31ª SEDUTA

MERCOLEDÌ 11 OTTOBRE 1995

Presidenza del Presidente PELLEGRINO

La seduta ha inizio alle ore 18,10.

COMUNICAZIONI DEL PRESIDENTE

PRESIDENTE. Informo che è in distribuzione l'elenco dei documenti pervenuti dopo l'ultima seduta che la Commissione acquisisce agli atti dell'inchiesta.

Informo altresì che i collaboratori Giannuli e Leone De Castris hanno consegnato loro elaborati concernenti rispettivamente il convegno del «Parco dei Principi» e la strage di Gioia Tauro ed i moti per Reggio capoluogo.

Comunico che il dottor Libero Mancuso, l'ammiraglio Martini e il ministro dell'interno Coronas hanno restituito il resoconto stenografico delle loro audizioni tenutesi rispettivamente il 21 giugno e l'11 e il 27 luglio 1995 apportandovi correzioni di carattere meramente formale.

INCHIESTA SU EVERSIONE E LA FALANGE ARMATA: INCONTRO DI LAVORO CON IL DOTTOR PIETRO PAOLO SAVIOTTI ED AUDIZIONE DEL DOTTOR ALESSANDRO PANSA, DIRETTORE DEL NUCLEO CENTRALE CRIMINALITÀ ECONOMICA ED INFORMATICA DEL SERVIZIO CENTRALE OPERATIVO (SCO) DELLA POLIZIA DI STATO **(1)**

PRESIDENTE. L'ordine del giorno reca il seguito dell'inchiesta - già in corso nella passata legislatura - su eversione e Falange armata.

Su questo tema l'Ufficio di Presidenza ha tenuto un'audizione informale con il dottor Saviotti che conduce l'indagine in corso presso la procura di Roma. Alla fine di settembre-inizio di ottobre, come sapete, ci sono state nuove aggressioni informatiche che fra l'altro sembravano aver colpito (poi ci verrà detto in quali limiti la notizia era reale) il si-

(1) Per l'autorizzazione alla pubblicazione di passaggi svoltisi originariamente in seduta segreta, si veda il prospetto riportato a pag. XXV degli indici

stema informatico della Banca d'Italia. Per questo abbiamo ritenuto di fare questa seduta di aggiornamento per cui in libera audizione sentiremo anzitutto il dottor Pansa, che dirige il Nucleo centrale criminalità economica e informatica della Polizia, e poi il dottor Saviotti, il quale valuterà il grado di segretezza che caratterizza la sua indagine, sia per quanto vorrà dirci per aggiornarci, sia per quanto ritiene opportuno che sia detto in seduta segreta.

La seduta di oggi dovrebbe in qualche modo superare anche i limiti della vicenda Falange armata. Sarebbe bene approfittare dell'occasione che abbiamo per aggiornarci su questa che può definirsi una nuova forma di terrorismo. È una definizione che al primo impatto potrebbe anche sorprendere: non ci sono morti, attentati alla pubblica sicurezza o alla pubblica incolumità; ma direi che fa parte del vissuto della Commissione l'idea che il gesto di terrorismo è sempre qualcosa che vuole determinare allarme sociale ma che poi ha un fine ulteriore, cioè un allarme sociale che a sua volta è realtà strumentale, che tende a qualcosa. Direi che tutte le inchieste che stiamo facendo ci convincono che la finalità ultima del gesto terroristico è quella di influire in qualche modo su ciò che potremmo chiamare il corso apparente degli eventi.

Si tratta di fenomeni nuovi per cui la società moderna è opportuno che si attrezzi per le azioni di contrasto. È per questo che all'Ufficio di Presidenza è sembrato giusto fare questa seduta informativa e di studio.

Ritengo che sia opportuno iniziare proprio con il dottor Pansa che ringrazio di essere presente ai lavori della Commissione.

PANSA. Signor Presidente, fin dall'inizio chiedo scusa per eventuali imprecisioni che ci saranno nella mia esposizione. In poche parole mi viene chiesto di fare una presentazione di carattere generale sul problema dell'informatica e della sicurezza in questo settore e sebbene io abbia un'esperienza quasi decennale in materia, non ho una preparazione professionale specifica, essendo un laureato in giurisprudenza ed esperto di indagini in genere. La mia professionalità poi si è orientata verso questo settore, da un po' di anni, da quando ha cominciato a diventare di particolare allarme per la sicurezza pubblica.

Il problema dell'informatica è cresciuto rapidamente anche dal punto di vista della sicurezza negli ultimi tempi, per due ordini di motivi. Da un lato, vi è stata una rapidissima crescita delle capacità elaborative dei *computer*: fino a pochissimo tempo fa avevamo grosse macchine, molto lente, che raccoglievano molti dati ma che ne consentivano l'uso con estrema lentezza. La tecnologia ha consentito di ridurre la dimensione di queste macchine e dei loro costi e consente di gestire, con grande rapidità e con forme quasi intelligenti di elaborazione, una massa enorme di dati.

Contemporaneamente si è determinato uno sviluppo in un settore che fino a sei o sette anni fa e nell'ultimo trentennio aveva visto progressi estremamente scarsi, cioè le telecomunicazioni. Le telecomunicazioni, fino all'inizio degli anni '80, non avevano mai avuto un'evoluzione rapida o comunque di pari passo con la rivoluzione dell'informatica. Invece, sulla spinta dell'evoluzione informatica e sfruttando le risorse di quest'ultimo settore ed alcune alte tecnologie, le telecomunicazioni sono

diventate rapidissime, tanto che si parla di telematica, cioè una nuova forma di espressione delle telecomunicazioni che si avvalgono di strumenti informatici. Per cui non soltanto abbiamo grandi capacità elaborative, grandi masse di informazioni raccolte in vari posti – che nel gergo vengono detti «siti» –, ma abbiamo anche la possibilità di collegare tali siti fra di loro rendendo enormi le capacità di accedere alle informazioni da parte di chiunque, nel bene e nel male. Nel senso che la libertà di accedere a queste informazioni può rappresentare un bagaglio di conoscenze e una spinta allo sviluppo di una serie di attività, ma la libertà e la facilità di accesso a queste informazioni può determinare danni, perchè può impossessarsene chi non è autorizzato ed utilizza in maniera scorretta, chi non rispetta le regole.

Questo problema comincia a diventare fondamentale, perchè una miriade di attività che fino a poco tempo fa non ritenevamo potessero essere effettuate attraverso l'informatica, oggi convivono con questa realtà. Oggi l'informatica entra nella gestione delle informazioni più banali ma anche nella gestione di quelle più sofisticate: si parla di telelavoro, di telemedicina, di una serie di attività connesse ai sistemi informatici.

Vi sono moltissime procedure all'interno della pubblica amministrazione e dei processi produttivi industriali delle aziende, le quali non possono in alcun modo rinunciare alle potenzialità informatiche. In poche parole oggi l'informatica e le telecomunicazioni ci hanno portato ad un punto dal quale non possiamo tornare indietro. Cioè, abbiamo rinunciato – giustamente secondo me – ad alcune forme più arcaiche di gestione di una serie di attività per passare a quelle informatizzate. Non conserviamo più i vecchi sistemi e quindi la nostra funzionalità è affidata esclusivamente all'informatica.

