Brunei, il segretario di Stato Usa Kerry alla conferenza ASEAN FOTO DI JACQUELYN

Napolitano: una questione spinosa

● **L'Italia** «spiata» reagisce ● **Il ministro** della Difesa Mauro: a rischio i rapporti con l'alleato

UMBERTO DE GIOVANNANGELI
udegiovannangeli@unita.it

L'Italia non si accontenta della giustificazione di John Kerry. E, come hanno fatto Parigi e Berlino, anche Roma alza la voce. E chiede conto a Washington di un comportamento inaccettabile - quello del «Datagate» - che non può essere banalizzato, come ha tentato di fare il segretario di stato Usa sostenendo che cercare informazioni «non è inusuale».

Da Zagabria è sceso in campo lo stesso presidente della Repubblica, Giorgio Napolitano, per sollecitare chiarimenti: «È una questione spinosa che dovrà trovare risposte soddisfacenti». «Se è vero che le ambasciate europee compresa quella italiana sono state spiate, i rapporti fra Italia e Usa sarebbero compromessi», ha aggiunto, il ministro della Difesa, Mario Mauro.

FIDUCIA

«Se siamo alleati, se siamo amici non è accettabile che qualcuno si comporti come faceva una volta l'Unione Sovietica». Ribadendo che la vicenda è «molto spinosa», il ministro degli Esteri, Emma Bonino, ha riferito che la Farnesina si è attivata per sollecitare «i necessari chiarimenti» dagli Stati Uniti e si è detta fiduciosa che, «nello spirito di collaborazione e amicizia che caratterizza il rapporto tra i due Paesi, verranno fornite tutte le informazioni e assicurazioni necessarie». Ma l'imbarazzo resta. E va oltre le stesse dichiarazioni ufficiali. A gettare acqua sul fuoco delle polemiche è, da Gerusalemme, Enrico Letta. Le parole del presidente Obama ci confortano sul fatto che tutti i chiarimenti saranno dati. Non ho dubbi che questo avverrà e noi chiederemo che questo avvenga», dichiara il presidente del Consiglio ai microfoni di *Sky Tg24*. «Nella giornata di ieri (domenica, ndr) - spiega Letta - abbiamo concordato con il ministro Bonino la richiesta di informazioni che il ministro degli Esteri ha fatto nei confronti del governo degli Stati Uniti. Ma le parole - ha aggiunto - del presidente Obama oggi (ieri, ndr) mi confermano e ci confermano che possiamo avere fiducia nei suoi confronti e nei confronti della sua amministrazione che tutti i chiarimenti saranno dati. Non ho dubbi - ha concluso Letta - che questo avverrà e noi chiederemo che questo avvenga».

Ma la preoccupazione resta. «Apprendiamo con sconcerto dal sito del *Guardian*, che cita documenti fatti filtrare da Edward Snowden, l'ex analista dell'agenzia americana e talpa del *Datagate*, che l'Italia sarebbe stata un obiettivo della operazione di spionaggio messa in piedi dalla Nsa e perfino che agenti segreti Usa sarebbero arrivati a piazzare delle cimici all'interno dell'ambasciata italiana a Washington». Ad affermarlo è il vicepresidente dei senatori del Pd e capogruppo in Commissione Esteri a Palazzo Madama Giorgio Tonini. «Proprio la forza dei legami di amicizia che uniscono il nostro paese agli Stati Uniti d'America e la stima che nutriamo per il presidente Obama e la sua Amministrazione - prosegue l'esponente democratico - impongono che si faccia subito chiarezza sull'intera vicenda, e la si faccia nella sede naturale che è il Parlamento». «Bene dunque la convocazione del Copasir, per gli aspetti che riguardano i rapporti tra i servizi dei due paesi - conclude Tonini - Ma è altrettanto necessario e urgente che il governo venga a riferire alle Commissioni Esteri e Difesa di Camera e Senato».Il governo riferisca in Aula: una richiesta rilanciata da Sel e sostenuta da Scelta civica.

