà quale angolo remoto del mondo, a nostra insaputa per fini politico-commerciali.

Google analytics, per esempio, è lo strumento per eccellenza di analisi, usato da quasi tutte le app di geolocalizzazione. Alcune di esse sono contraddistinte da un numero ID che svela vita, morte e miracoli dell'utente. Non dimentichiamoci poi degli apparecchi dotati di GPS; in questo caso, senza volerlo, noi stessi riveliamo la nostra posizione ovunque ci troviamo.

## **Da chi siamo spiati**

Dopo questa breve esposizione sullo spionaggio e sulla criticità della nostra privacy, passiamo a esaminare da chi oggi siamo spiati e per quali motivi.

In Inghilterra una folta schiera di politici ha chiesto al governo di vietare la vendita e l'uso nel Paese delle apparecchiature di sorveglianza cinesi prodotte da aziende come Hikvision e Dahua. Ufficialmente dette aziende sono da bandire in quanto avrebbero dei legami con la violazione dei diritti umani nello Xinjiang (una regione autonoma della Repubblica Popolare Cinese): segnatamente, le telecamere installate nei campi di rieducazione per gli uiguri proverrebbero dall'azienda Hikvision.

Riteniamo che questa presa di posizione faccia parte delle buone maniere (*politeness*) inglesi e che la realtà sia ben altra: ci troviamo di fronte allo “scontro crescente tra tecno-democrazie e tecno-autocrazie” così come ha recentemente affermato Antony Blinken, segretario di Stato statunitense. Ovvero, due 'sistemi' che si spiano reciprocamente senza esclusione di colpi, ma guarda un po', ad un certo momento ci si accorge che il mondo è invaso non solo dalle chincaglierie, ma anche e soprattutto dai sistemi di videosorveglianza cinesi.

Secondo quanto rivelato su Rai 3 dal team di «Report» ci sono telecamere della Hikvision che aprono comunicazioni con IP cinesi. In altre parole possono inviare informazioni italiane alla Cina e cioè immagini, dati, intrecci di carte di credito, soldi e quant'altro immaginabile. A far capire la pericolosità di detta situazione basta ricordare che i termoscanner Dahua sono operanti a Palazzo Chigi e le telecamere Hikvision nelle Procure, nei Tribunali, nei siti sensibili come Malpensa e Fiumicino e infine nelle principali città italiane.

In Cina già da tempo esiste, oltre ai vari strumenti di controllo sui cittadini, il sistema del credito sociale (SCS), attraverso il quale il cittadino, per poter acquisire punti di merito o demerito, viene analizzato in tutti i suoi comportamenti attraverso l'incrocio dei dati che l'intelligenza artificiale ha raccolto su di lui: robe da fantascienza, è vero, ma occhio alla penna... dal momento che anche noi siamo 'osservati' dalle telecamere cinesi.

Un gruppo di specialisti svedesi accreditati presso lo «Swedish Center for China Studies» ha infatti stabilito che la tecnologia cinese per le smart city comporterebbe tra le altre negatività la possibilità dello Stato cinese di accedere con estrema facilità ai dati sensibili dei siti controllati. E vi sembra poco?

## **Soluzione**

Allo stato non esiste una soluzione: in vari paesi tra cui gli USA, l'Inghilterra, il Canada e l'Australia, esperti di cyber-security stanno analizzando i prodotti della Huawei e di altre industrie cinesi per verificare se esistano rischi per la sicurezza nazionale dal momento che, come abbiamo visto, la Cina pratica una strategia molto aggressiva e pericolosa di cyber-spionaggio industriale e... non solo.

il Parlamento europeo nel contempo ha votato per la rimozione delle telecamere Hikvision, mentre l'Italia, dal canto suo, ha preso opportuni provvedimenti, costituendo il Cvcn (Centro di valutazione e di certificazione nazionale) in capo all'ACN (Agenzia per la Cybersicurezza Nazionale). Ma serviranno queste misure a renderci liberi dalle insidie delle telecamere di sicurezza cinesi? Probabilmente non del tutto!

Anche se c'è 'puzza di bruciato', dal momento che non è la prima volta che il nostro Parlamento insabbia il dossier sulle telecamere cinesi, si spera che almeno le opportune contromisure di cybersicurezza riescano a neutralizzare in qualche modo indesiderate invasioni della nostra privacy.

Comunque sia, ahinoi, una civiltà sta finendo: siamo già nell'era digitale, dell'IA e ce ne dobbiamo rendere conto! Orbene, «Chi si è guardato si è salvato» dice un vecchio adagio calabrese, per cui nel dubbio, in questo ormai pazzo mondo orwelliano, sussurriamo: Pssst... il nemico ci ascolta e... ci scannerizza!

*G.&G.Arnò*