Cosa comporta questo? Comporta che questi sistemi, sia per la loro sofisticazione che per la loro importanza e diffusione e per il ruolo sempre più importante che stanno avendo (la Convenzione di Strasburgo del 1981 parla di princìpi e diritti fondamentali del cittadino nelle comunicazioni e nella gestione delle informazioni, non soltanto in relazione alla tutela della *privacy*, ma anche in relazione alla possibilità di accesso alle informazioni attraverso i sistemi informatici) presuppongono un'assoluta democrazia e libertà di queste strutture. Per cui il problema fondamentale è che queste forme di gestione e di comunicazione dei dati debbono essere quanto meno sicure.

Ogni paese, ogni responsabile di area detterà le regole affinchè queste informazioni vengano utilizzate, raccolte e scambiate in un determinato modo. È indispensabile che queste regole possano essere rispettate; che vi sia una sicurezza formale ma anche una sicurezza sostanziale. In termini generali è evidente che abbiamo un'esigenza di tutela, prima di tutto a livello normativo. Nel nostro paese abbiamo dato il via ad una normativa nella materia attraverso un ordine inversamente proporzionale all'importanza dei diritti da tutelare: con l'informatica si è posto il problema – anche a livello comunitario – di introdurre norme specifiche che tutelassero i diritti fondamentali del cittadino, tutelassero e sanzionassero i comportamenti criminali, tutelassero i produttori di *software* con una estensione della tutela del diritto di autore. Nel nostro paese alla fine del 1992 e agli inizi del 1993 è stata deliberata soltanto la tutela

del *software;* agli inizi del 1994 è stata emanata una normativa sui crimini informatici e ancora si sta discutendo sulla tutela della *privacy*. Siamo dunque riusciti a tutelare in parte questo fenomeno, lasciando probabilmente da parte l'aspetto più importante.

Accanto a questa esigenza di creare delle regole, che il legislatore dovrebbe al più presto esaminare, c'è un'indispensabile esigenza: che le regole siano sicure, che l'informatica diventi sicura. Qui ci scontriamo con una realtà veramente preoccupante. I sistemi informatici, quelli di telecomunicazione, di telematica sono scarsamente sicuri; vi è una scarsa sicurezza a livello globale. C'è uno scontro anche di filosofie nella creazione delle architetture dei sistemi informatici tra coloro che concepiscono i sistemi ultrasicuri e ristretti e coloro che (e sono la maggior parte) creano sistemi aperti e accessibili contemporaneamente da varie parti. Nel nostro paese questo fenomeno di scarsa sicurezza diventa ancora più preoccupante per una serie di elementi che caratterizzano la realtà italiana.

In genere vi è una scarsa sicurezza nei sistemi informatici: e questo perchè da un lato tali sistemi sono patrimonio di un numero ristretto di persone che ha alte conoscenze della materia e che quindi può propinare a tutto il resto della società civile informazioni non verificabili e non controllabili. Questo consente a determinate persone di dire che certe cose non si possono fare, mentre dopo sei mesi scopriamo che si potevano fare, oppure che un sistema è sicurissimo e inaccessibile, per scoprire dopo quindici giorni che il sistema è accessibile anche a persone scarsamente esperte. Questa ristrettezza nell'accesso alle conoscenze dell'informatica è quindi un primo elemento. Vi è anche l'esigenza di proliferazione, sotto il profilo economico, dei sistemi informatici e dei sistemi distribuiti con innovazioni continue. Ciò che oggi è all'avanguardia nel settore dell'informatica diventa superato nel giro di pochissime settimane, di pochissimi mesi. In questi giorni si vede una pubblicità diffusissima, quella del programma Microsoft '95. Questo prodotto viene pubblicizzato come un prodotto altamente sofisticato, il più sofisticato nel campo del *personal computer*, ma già esistono e stanno per essere commercializzate le versioni più avanzate, che potranno essere reperite in commercio all'inizio del prossimo anno, tant'è che si chiameranno Microsoft '96. Quindi vi è una continua crescita delle capacità.

Questo significa che quello che noi oggi realizziamo in termini di sistemi sicuri all'esterno, rispetto agli accessi abusivi, nel giro di pochi giorni diventa insicuro perchè la tecnologia avanza e ha una grande capacità di superare le difese che vengono create. È un po' la vecchia storia delle forme di difesa: si creava il proiettile di maggiore potenza e conseguentemente si creava la corazza più resistente. Era una gara continua: un giorno vinceva il proiettile, e il giorno successivo la corazza. Nell'informatica succede la stessa cosa: un giorno vince la difesa, un giorno vince l'attacco. Proprio per queste ragioni la difesa non è affidabile in quanto è costretta a rincorrere continuamente le tecnologie.

A parte questo, vi sono situazioni contingenti che nel nostro paese rendono il problema un po' più grave che in altri paesi. L'Italia è sicuramente un paese in cui l'informatica è sufficientemente diffusa, non a livello di altri paesi industrializzati, però nella graduatoria mondiale dei

consumatori di informatica non siamo agli ultimissimi posti. Purtroppo, siamo però, per alcuni versi, ai primi posti tra i responsabili autori di crimini informatici. Siamo il primo paese europeo nella produzione di *virus* per *computer*: l'espressione *virus* è stata mutuata dalla biologia e significa che un programma *killer* può essere inserito nei sistemi informatici e può far ammalare l'apparecchiatura informatica, allo stesso modo del *virus* biologico per l'uomo. Esso soprattutto si diffonde e crea delle epidemie, così come nel campo medico. L'Italia è uno dei maggiori produttori, come dicevo, a livello europeo e sarà forse il secondo o terzo nel mondo. Inoltre ad una mancanza di sicurezza nel settore informatico nel nostro paese corrisponde anche una scarsa cultura dell'informatica. È difficilissimo fare entrare nella mente dei consumatori di informatica che le regole di sicurezza sono un elemento fondamentale per rendere sicuro il proprio lavoro. Per abitudine, quasi come una battuta, dico che una delle chiavi di volta per aprire il *computer* è una delle cose più semplici: il bigliettino autoadesivo «*post-it*». Se girate tra i *computers*, probabilmente anche di questo palazzo, troverete le *passwords* scritte sul bigliettino «*post-it*» attaccato al *computer*. Lo si fa per evitare di dimenticare la *password* ma in questo modo il sistema di sicurezza, vale a dire la *password*, che dovrebbe essere composta peraltro da un certo numero di caratteri alfabetici e da numeri in modo da rendere difficilissima la sua individuazione, si trova indicato in chiaro proprio vicino al *computer*. Quando non si trova il «*post-it*» si scopre che le *passwords* più diffuse sono le date di nascita o i nomi delle persone. Il caso specifico dell'accesso abusivo fatto all'Istituto nazionale di fisica nucleare - la fisica nucleare vive al di sopra delle nostre teste - è stato proprio l'uso come *password* del nome «Elisabetta». Esistono programmi che scandiscono e trovano le *passwords* per data o per nome. Considerate che un *computer* può scandire le date degli ultimi settanta-ottanta anni in cinquanta-sessanta secondi, oppure può scandire un intero vocabolario della lingua italiana o della lingua inglese in un minuto e mezzo.