INDAGINI

«Come Pd avevamo già chiesto nelle scorse settimane di discutere il caso Datagate come uno dei temi fondamentali da affrontare. La questione è molto delicata e chiediamo che vengano coinvolti gli organismi parlamentari analoghi al Copasir esistenti negli altri stati europei e a livello di Unione. La valutazione e le risposte a nostro modo di vedere devono essere comuni e collegate perché riguardano alcuni dei diritti fondamentali delle persone», afferma il segretario Pd del Copasir Felice Casson.

...

La Farnesina ha chiesto i «necessari chiarimenti» all'amministrazione Usa Si attende arrivino presto

La pressione va a segno. «Il comitato che presiedo monitorerà la situazione in modo pressochè quotidiano sia con l'acquisizione di documentazione che con l'audizione diretta dei soggetti interessati». Lo ha detto il senatore Giacomo Stucchi, presidente del Copasir ai microfoni di *Radio1 Rai* a proposito della vicenda Datagate. «Domani (oggi, ndr) incontreremo l'ambasciatore Giampiero Massolo (direttore del Dis (Dipartimento informazioni per la sicurezza), per affrontare in modo specifico alcuni aspetti di questa questione che sta assumendo nell'opinione pubblica un certo rilievo ma che per la sua effettiva portata deve essere ancora ben definita- aggiunge- prima di esasperare l'opinione pubblica è opportuno capire bene quali siano stati gli atteggiamenti sbagliati in questa vicenda. Le trasmissioni dei dati sensibili avvengono solo in casi particolari, sono disciplinati dalle norme».

Fuori dalle dichiarazioni ufficiali, c'è un lavorìo sotterraneo che vede impegnata la nostra diplomazia.

Si tratta, spiegano a l'Unità fonti bene informate, di tenere insieme i buoni rapporti con l'amministrazione Obama senza dare l'impressione di sganciarci dalla dura reazione di Parigi e Berlino. E da una richiesta di chiarimento che non può restare inevasa.

«È con Echelon che parte la spy-story targata Usa»

Se Prism fosse solo la punta dell'iceberg? È questo il dubbio che è venuto a molti, anche nelle più improbabili spy-story e ricostruzioni dell'ultima ora, supportate da continue vere o presunte indiscrezioni e talvolta da notizie poco supportate da fonti, come nel caso di due giorni fa, quando il *Guardian* ha dovuto «congelare» una sua notizia per ulteriori approfondimenti. Le domande sono molte. Davvero gli Stati Uniti hanno spiato altri Paesi? Come si concilia questo con la sicurezza interna e l'antiterrorismo? Sino a che punto è penetrante questa attività di controllo? Si tratta della «mappatura» delle comunicazioni come per Prism, o anche dell'intercettazione del contenuto?

La macchina Usa del controllo delle comunicazioni è molto complessa e spesso rientra nella competenza di agenzie diverse, che hanno talvolta anche capi differenti (la Cia risponde al Pentagono e non ha competenza interna, l'Fbi risponde al ministro della Giustizia e ha competenza federale, l'Nsa risponde al gabinetto esecutivo del Presidente e così via) e comunque quasi sempre rispondono alle relative commissioni congressuali di controllo. Il più imponente sistema di controllo delle comunicazioni è Echelon - una denominazione utilizzata dai media e nella cultura popolare per descrivere la raccolta di *signal intelligence* e analisi gestita per conto dei cinque Stati firmatari dell'accordo di sicurezza (Australia, Canada, Nuova Zelanda, Regno Unito e gli Stati Uniti) noto come «cinque occhi».

