

UMBERTO DE GIOVANNANGELI
udegiiovannangeli@unita.it

«Fare chiarezza, senza lasciare alcuna zona d'ombra. È questo il passaggio ineludibile per ristabilire un corretto bilanciamento fra il diritto alla sicurezza e il rispetto della vita privata». Il «Datagate» analizzato da una delle massime autorità nel campo del Diritto internazionale: Fausto Pocar. Dal 1984 al 2000, il professor Pocar è stato eletto membro del Comitato per i Diritti Umani delle Nazioni Unite. Nel 1999 è stato nominato giudice del Tribunale internazionale per i crimini nella ex-Jugoslavia, divenendone presidente nel 2005, incarico che ha ricoperto fino al 2008. Dal 2000 è anche membro della Camera di Appello del Tribunale Penale Internazionale per il Ruanda.

Il «Datagate» si allarga a macchia d'olio. Soprattutto in Europa. Secondo quanto rivelato dal settimanale tedesco *Spiegel*, la cancelliera Angela Merkel era spiata dal 2002 e dal 2010 la National Security Agency e la Cia avevano attivato circa 80 reti di spionaggio ed intercettazioni in tutto il mondo, sul modello di quelle installate sulla fine degli anni 70 in Paesi nemici. Diciannove di questi gruppi di «ascolto» si trovavano in capitali europee, inclusa Roma.

il «Datagate» ripropone a livello globale il nodo non sciolto del rapporto tra il diritto alla sicurezza e quello alla privacy.

«Il problema sta nel bilanciare i diritti, quando in qualche modo possano confliggere. Così, ad esempio, il diritto alla libertà di espressione e il diritto alla reputazione delle persone. Spesso si evidenziano problemi di bilanciamento. Un punto cruciale, un vero e proprio discrimine, è quello che è stato più volte posto anche dagli organi internazionali sui diritti umani: il bilanciamento non può portare mai all'annullamento di uno dei diritti da bilanciare, a favore dell'altro. In questo caso, mi sembra che l'indagine a tappeto che ha messo a disposizione dell'Agenzia di sicurezza americana, la Nsa, questa enorme massa di dati si è spinta ben al di là di un bilanciamento che deve essere mantenuto all'interno della minore restrizione possibile dei diritti».

Qual è l'elemento più stravolgente che, allo stato delle conoscenze, è possibile individuare nel «Datagate»?

«Lo spionaggio relativo a qualsiasi tipo di dato, compreso quello di persone che non possono essere sospettate di terrorismo, o anche semplicemente di appoggio ad esso, come i capi di Stato e di governo europei o i membri dei Parlamenti nazionali, finisce per annullare completamente il diritto alla vita privata e

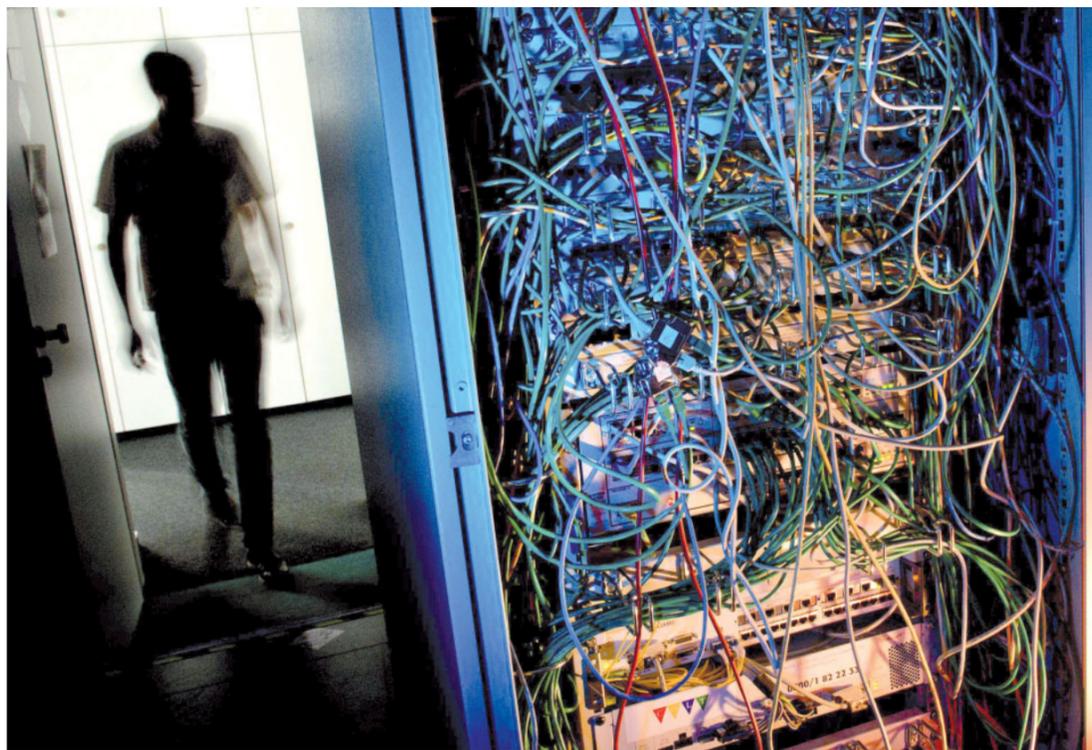


FOTO INFOPHOTO

Centro di ascolto a Roma Pocar: «Abusi inaccettabili»