Quindi i nomi più o meno comuni verranno scanditi in circa due minuti. Perciò, una *password* che non ha una logica costruzione basata sulla raccolta di numeri e di caratteri non legati al linguaggio naturale o alle numerazioni viene ormai scoperta potrei dire dai bambini, da chiunque ha un minimo di conoscenza d'informatica. Esistono programmini che sono di una facilità enorme per cercare le *passwords*. Vi sono regole fondamentali che vanno rispettate: non attacchiamo *post-it*, oppure chiudiamo la porta a chiave dell'ufficio dove esiste un *computer* che resta acceso, durante la notte perchè in quel periodo svolge un'attività di elaborazione che non ha bisogno della presenza dell'uomo, che è particolarmente lunga così la mattina, quando si torna in ufficio, il lavoro già è pronto: se lasciamo la porta aperta, quell'elaborazione può essere interrotta, modificata, alterata o resa non più utile da chiunque.

Accanto a questa situazione di scarsa cultura della sicurezza e a un ampio numero di autori di delitti in questo settore, c'è poi un'assoluta mancanza di disponibilità da parte dei gestori di sistemi informativi, dei titolari dei sistemi informativi e dei titolari delle aziende che utilizzano i sistemi informativi a denunciare i casi di accesso abusivo e di violazione.

Innanzitutto ci sono i responsabili dei sistemi informatici, sia nel settore privato sia nel settore pubblico, i quali per una questione di orgoglio, di superbia personale non ammettono che il loro sistema sia stato attaccato dall'esterno. Per cui, anche quando ciò accade, quando il loro sistema è oggetto di un'attività delinquenziale prevista dalla legge come delitto, non lo dicono, non lo denunciano e non hanno l'obbligo di farlo perchè non esistono leggi in tal senso. Tornerò poi su questo punto in particolare.

I titolari delle aziende, soprattutto quelle private, non ci tengono a far sapere che la propria azienda ha subìto un attacco informatico o un'azione o crimine informatico perchè ritengono (in questo caso soprattutto nel mondo bancario) che la caduta e il danno d'immagine sia sicuramente superiore al danno economico che può aver comportato il crimine informatico. Questo determina che noi non sappiamo realmente quale sia il numero dei delitti; non sappiamo realmente quale sia il *modus operandi* più comune e diffuso di fronte al quale ci potremmo difendere, conosciamo scarsamente questa realtà.

Accade spessissimo di leggere letteratura specializzata, di partecipare a conferenze, a simposi tra persone di altissimo livello (il dottor Saviotti ne è testimone) in cui ci raccontano di attacchi informatici e di epidemie di virus che sono accaduti in Italia e poi riscontriamo che non esiste una segnalazione all'autorità di pubblica sicurezza, non esiste la denuncia all'autorità giudiziaria di un fatto di questo genere. Si dibattono, si analizzano e si studiano casi del genere tenendo fuori però i tutori dell'ordine.

Veniamo qui al punto: esiste in Italia una normativa che sanziona i crimini informatici, che è abbastanza articolata, perfettibile o non perfettibile (tutta la normativa che riguarda i fenomeni criminali che sono fenomeni dinamici secondo me è sempre perfettibile), ma è una normativa ispirata un po' in maniera opposta a quella che dovrebbe essere una giusta tendenza. Sono cioè previsti numerosi reati perseguibili a querela di parte, meno sono i reati perseguibili d'ufficio. Quindi se viene consumato un delitto è la vittima del delitto che può, in relazione alla propria utilità, decidere se sia esercitabile o meno l'azione penale, se quel reato sia perseguibile o meno. In poche parole, questa normativa è ispirata ad un concetto di tutela dei diritti del singolo in via privata, cioè una tutela di diritti privati dei singoli utenti. Pertanto, non si pensa che il maggior bene che la normativa dovrebbe tutelare è l'interesse della collettività alla sicurezza dell'informatica perchè ogni piccolo delitto contribuisce a rendere meno sicuro il sistema informatico e l'utilizzazione dell'informatica e telematica nel proprio campo.

Veniamo adesso ad una valutazione del fenomeno criminale in Italia in merito ai crimini informatici. Abbiamo detto che non esiste una legislazione che tuteli la *privacy*, quindi la raccolta di informazioni anche a discapito del cittadino è un'attività per il momento non sanzionata dalla legge. Le banche dati, in Italia, hanno un solo obbligo, quello di farsi censire come tali, non per il contenuto dei dati e per l'uso che ne viene fatto. Quindi, l'unica banca dati – sembra assurdo – soggetta al controllo pubblico di una Commissione parlamentare è la banca dati delle Forze di polizia. Qualsiasi privato può raccogliere le informazioni che vuole e non c'è nessuna forma di controllo. Questo avviene solo per

la banca dati delle Forze di polizia. È giustissimo che essa venga controllata, ma non vedo perchè non debbano essere controllate le altre banche dati.

Quindi, a parte questa carenza normativa, oggi in Italia ci confrontiamo con un ampio fenomeno criminale. Per quanto riguarda la criminalità informatica, volendo oggi schematizzarla soltanto a scopo di esemplificazione e non di classificazione valida dal punto di vista criminologico, possiamo dire che esistono i reati informatici posti in essere dalla criminalità comune, quelli della criminalità eversiva e quelli della criminalità organizzata. La criminalità comune è sicuramente quella che ha la fetta maggiore di delitti consumati attraverso i sistemi informatici. Raccontavo prima al Presidente che vengo da un convegno che si è tenuto la settimana scorsa a Toronto e raccoglieva investigatori di trentacinque paesi. I colleghi canadesi ci comunicavano che i reati commessi con i *computers* nel loro paese determinano il danno maggiore per l'economia nazionale, più del traffico di stupefacenti, più delle rapine, delle estorsioni e di altre forme di reato che noi non abbiamo nel nostro paese, per fortuna, come le bande di motociclisti, eccetera.

Quindi, vi sono dei paesi a più alta tecnologia, a più alta evoluzione economica rispetto al nostro ma alla quale noi presto dovremo arrivare, che hanno come *target* principale dell'azione di contrasto e di prevenzione della sicurezza pubblica le frodi attraverso i *computers*. Ora, poichè ormai è noto che le fenomenologie che avvengono nell'America del Nord nel giro di pochi anni approdano in Italia, dovremmo incominciare a pensare che esiste una criminalità comune particolarmente agguerrita che è capace di sfruttare le tecnologie dell'informatica per commettere reati. Oggi falsificare titoli, documenti o banconote sfruttando le risorse dell'informatica è semplicissimo. Oggi le cosiddette carte intelligenti (la chiave del futuro per evitare le frodi attraverso le carte di credito o le carte di debito) già costituiscono una barriera superata perchè abbiamo cominciato a trovare dei criminali che riescono a contraffare i *microchip*. Le carte intelligenti sono quelle carte di credito che contengono in un angolo un *microchip* incorporato; questo microchip conterrebbe una chiave inviolabile da parte di un normale contraffattore. Invece recentemente hanno rubato in un paese europeo – non ricordo quale – non so quanti milioni di *microchip* per carte intelligenti. Questi *microchip* rubati devono avere una destinazione e sicuramente sarà quella di milioni di carte intelligenti false. Pertanto, le innovazioni tecnologiche che portano sicurezza nel settore incominciano a diventare scarsissime.