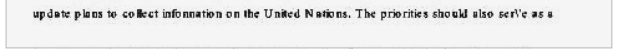
L'infrastruttura satellitare è stata insediata all'inizio degli anni Sessanta, in piena Guerra fredda. A lungo negata la sua esistenza, se ne deve la rivelazione a Margaret Newsham che sostenne di aver lavorato alla configurazione e all'installazione di alcuni software quando era impiegata alla Lockheed Martin, tra il 1974 e il 1984. In quel periodo il nome in codice «Echelon» era anche il nome della rete dei computer della Nsa. Lockheed lo chiamò P415. Con lo sviluppo della rete, e con la capacità di quest'ultima di trasmettere messaggi, grandi volumi di dati e informazioni e di consentire anche la comunicazione telefonica, si è reso necessario - in quel sistema - creare qualcosa di più «adatto ai tempi». Per farlo tuttavia si doveva in qualche modo bypassare la normativa sulla privacy e una serie di sentenze molto chiare e precise in termini di diritti civili che proprio negli Stati Uniti limitavano fortemente la capacità di controllo e di intercettazione.

L'occasione venne favorita dal Patrioct Act del 26 ottobre 2001 (sull'onda anche emotiva degli attentati dell'11 settembre) e dal successivo e specifico Homeland Security Act del novembre 2002 con cui venne riorganizzata complessivamente la Difesa, e ulteriormente dall'Irtpa, la riforma dell'intelligence e della prevenzione del terrorismo del 2004. All'interno di questo nuovo e poco conosciuto quadro normativo molta attenzione viene data al traffico dati, alla posta elettronica, internet, attività social e ai nuovi strumenti di telefonia e comunicazione in rete. Quasi tutti gli appalti - non solo di realizzazione ma soprattutto di gestione - vengono affidati a imprese private. Gli investimenti crescono in maniera proporzionale alla crescita della rete e le aziende private che ricevono grandi finanziamenti dalla Cia e dall'Nsa sono le stesse che svilupperanno gran parte dell'infrastruttura su cui girano attualmente i vari Google, Twitter, Facebook... In particolare «il padre» di Prism si chiama Perfect Citizen (sic!), un programma per rilevare gli attacchi informatici sulle aziende private e agenzie governative che controlla direttamente le «infrastrutture critiche», come la rete elettrica e le centrali nucleari, la rete telefonica, la rete del traffico aereo. Il programma nasce per mettere a disposizione dell'Nsa una rete di sensori distribuiti nelle reti di computer per le infrastrutture critiche, che avvisa in caso di attività insolite che possano suggerire un imminente «cyber attacco». Per la sola fase iniziale del progetto la Raytheon Corporation ha vinto un contratto segretato da 100 milioni di dollari. Le informazioni raccolte da «perfetto cittadino» fungono anche da banca dati utile per supportare le aziende e le agenzie che chiedono l'aiuto della Nsa per le indagini sugli attacchi informatici, come ha fatto Google quando ha subito un grande attacco alla fine del 2009.

Il programma è stato poi ampliato con il finanziamento multimiliardario del Cybersecurity National Comprehensive Act, iniziato alla fine dell'amministrazione Bush e continuato da parte dell'amministrazione Obama. Un atto così voluminoso (oltre 3000 pagine) che è probabile che nessuno si sia davvero preso la briga di leggerlo tutto, perché ad esempio avrebbe scoperto che consente «al Presidente degli Stati Uniti (...) in caso di grave minaccia per la sicurezza nazionale e la violazione delle informazioni (...) di "chiudere" la rete internet» (vedi foto 1). E qui la storia si complica, perché si salda con la visione del ruolo di internet come strumento politico-diplomatico. Da un lato infatti la rete va controllata, spiata, moderata e dall'altro la segreteria di Stato ne propone un'idea rivoluzionaria di esportazione della democrazia.