L'INTERVISTA

Fausto Pocar

**Per l'esperto di diritti umani «la lotta al terrorismo non deve portare a gravi violazioni della riservatezza»
Centro Nsa nella Capitale**

quindi non rispetta quel principio di bilanciamento di cui parlavo in precedenza».

Questo spionaggio a tappeto è stato giustificato come necessario nella lotta al terrorismo.

«Dopo l'11 settembre, gli Stati Uniti hanno introdotto una serie importante di deroghe ai diritti fondamentali: tra queste deroghe, quella del controllo dei dati è solo l'ultima di una lunga catena, e se risulta più eclatante è perché a restarne coinvolti sarebbero leader europei e mondiali».

Una lunga catena. Quali i suoi gangli più significativi?

«Uno riguarda certamente la riduzione delle garanzie processuali in certi procedimenti penali, così come altre misure di controllo delle libertà di movimento. Per quanto riguarda i dati, mi sembra

che questo sia stato un punto centrale nella politica di sicurezza americana, e l'Europa ha contribuito all'acquisizione di molti dati».

A cosa si riferisce?

«Mi riferisco, in particolare, all'accordo con gli Stati Uniti che obbliga le compagnie aeree europee a fornire agli Usa le informazioni sui passeggeri che viaggiano tra i due continenti. E questi dati devono essere forniti per tutti i passeggeri, prima che arrivino sul territorio americano. C'è poi l'intesa riguardante i dati bancari. È vero che la sua gestione è affidata ad un'agenzia con sede in Belgio, ma questo accordo permette agli Stati Uniti di controllare tutte le transazioni interbancarie. Per non parlare dell'accordo che riguarda le società europee che trasferiscono personale negli Usa».

Cos'è che non va in questo accordo?

«Questo personale dovrebbe avere le stesse garanzie che ha in Europa sui dati, ma sta di fatto che gli Stati Uniti questi vincoli non li rispettano».

Come valuta la portata del «Datagate» e la reazione europea?

«È una situazione molto seria, rispetto alla quale le reazioni europee sono state finora molto limitate. Forse anche per il contributo che l'Europa ha fornito a questa politica, non necessariamente in blocco, da parte di tutti i Paesi, ma certamente da parte di alcuni Paesi importanti, come il Regno Unito, l'Irlanda e i Paesi Bassi. La cosa importante che si dovrebbe realizzare - al di là della reazione immediata di chi vuole denunciare gli accordi con gli Usa - è fare chiarezza. Una chiarezza necessaria per ristabilire un corretto bilanciamento fra il diritto alla sicurezza e il rispetto della vita privata e del diritto alla riservatezza».

Negli Usa le associazioni per i diritti umani contestano l'operato di Obama. In questo ambito, si sente deluso dal presidente?

«Un po' sì e me ne dispiace. Certo, la lotta al terrorismo ha registrato qualche successo con la presidenza di Barack Obama, anche se talora ciò è avvenuto con mezzi che a loro volta sollevano non pochi problemi nel Diritto internazionale, come gli omicidi a distanza commessi con l'uso dei droni».

Questa vicenda non pone il problema della qualità della democrazia?

«Direi proprio di sì. A essere messo in discussione è il rapporto tra cittadino e autorità, nel senso che il cittadino si trova esposto a qualunque iniziativa delle autorità basata su dati che non avrebbe l'obbligo di rendere noti alle autorità. Non è un caso che quanti hanno sollevato critiche negli Usa lo hanno fatto evocando il V emendamento della Costituzione».

La minaccia alla rete non viene dagli hacker

La notizia del giorno sul Datagate è quella di un fantomatico attacco hacker al sito della Nsa, che non è stato visibile per alcune ore. Secca smentita di *Anonymus*, che per la verità non ha mai nemmeno pensato ad azioni contro quel sito, e smentita anche da parte dell'agenzia d'intelligence americana che ha confermato quello che un po' tutti avevamo intuito: un semplice aggiornamento di sistema già previsto, che infatti si è svolto di sabato mattina, con il minore impatto possibile su dipendenti e utenti. La questione tuttavia riporta alta l'attenzione e l'allarmismo sull'idea che qualsiasi cosa non vada in rete «è colpa di hacker esterni». Questo può portare ad allentare la tensione sul tema delle intercettazioni illegali rilanciando la necessità di difendersi da questi attacchi. Ma il tema delle minacce alla rete è anche collegato alla difesa del diritto di espressione e di conoscenza e informazione, anch'esso minacciato in molte aree del mondo, soprattutto grazie al filtraggio o alla censura preventiva da parte di alcuni governi.