PRESIDENTE. Che cosa significa carta di credito falsa? Si parla forse della possibilità di addebitare il prelievo ad un'altra carta?

PANSA. L'addebito ad un titolare di carta di credito che l'abbia smarrita o la cui carta di credito è stata copiata è la forma più diffusa, ma la meno grave. Esistono forme di contraffazione di carte di credito che vanno quasi esclusivamente a danno o dell'ente gestore del servizio o del cliente, non del titolare della carta bensì del distributore di prodotti. Vengono infatti realizzate carte false o che non hanno corrispondenza con un vero titolare, che hanno una libertà di accesso completa e

che anche i sistemi di controllo non riescono più a bloccare. Ciò dà luogo a danni enormi, perchè la ripetitività di queste azioni è notevole.

Due o tre anni fa abbiamo avuto un caso - e mi riallaccio al tema della criminalità organizzata - a Roma, dove un gruppo di delinquenti comuni, anche se pericolosi, aveva organizzato la falsificazione di alcune carte Bancomat. Stavano cercando di intercettare le comunicazione tra lo sportello Atm (cioè il distributore dei soldi), il sistema della banca e la società che gestisce il servizio Bancomat in tutta Italia, la cui rete scorre attraverso linee dedicate. Con apparecchiature *vampire* (vampiri elettronici) via radio captavano e trasmettevano i dati. Quando un utente inseriva la carta essi attraverso la loro apparecchiatura vedevano cosa correva sulla linea e così capivano quale era il meccanismo. Con una serie di queste iniziative stavano cercando non più di prelevare con carte false bensì di immettersi nel sistema e, attraverso un meccanismo fraudolento di comandi informatici, far distribuire i soldi senza neppure le carte. Abbiamo subito consultato degli esperti del settore i quali hanno avuto una grossa preoccupazione ed hanno studiato bene quello che stavano facendo. Le persone furono arrestate e furono sequestrate tutte le attrezzature: erano arrivati ad un punto molto avanzato in questa tecnica, però mancava loro qualcosa per essere efficientemente operativi, qualcosa che secondo i tecnici costoro non avrebbero mai potuto ottenere perchè si trattava di codici custoditi in archivi segreti eccetera eccetera. Nessuno di loro però ha pensato che l'organizzazione criminale può superare questa difficoltà: sequestra il figlio del titolare della Sia, quello gli dice la cosa supersegreta che loro non avevano la possibilità di ottenere. Questo succede a livello di criminalità organizzata, la quale comincia ad impossessarsi delle tecniche aggiungendo risorse proprie della criminalità organizzata: la violenza, la capacità di corrompere. L'informatica in mano alla criminalità organizzata rischia di diventare uno strumento veramente pericoloso.

Per venire al tema di oggi, cioè alla criminalità eversiva e al terrorismo, il fenomeno in effetti nel nostro paese, come in altri, è abbastanza diffuso; in forme probabilmente non molto preoccupanti, fino ad oggi, ma non sappiamo quale sarà l'evoluzione.

Abbiamo conoscenza molto generica delle tecniche che sono state usate da alcuni paesi durante alcune situazioni conflittuali. La guerra del Golfo è un caso di questo genere ma anche l'Organizzazione per la liberazione della Palestina pare che in alcuni momenti abbia avuto piani e programmi di guerra elettronica o di attacchi elettronici per rendere meno efficienti le difese dei paesi. Se n'è parlato, ma non si è mai avuta diretta conoscenza, di controlli a distanza di petroliere, di metanodotti, che potevano essere realizzati attraverso incursioni informatiche da parte di terroristi. Sono tutte ipotesi, probabilmente quasi tutte di fantasia che però potrebbero diventare realtà fra pochissimo tempo.

La realtà che conosciamo per certa è fatta di un numero abbastanza vario di situazioni. Possiamo dire che il terrorismo, l'eversione informatica è nata un po' con l'informatica stessa. Da diversi anni esiste ad Amburgo - ormai funziona a scartamento ridotto - il *Caos Computer Club*, un circolo regolarmente autorizzato che negli anni si è scoperto essere il covo di un gruppo di persone di varia estrazione che coltivavano una

comune ideologia di tipo anarcoide, cioè la liberalizzazione totale dei sistemi di comunicazione. A tale fine essi dimostravano come i sistemi fossero inefficienti. Sono gli autori degli attacchi ai sistemi della Nasa, del Pentagono e degli episodi più eclatanti, gli attacchi più noto del passato.

Questa realtà nel tempo è andata a sparire, in Germania, mentre hanno proliferato organizzazioni similari in molti paesi. Anche in Italia esistono gruppi di ispirazione libertaria, con base ideologica non ben definita ma di tipo anarcoide, che svolgono attività di *hackeraggio*, cioè arrembaggio attraverso le reti telematiche o sistemi informatici. In altre parole, attraverso un collegamento io posso accedere a qualsiasi *computer* per utilizzarlo oppure diventarne il gestore. Assunto il controllo di un *computer*, riesco ad aggredirne altri a distanza e riesco ad usarlo per qualsiasi tipo di elaborazione o, per esempio, per collegarmi con altri *computer*. Esistono dei sistemi di comunicazione gestiti da gruppi antagonisti dell'eversione di destra o dell'eversione di sinistra (quelli che hanno quasi esclusivamente scopi di proselitismo) che utilizzano dei Bbs, cioè piccole banche dati che collegano fra di loro vari soggetti. Ad esse si accede attraverso un semplice *modem*, cioè un accoppiatore *computer*-linea telefonica: il *modem* non è altro che un modulatore della frequenza che assimila la frequenza del *computer* a quelle telefonica. Esso consente di collegarsi attraverso la rete telefonica con altri *computers* o ad un *computer* centrale, gestore e distributore di informazioni. Attraverso i *computers* poi si può inviare un messaggio ad un'area comune ove un altro mi risponde, oppure un terzo interviene e dibatte con me l'argomento del mio messaggio.

Poi ci sono gruppi dell'area dell'autonomia che utilizzano i sistemi informatici allo stesso modo di quando io andavo all'università ed usavo il ciclostile che all'epoca era il sistema più diffuso di diffusione delle informazioni. Oggi questo viene fatto attraverso il *computer*, ciò è corretto quanto si tratta di dibattiti politici o culturali. Vi si trasmettono però anche ordini e direttive a distanza. Sulle reti informatiche circolano quei libercoli che noi trovavamo nei covi: il libro di Marighella «Cos'è un terrorista», «Come si fa una bomba atomica», oggi circolano attraverso le reti telematiche. Nessuno farà la bomba atomica, perchè chi ha queste informazioni non ha la tecnologia per utilizzarle, ma può stabilire dei legami, impartire degli ordini, costruire attraverso la telematica reti che consentono a gruppi organizzati sul territorio di comunicare fra di loro, anche a bassissimi costi. Infatti l'informatica oggi rappresenta probabilmente anche la nuova frontiera della democrazia, perchè ha costi bassissimi. Oggi è possibile accedere ad informazioni che prima, essendo a distanza enormi, erano difficilissime da raggiungere ed altri sistemi per ottenere questo tipo di informazioni erano impraticabili. Prendiamo ad esempio l'enciclopedia Treccani, molti ce l'hanno, molti la sognano: oggi si può accedere a questo tipo di informazione con uno strumento che costa poco più di un milione (il *computer*); ma posso accedere anche a migliaia di biblioteche spase nel mondo, a migliaia di risorse informative e culturali. Si tratta probabilmente di una nuova espressione di democrazia, che addirittura fa rendere evolutivo il fenomeno in quanto è un metodo di accrescimento della cultura e delle possiblità di comunicare.