Prism nasce in questo difficile contesto, e deve bilanciare (ed essere bilanciato) da tre diverse tensioni e legislazioni: la salvaguardia della privacy, il controllo e l'intercettazione di messaggi e informazioni e la difesa dagli attacchi esterni. Diventa in qualche modo «l'aggiornamento 2.0» di Echelon, ma essendo la rete ontologicamente mondiale, a differenza del nonno (Echelon) e del padre (Perfect citizen) non ha né territorio, né confini e quindi non può avere in sé limiti. In più deve essere strumento al servizio di agenzie diverse, con regole diverse, che rispondono a capi diversi, e che hanno anche esigenze diverse. La stessa Hillary Clinton che al «News Musem» a gennaio 2010 propugnava una rete libera e democratica, il 26 novembre dello stesso anno scriveva alle rappresentanze diplomatiche americane nel mondo di dare il massimo supporto alle attività di intelligence della Nsa (foto 2 a destra), che operava nel quadro di un «accordo» tra dipartimento della Difesa e l'Agenzia per la Sicurezza Interna. Ed è tra le maglie del «non scritto - non vietato» di questi accordi che è stato possibile per la Nsa attraverso (anche) Prism di intercettare e controllare ben al di fuori del proprio territorio, dei confini nazionali e delle proprie competenze, in una inedita e insolita collaborazione con la Cia.

Il nodo di fondo non è solo il grado e la profondità delle intercettazioni, ma anche chi effettivamente abbia accesso - e in che modo e forma - a quel sistema che, a quanto è dato sapere, è gestito in appalto da aziende private. E in questo caso il conflitto di interessi sul contenuto delle informazioni acquisite può essere enorme.



US embassy cables; Washington calls for intelligence on top UN ofUcials

28 November 2010

Friday, 31 July 2009. 2024 SECRET SECTION 01 OF 24 STATE 080163 NOFORN SIPDIS EO 12958 DECL: 07/31/2034 TAGS PINR, KSPR, BOON, KPKO. KUNR SUBJECT:

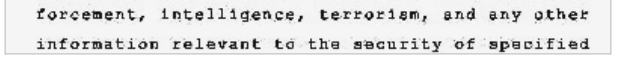
(S) REPORTING AND COLLECTION NEEDS: THE UNITED NATIONS REF: STATE

048489 Classified By: MICHAEL OWENS, ACTING DIR, INR/OFS. REASON: 1.4(C).

I. (S/NF) This cable provides the full text of the new National HUMINT Collection Directive

(NHCD) on the United Nations (paragraph 3-end) as well as a request for continued DOS reporting of biographic information relating to the United Nations (paragraph 2).

A- (S/NF) The NHCD below supercedes the 2004 NHCD and reflects the results of a recent Washington review of reporting and collection needs focused on the United Nations. The review produced a comprehensive list of strategic priorities (paragraph 3) and reporting and collection needs (paragraph 4) intended to guide participating USG agencies as they allocate resources and update plans to collect infonnation on the United Nations. The priorities should also serl'e as a



6/10/2010-Protecting Cyberspace as a National Asset Act of 2010-Establishes in the Executive Office of the President an Office of Cyberspace Polic which shall: (1) develop a national strategy to increase the security and resiliency of cyberspace; (2) oversee, coordinate, and integrate federal policies and activities relating to cyberspace security and resiliency; (3) ensure that all federal agencies comply with appropriate guidelines, policies, and directives from the Department of Homeland Security (DHS), other federal agencies with responsibilities relating to cyberspace security or resiliency, and the National Center for Cybersecurity and Communications (established by this Act); and (4) ensure that federal agencies have access to, receive, and appropriately disseminate law enforcement, intelligence, terrorism, and any other information relevant to the security of specified

Due documenti tratti dal Cybersecurity National Comprehensive Act

L'ANALISI

MICHELE DI SALVO
@disalvo

All'inizio la raccolta di «signal intelligence» su scala mondiale aveva il nome di «Cinque occhi». Poi le risposte agli attentati terroristici e il Patriot act tolsero altri freni allo spionaggio informatico