Spesso vittima di attacchi sono proprio siti e blog che fanno politica ed opinione, e qui il tema è in ottica diametralmente opposta. Nel corso del summit «Conflict in a Connected World» sono stati presentati alcuni nuovi servizi utili proprio a difendersi da questi at-

L'ANALISI

MICHELE DI SALVO

Per la Digital Attack Map sono più di 2mila gli attacchi digitali al giorno nel mondo. I più numerosi e intensi sono concentrati negli Usa

tacchi, e per poterli in qualche modo «misurare». Il più importante per i tecnici del settore è senza alcun dubbio quello realizzato da Arbor Networks in collaborazione con Google Ideas per la creazione di un sistema di mappatura degli attacchi DDoS globali attraverso la Digital Attack Map.

LA MAPPA

Sulla mappa mondiale vengono mostrati gli attacchi in ingresso e in uscita da un paese e l'eventuale attacco in corso tra due paesi. Ogni attacco è corredato da una serie di informazioni, tra cui la durata e «la forza». La Digital Attack Map viene aggiornata quotidianamente, e i dati storici sono consultabili per tutti i Paesi. Gli attacchi DDoS rappresentano la più diffusa, e semplice, forma di hackeraggio e si basano su una rete di computer che inviando numerose richieste di varia natura ad un sito, ne esauriscono le risorse (potenza di calcolo, banda) impedendo così l'erogazione del servizio a cui il sistema è adibito. Di fatto un attacco di pochi minuti può rendere un sito o un sistema o un intero servizio inagibile per ore se non giorni, e può provocare enormi danni, sia alle aziende o istituzioni che lo subiscono sia agli utenti.

Lo scopo principale della nuova mappa è quello di identificare quali sono i paesi da cui partono più attacchi e

quali sono i più bersagliati. Secondo Arbor Networks sono più di 2mila al giorno gli attacchi osservati nel mondo.

A leggere i dati si scopre che proprio gli Stati Uniti del tempo del *Datagate*, di *Prism* e delle intercettazioni dell'*NSA*, e della cyber guerra «contro gli attacchi esterni» sono anche il paese che di gran lunga esercita la maggiore potenza e intensità di questi attacchi, e prevalentemente entro i propri confini. Secondo alcuni analisti questi attacchi generano insicurezza, e fanno crescere l'esigenza di privati e imprese di sistemi e investimenti nella sicurezza informatica. Un po' come le aziende «antivirus» che negli anni novanta diffondevano virus per vendere la cura. Secondo altri questi attacchi interni servono a nascondere le infiltrazioni e le intercettazioni informatiche e nascondere le tracce.

Quello che però appare certo è che una simile potenza di attacco non è generata da singoli o gruppi di hacker, ma poggia necessariamente su infrastrutture di vasta dimensione. E questo non solo a guardare i dati Usa, ma anche quelli di Cina, Russia, Francia e Gran Bretagna. Ancor più se consideriamo che spesso queste risorse sono orientate entro gli stessi confini.

Come ha osservato un autorevole esponente della comunità *Anonymus* tedesca «alla fine è facile dare la colpa

agli hacker: tutti sanno che ci sono, ma nessuno sa chi siano, e la gente ci crederà perché gli hacker sono i cattivi. Peccato che Harper Reed, che ha curato la comunicazione web di Obama si auto-definisca egli stesso un hacker. Chissà se alla Nsa lo sanno».

L'INIZIATIVA DI ANGELA MERKEL

È proprio dalla Germania che in questi giorni è partita l'offensiva diplomatica che chiede conto agli Stati Uniti delle intercettazioni targate Usa. Sul piatto è stato messo tutto, dalle risoluzioni Onu alla interruzione delle trattative sull'area commerciale di libero scambio Usa-Ue. Sono stati proprio i «servizi» tedeschi e quelli francesi a far trapezare che ad essere intercettati non erano solo cittadini comuni, ma anche politici e membri di governo, facendo uscire la questione dai semplici confini di tutela della privacy, per farla rientrare nella sfera del vero e proprio controllo e spionaggio politico-finanziario.

Tra l'imbarazzo di Washington e qualche ammorbidimento delle posizioni nel documento congiunto di Bruxelles si delinea lo scenario della trattativa cui mirano i Servizi dei paesi Nato: condividere la grande mole di informazioni e dati raccolti, e soprattutto «la macchina» di decrittazione messa in piedi dalla Nsa. Oggi è un'arma paragonabile all'atomica nel 1948.