A questo punto probabilmente è opportuno che io fornisca proprio sulle reti telematiche qualche cenno, anche perchè quando si parlerà poi del caso specifico della Falange armata potremo vedere meglio a quale fenomenologia l'attacco informatico di questa presunta organizzazione corrisponde. La rete telematica più nota è Internet. Internet non è una vera e propria rete ma un insieme di *gateway*, di elaboratori che vengono utilizzati come porte per accedere a reti telematiche già esistenti. Sparse per il mondo ci sono grosse banche dati e grosse reti di collegamento a queste banche dati; esistono elaboratori che hanno la loro capacità di elaborazione...

PRESIDENTE. Chi ha organizzato la rete *Internet?*

PANSA. È un'iniziativa privata. Internet nasce prima di tutto in sede universitaria come esigenza accademica per collegare le banche dati di varie università nordamericane ed occidentali; poi mano a mano questa rete si è sviluppata con la creazione di *gateway*. Non c'è un gestore di *Internet* ma esistono quelli dei vari snodi di *Internet*; pertanto *Internet* è formata da varie società. Più che un meccanismo tecnologico è un meccanismo commerciale: esistono delle porte per accedere a delle reti che vengono collegate tra di loro.

PRESIDENTE. Ci saranno quindi anche dei commercianti?

PANSA. Sono i titolari delle *gateway*: sono delle aziende che danno la possibilità di accedere alle reti creando dei programmi che consentono di comunicare con facilità ed uniformità di linguaggio tra diversi elaboratori che normalmente parlano lingue diverse. L'informatica ha determinato una proliferazione di linguaggi: alcuni *computers* non possono colloquiare con altri *computers* perchè parlano lingue diverse: uno parla inglese l'altro scrive in italiano. Come farebbero questi *computers* a comunicare: la risposta è la *gateway*; i *computers* si possono mettere in comunicazione proprio perchè la *gateway* rende la comunicazione meno difficoltosa attraverso un protocollo di comunicazione unico. Soprattutto è possibile a livello locale il collegamento con gli utenti, mentre i due *computers* si trovano a distanze enormi. Se volessi collegarmi direttamente con uno di questi *computers* dovrei fare un'interurbana di altissimo costo; invece collegandomi con la rete urbana italiana dove si trova il *gateway* la connessione con il *computer* a distanza viene realizzata dal *gateway* stesso. Devo soltanto pagare al gestore del *gateway* un abbonamento e la singola chiamata; il numero degli abbonamenti è tale che il gestore ha un utile economico. Questo meccanismo man mano che prolifera rende la rete sempre più ampia e distribuita per cui ognuno in teoria (fino adesso non credo che ci sia qualcuno che abbia la capacità di navigare in tutta Internet perchè bisogna conoscere le modalità di accesso) può conoscere l'elenco delle autovetture di Tokyo. Se volete sapere come si può arrivare a questa informazione difficilmente potrei dirvelo: avrei bisogno almeno di lavorare venti giorni su Internet: per scoprirlo anche se alla fine ci arriverei. Questa è la realtà di Internet una delle vie più diffuse.

In Italia vi è una rete di comunicazione dati che si chiama *Itapac*: una rete costituita da Telecom Italia. Si tratta di una rete di telecomunicazione attraverso *computers*: esistono delle centrali, come le centrali telefoniche; gli utenti sono collegati con dei terminali che non sono dei telefoni ma dei *computers*. La rete Itapac è accessibile anche per linee telefoniche e quindi non solo mediante linee di trasmissione dati. Esistono dei numeri di centrali telefoniche alle quali qualsiasi *computer* con un *modem* (il modulatore che cambia la voce del *computer* facendola diventare voce telefonica) può collegarsi per entrare nella rete *Itapac*. Anche questa rete è nata per esigenze universitarie e poi si è diffusa tra un certo numero di aziende che avevano magari i propri uffici distribuiti per il territorio e non avevano la possibilità di creare una propria rete privata. Queste aziende hanno così usufruito della rete pubblica. Esistono poi dei *computers* che hanno delle piccolissime reti e offrono la possibilità di accesso attraverso un numero telefonico. Ci sono grossi *computers*, grosse banche dati accessibili per via telefonica: basta comporre un numero per parlare con la base dati. Ovviamente occorre avere il *computer* che parla il linguaggio adatto, ma basta una telefonata. Il concetto che ispira le comunicazioni nel settore dell'informatica è la massima apertura, la massima capacità di comunicare anche con il famoso *computer* dove, come dicevamo, è nascosto l'elenco delle vetture di Tokyo. Questa comunicazione è difficilissima se non conosco l'indirizzo, il numero di telefono o il numero di Internet, ma se ho quel numero non impiego niente a chiamare per telefono con un *computer* e a ottenere l'informazione, una informazione così lontana eppure così facilmente accessibile. All'interno di questi circuiti, *Internet* o *Itapac* che siano, vi sono dei gestori di informazioni che come unica attività gestiscono gli indirizzi. In Italia esiste la Seat che compila gli elenchi telefonici; allo stesso modo alcune aziende compilano gli elenchi dei numeri Internet. Chiunque si collega ad Internet rende pubblico il numero proprio per avere la possibilità di ricevere comunicazioni. D'altronde se il suo numero fosse privato a che cosa gli servirebbe tale collegamento? Quanto più il suo numero è diffuso tanto più può comunicare. È come il numero telefonico apposto sul biglietto da visita che viene dato a tutti; oggi viene inserito anche il numero Internet. Per accedere alla porta Internet della Banca d'Italia, dietro la quale non c'è praticamente quasi niente, basta conoscere il numero che la Banca d'Italia ha reso pubblico. Chiunque voglia ricevere informazioni o comunicare può mettersi in contatto, grazie ad un *computer*, con la Banca d'Italia ma è bene tenere presente che il centro dati della Banca d'Italia è da tutt'altra parte. Anche le banche danno informazioni per motivi di studio, di informazione e di pubblicità ai clienti: esse sono collegate con questi sistemi, ma il sistema informatico delle banche si trova da tutt'altra parte. Credo di aver già occupato troppo tempo e spero di essere stato sufficientemente chiaro.

PRESIDENTE. Ringrazio il dottor Pansa di questa lezione introduttiva su questo nuovo, complesso e interessante settore. Darei adesso la parola al dottor Saviotti perchè tutte queste nozioni di carattere generale possano essere riportate allo specifico tema della nostra inchiesta che riguarda questa nuova forma di terrorismo informatico condotta

dalla Falange armata. Ricordo al dottor Saviotti che, quando lo ritiene opportuno, possiamo passare in seduta segreta.

SAVIOTTI. Se posso, con una battuta, ricollegarmi all'intervento del dottor Pansa quando richiamava i volantini ciclostilati dell'università, direi che oggi il comunicato della Duchessa sarebbe diffuso via *Internet*. Ecco un particolare su cui vi è necessità di tornare: il sistema è tale da garantire già di per sè (salvo qualche ulteriore accorgimento) l'anonimato di chi entra, di chi va a depositare informazioni o a prenderle o eventualmente a inserirsi e a manipolare banche dati. L'anonimato è un po' insito nel sistema stesso ed è voluto e ricercato da coloro che gestiscono i diversi sistemi telematici. Tutto questo è facilmente realizzabile attraverso minimi accorgimenti che un buon gestore di *computer* è in grado di mettere in atto.

Ora, per essere pertinente - per quanto è possibile, anche in relazione alle indagini in corso - al tema dell'incontro di oggi, passerei ad una breve panoramica, una breve spiegazione di ciò che è successo tra venerdì 29, sabato 30 settembre e domenica 1° ottobre scorsi.

Nel giro di poche ore sono state violate almeno quattro banche dati perchè attraverso i sistemi di comunicazione - *Internet* o *Itapac* - gli accessi, come diceva il dottor Pansa, esposti all'indirizzario comune erano anche accessi, contemporaneamente, alla banca dati e al sistema informativo che lavorava con lo stesso macchinario, la stessa strumentazione utilizzata per il collegamento. Questo molte volte è funzionale all'attività che si svolge all'interno di quel sistema informativo che deve essere in grado di ricevere, dialogare e scambiare informazioni, ovviamente previe le autorizzazioni del caso.

Quindi, l'essere riusciti ad accedere ad un determinato terminale, ad un punto di riferimento, ad un indirizzario *Internet*, ad un punto *Itapac* ha poi comportato questa ulteriore attività di superare le *password*, le parole chiave, di usare il nome di utente giusto per entrare all'interno di quel sistema.

Nel giro di poche ore - dicevo - abbiamo queste quattro violazioni.

PRESIDENTE. Vorrei chiederle se si entra nella banca dati per sapere che cosa c'è oppure per modificare e quindi falsare i dati che sono depositati nel sistema? Per esempio, entro nel sistema per sapere quali sono le ricchezze bancarie del mio avversario politico e poi, quando ho l'occasione, chiedo polemicamente com'è che ha tutti quei soldi oppure com'è che ha tutti quei debiti, o mi inserisco per modificare i dati per cui, improvvisamente, se il mio avversario emette un assegno la banca non lo paga perchè il conto è scoperto?

SAVIOTTI. Posso fare tutto in dipendenza delle mie capacità e del livello di protezione del sistema: massimizzando l'uno e minimizzando l'altro posso veramente far di tutto a tutti i livelli. Poi, dipende da qual è il mio obiettivo. Posso solo curiosare, posso solo divertirmi, posso solo apprendere, posso manipolare, posso aggiungere qualcosa, posso cancellare tutto, posso inserire un *virus* a tempo per farne oggetto poi di un'estorsione. Molti di questi *hackers* lavorano proprio per fini di pro-

fitto, magari minacciano il sistema informativo di una banca dati, dimostrano le loro capacità di aggressione e poi chiedono di essere assunti, dimostrando di essere gli unici a poter tutelare quel sistema di sicurezza; oppure, si giunge ad estorsioni ancora più banali, proprio sul piano strettamente economico.

I sistemi informativi che sono stati aggrediti tra il 29 settembre e il 1° ottobre sono stati individuati in due sistemi pubblici e due privati: l'Istituto di fisica nucleare presso il Gran Sasso, la Banca d'Italia e due società private di buon livello economico, due medie imprese. L'aggressione si è verificata in poche ore. In realtà, in nessuno di questi casi si è verificato un effettivo danno: chi è entrato, pur potendolo fare, non ha cancellato nè manipolato dati.

PRESIDENTE. Possiamo sapere se siano stati acquisiti dei dati?

SAVIOTTI. *Sicuramente ha potuto leggere ciò che c'era all'interno* di questi sistemi informativi, ha potuto sicuramente trarne copia. Abbiamo appurato con un certo stupore che in realtà il sistema informativo aggredito dell'Istituto di fisica nucleare del Gran Sasso era un sistema marginale e periferico rispetto a quello che gestisce la massa di informazioni di esperimenti in corso sotto quella montagna, però aveva una sua funzionalità: gestiva la ricerca di un certo progetto «barex» sul neutrino del valore di svariati miliardi. Chi è entrato dentro il sistema ha potuto vederlo. È entrato dentro il sistema e vi permaneva - badate bene - mentre gli operatori lavoravano e non si accorgevano che qualcuno si era inserito nel sistema e poteva, volendo, bloccare tutto o cancellare dati, invece ha solo guardato.

Per quanto riguarda la Banca d'Italia, è successa una cosa analoga: vi è stata la forzatura della parola chiave e sono entrati in un sistema, questa volta sì marginale e periferico rispetto al complesso dei sistemi informativi attraverso cui la Banca d'Italia esercita le sue competenze.

Sui due sistemi privati vi è poco da dire: gestivano informazioni di natura commerciale, non mi sembra vi fossero dati di particolare interesse se non appunto la mera capacità di dimostrare di essere in grado di entrare ovunque si volesse.

Non a caso, poi, queste quattro azioni vengono rivendicate in modo chiaro e in tempi abbastanza rapidi con dei comunicati per un certo aspetto forse ingenui, ma sicuramente significativi: «Noi ci siamo. Voi avete le reti, avete le informazioni, avete la tecnologia: noi abbiamo voi, le vostre case, le reti. Rivoluzione sì, ma nuova, come non l'avreste mai immaginata. Falange armata».

PRESIDENTE. Vi sono segnali che vi portano a ritenere autentica quella firma?

SAVIOTTI. In un comunicato vi è una dizione specifica che ricorre in altri casi. Però, oltre questo, per il momento non siamo in grado di andare. Quello che colpisce e ha colpito sia me, sia gli investigatori *dello Sco e della Digos, è stata la simultaneità della diffusione di questi* messaggi di rivendicazione della Falange armata. Infatti, nel giro di poche ore sono pervenuti o via *fax* o via *Internet* o attraverso altri sistemi

di diffusione a più redazioni di giornali, a soggetti privati e a varie entità pubbliche.

Mi sono trovato, in particolare nel pomeriggio di sabato 30 settembre, tempestato di telefonate di giornalisti che già erano al corrente di quello che era avvenuto, cioè che c'erano state queste aggressioni, anzi, che la Falange armata le rivendicava. La prima reazione è stata veramente di forte preoccupazione, perchè se nel comunicato si diceva che era stata aggredita la Banca d'Italia, ad una prima verifica effettivamente un *computer* della Banca d'Italia era stato violato. Mi spiegavano che nell'ambito delle competenze della Banca d'Italia ve ne sono alcune importantissime: se la Banca d'Italia banalmente non riesce a sapere quanta carta moneta è stata ritirata e quanta emessa, se perde il controllo di questo dato quantitativo numerico sono guai grossi per il sistema monetario gestito dal nostro paese. Il fatto che attraverso questa contestuale emanazione di comunicati si diffondesse l'idea che la Banca d'Italia stesse perdendo colpi sotto il profilo della capacità di gestire le informazioni corrispondenti all'esercizio delle proprie attribuzioni istituzionali poteva diventare un fatto gravissimo.

In realtà era un *bluff*, il sistema principale della Banca d'Italia non era stato aggredito, il *computer* accessorio violato conteneva informazioni di carattere scientifico, scambi con altri enti di studio all'estero eccetera, per cui veramente grossi pericoli non ve ne sono stati. Ma sommando la simultaneità dei messaggi, la diffusione contestuale attraverso i sistemi informatici, vi è stato un rimbalzo da quel sistema informatico ad altri e ciò ha fatto sì che per qualche ora si è corso il rischio che si diffondessero notizie atte a produrre terrore in uno specifico settore che appunto si supponeva aggredito.

Su questo voglio riferire un altro dato di indagine, piuttosto che un risultato. Nel corso del 1995 si è parlato poco di Falange armata; sui giornali non si è parlato di numerosi comunicati e credo che l'opinione pubblica abbia potuto percepire una sorta di fenomeno discendente, di affievolimento. In realtà i comunicati ci sono stati, ben centocinquanta da gennaio fino ad oggi. Poi potremo fare una panoramica di questi comunicati, se questo interessa al Presidente. Alcuni sono significativi, alcuni con una idea, con un contenuto, con espressioni, con riferimenti o soggettivi o di strategia ad un filone che già personalmente e in altre sedi è stato individuato come portante di una consapevole linea strategica. Credo che siano emersi sulla stampa solo un paio di comunicati. Oggi si è parlato forse di quello che riguardava l'onorevole Berlusconi, qualche mese fa si è parlato di quello che riguardava il ministro Mancuso. In realtà quello che è accaduto non è casuale. Vi sono state direttive da parte del mio ufficio raccolte ed attuate da parte degli organi di polizia giudiziaria per evitare che questi comunicati della Falange armata avessero diffusione nei *mass media*, per evitare cioè l'effetto perseguito di volta in volta. Veniva individuato il ricevente, veniva diffidato dal comunicare ad altri il contenuto delle informazioni che stava dando in sede di indagine: ovviamente veniva informato il destinatario della minaccia per quanto il suo interesse e per quanto di competenza degli organi di sicurezza.

Vi è da dire – può testimoniare il dottor Pansa – che nonostante la mancanza di sicura attribuibilità di eventi violenti alla Falange armata,

l'effetto che il comunicato produce sull'individuo raggiunto continua ad essere di terrore. È incredibile sentirlo raccontare, ma vi posso testimoniare di persone degne del massimo rispetto che mi hanno riferito di essere o di sentirsi insidiate dal messaggio verbale o dal contenuto implicito o trasversalmene caricato nel messaggio stesso.

PRESIDENTE. Qualche incosciente non dà rilievo.

SAVIOTTI. Abbiamo qui l'eroico Presidente che per la sua attività, per la sua qualità di Presidente della Commissione stragi, è stato fatto segno di un comunicato che credo possa essere di interesse della Commissione e che mi sembra doveroso rappresentare in questa sede: «Sono il colonnello Gino, numero di codice...» - e segue un numero di codice effettivamente riportabile ad un filone di comunicati della Falange armata - «Qualcuno sta sottovalutando in maniera tragica le comunicazioni della Falange armata. Cercate di capire: il senatore Pellegrino della Commissione stragi sta compiendo una serie di errori che possono ripercuotersi sulla sua persona e sulla sua famiglia». Il comunicato è del 27 maggio 1995.

Tornando agli episodi del 29 e del 30 settembre, non siamo in grado di sciogliere in questa fase il dubbio se si tratta di un gruppo di ragazzi particolarmente bravi, di *hackers* che si divertono emulando o scimmiottando la Falange armata o se chi finora ha gestito con determinati comunicati e interventi quella sigla abbia pensato e abbia avuto l'opportunità di rivolgersi a questo strumento nuovo per la diffusione delle informazioni per la pressione sui contenuti informativi che circolano presso l'opinione pubblica.

Indubbiamente questo degli *hackers* è un terreno fertilissimo. Sono individuabili in una fascia generazionale molto ristretta, tra i venti e i venticinque anni; oltre i venticinque anni sembra che non si possa più tenere il passo con la crescita delle capacità di aggressione informatica. Scherzando alcuni esperti dicevano che a ventisei anni si viene assunti dalle ditte che costruiscono i programmi di sicurezza: quando non si può fare più l'*hacker* si retrocede e si va a sviluppare il sistema di sicurezza, come quando uno non è più bravo a fare il ladro, non è più veloce a correre, comincia a fare il poliziotto. Una pregnanza così caratteristica e precisa non c'è in altri settori, perchè per definizione chi fa programmi di sicurezza è meno all'avanguardia di chi i programmi di sicurezza si diverte ad assalirli, a violarli, a superarli. Se pensiamo alle possibilità di sabotaggio, di manipolazione delle informazioni, alla possibilità di inserirsi in un sistema informativo molto più rapido della carta stampata, immediato, difficile da controllare e contenere e gestire sotto il profilo della legittimità, vediamo come agevolmente interventi di intossicazione della vita politica possano essere raggiunti attraverso questo strumento.

PRESIDENTE. Secondo la vostra riflessione resta confermato che il tentativo della minaccia è quello di influenzare l'attività di attori istituzionali, comunque di influenzarli?

SAVIOTTI. Attraverso questa vicenda specifica del 29 e 30 settembre non possiamo indurre nessun obiettivo.

PRESIDENTE. È stata una prova di potenza?

SAVIOTTI. Sì, mi sono trovato di fronte al rischio di un effetto massimo di diffusione dell'intervento stesso.

Volevo richiamare l'attenzione su un comunicato della Falange armata del marzo 1995; credo che anche questo non abbia avuto diffusione.

Sarete meglio di me in grado di collocare il comunicato di cui parlo nel contesto della situazione politica e delle informazioni che circolavano in quel momento. Il codice di identificazione è lo stesso citato nel comunicato che riguarda il presidente Pellegrino.

1. «Quando il 1° dicembre 1994 affermammo che il 1995 sarà un anno in cui o per via politica, o per via istituzionale o per via militare si riscriverà la nuova storia d'Italia, questo deve essere ritenuto realistico».

2. «Sabato 17 settembre 1994 rilasciammo un comunicato nel quale si affermava che la vita e la vicenda umana e politica di Antonio Di Pietro sarebbe stata molto breve».

È vero, c'era stato un comunicato il 17 settembre 1994.

«Non ha voluto seriamente ascoltarci e adesso deve considerare che la sua stessa vita è in costante e tendente pericolo».

3. «Falange armata non dimentica Oscar Luigi Scalfaro: come abbiamo più volte annunciato, deve essere e sarà certamente spazzato via, con le buone o con le cattive».

4. «Dopo l'operazione del 18 agosto 1991 a Bellaria contro i tre senegalesi il gruppo di fuoco falangista che quell'azione era stato chiamato ad eseguire venne messo subito in disarmo per manifesta imprudenza e inadempienza agli ordini ricevuti. Ecco perchè i fratelli Savi sono solo davvero dei poveri, utili idioti che con quella e altre azioni rivendicate dalla Falange non hanno nulla a che vedere».

5. «I giudici D'Ambrosio di Milano e Salvini hanno cosparso l'Italia già di fin troppe boriose menzogne e falsità per non essere ormai da noi considerati come dei semplici cadaveri ambulanti».

Direi che questo è uno dei comunicati caratterizzato da una confusa complessità strategica. Richiamo l'attenzione di tutti – se si può a questa dare un significato – alla collocazione nel tempo del comunicato e dei riferimenti che esso contiene. Lo sforzo del mio ufficio e degli uffici di polizia giudiziaria che con me si sono affaticati in queste indagini non è rivolto solo all'indagine. Concrete possibilità di sviluppo su quest'ultimo episodio le abbiamo individuate. Non siamo però in grado di dare una lettura specifica, nel senso di orientare la soluzione finale verso ipotesi di ragazzacci molto bravi o di qualcuno che di ragazzacci molto bravi si sia impossessato o che abbia gestito o fatto gestire. Linee investigative che ci possono consentire di avvicinarci a dei possibili tramiti di queste attività informatiche li abbiamo individuati, però sono ancora scottato dall'esperienza investigatimante vissuta con l'arresto di Scalone Carmelo. Ne abbiamo parlato di questo e credo che la Commissione sia informata. Scalone Carmelo è sicuramente l'autore di comuni-

cati di particolare rilievo strategico che riguardavano il Presidente della Repubblica, la figlia Marianna e che preannunciavano situazioni ed eventi che, con una certa chiave di lettura, si sarebbero poi verificati. Scalone Carmelo aveva una soluzione a portata di mano, immediata: confessarsi colpevole e proclamare che la sua attività era dovuta esclusivamente ad un intento autocelebrativo, di autocommiserazione rispetto all'amministrazione pubblica o a chi doveva dargli riconoscimenti, scorte o comunque collegare questa sua attività ad un momento di delirio.

PRESIDENTE. Chiariamo alla Commissione che Scalone Carmelo era un operatore carcerario.

SAVIOTTI. Un operatore carcerario che ricorreva spessissimo nella prima fascia di comunicati: era uno dei quattro operatori carcerari che risultavano più minacciati.

In realtà Scalone Carmelo ha optato per la linea difensiva, e questo lo posso dire senza violare alcun segreto. Dal mio punto di vista ha optato per la linea difensiva più difficile da sostenere, quella secondo cui quelle telefonate non le avrebbe fatte lui; evidentemente qualcuno avrebbe avuto interesse a far risultare sul suo telefono quelle telefonate, quasi quasi accreditando l'ipotesi di un progetto clandestino o comunque con reconditi significati dietro l'attribuzione di questa attività di comunicati allo stesso Scalone Carmelo. Ripeto, con una confessione e con un'ammissione di stato di delirio se la sarebbe cavata con un reato che neanche gli avrebbe impedito di continuare a lavorare per l'amministrazione pubblica, forse con una semplice contravvenzione. Egli non avrebbe certamente sofferto sei mesi di carcerazione, durante i quali peraltro i comunicati sono continuati e non avrebbe potuto affrontare – così come dovrà fare – un processo con gravi ipotesi delittuose. Scalone Carmelo è rimasto sotto il profilo investigativo per me una sconfitta, anche se mi ha consentito di arricchire l'analisi di alcuni elementi: le sue dichiarazioni sono state assai valide e sono attualmente all'esame di un professore abbastanza noto che darà sotto questo profilo il suo contributo, che potrà confermare – in questo senso si stanno attestando i primi risultati – l'esito delle analisi foniche. Sono stati individuati gruppi di parlatori e sono state attribuite a Scalone oltre alle telefonate della sua utenza anche un'altra ventina di telefonate di contenuto omogeneo con le altre in cui magari compare lo stesso numero di codice e lo stesso contenuto intrinseco ma sicuramente attribuite a parlatori diversi. Così come altre telefonate ancora che ricorrono nel periodo di carcerazione dello Scalone e nel periodo successivo, quando, scarcerato, è stato sottoposto per quanto possibile ad una vigilanza sul territorio per verificare se fosse nuovamente all'opera con questa attività telefonica.

Posso fare una panoramica di questi comunicati che non hanno avuto diffusione, una rapida panoramica. Nel gennaio 1995, prima decade, generiche telefonate a scopo allarmistico a nome Falange armata che segnalano la presenza di ordigni esplosivi in varie parti del paese. In questo periodo entra in gioco un effetto emulativo che amplifica gli effetti intossicanti dell'attività della Falange generale. Il 10 gennaio viene

minacciato Giuseppe Marra, direttore dell'agenzia Adn-Kronos, che era stata oggetto di una intrusione nel dicembre precedente. Questa è l'agenzia di stampa che, se non ricordo male, per prima diffuse una delle quattro copie del progetto Amato sulle privatizzazioni. L'Adn-Kronos viene nuovamente citata in questi comunicati dell'aggressione informatica del 1995. L'Adn-Kronos in alcuni comunicati della Falange armata viene definita agenzia insubordinata e scorretta. Il 10 gennaio viene minacciato Giuseppe Marra con un comunicato che fa esplicito riferimento ad una personale amicizia dello stesso con un senatore della Repubblica. Sembra che il riferimento è alla visita del presidente Cossiga avvenuta all'agenzia proprio in quei giorni. Nello stesso periodo una sequenza di telefonate a nome Falange armata preannuncia attentati, non verificatisi, e attacca espressamente l'ipotesi di governo Dini.

Il successivo 20 gennaio vengono minacciati Luciano Violante, il procuratore capo della Repubblica di Firenze Vigna al quale, in particolare, viene detto che ha passato il segno e che nessuno potrà impedire la sua esecuzione.

Devo dire che nel corso del 1995, poi, viene individuata una serie di comunicati, per lo più manoscritti che giungono per posta. A Milano e a Firenze vengono individuati due mitomani, uno dei quali con una approssimativa ideologia nazista, anche per i modi di scrittura idonei a richiamare quell'ambito pseudo culturale e pseudo ideologico, mentre l'altro insiste su Firenze e sulle Forze di polizia e i cittadini di quella città. Sono due soggetti, individuati e denunciati alla rispettiva autorità giudiziaria di competenza, responsabili di questi comunicati che vengono manoscritti.

Il 28 gennaio viene attaccata, con un comunicato all'Adn-Kronos, la figura del Presidente della Repubblica, che viene definito bugiardo, e l'interlocutore utilizza nuovamente l'espressione «colpire in ciò che ha di più caro e sacro», riferendosi evidentemente alla figlia Marianna, con l'utilizzazione del numero di codice usato a suo tempo da Carmelo Scalone.

Il 28 febbraio, esattamente ad un mese di distanza dal precedente comunicato, c'è un nuovo comunicato all'agenzia Adn-Kronos di Milano in cui si torna a minacciare il presidente Scalfaro che ugualmente viene definito bugiardo e irresponsabile sacrestano. Contestualmente si fa nuovamente riferimento alla figlia Marianna.

All'inizio del mese di marzo 1995 minacce al prefetto di Palermo, dottor Serra e all'onorevole Marianna Li Calzi, sottosegretario al Ministero dell'interno, definita serva del potere.

Il 5 marzo minacce al comunista Santoro; il 14 marzo viene minacciato un attentato in danno dell'onorevole Berlusconi; il 27 maggio, come abbiamo già detto, viene minacciato il senatore Pellegrino. Nella stessa data minacce vengono rivolte all'Adn-Kronos, presso la redazione romana, accusata dall'anonimo interlocutore di essere insubordinata e scorretta.

A marzo, lo ricordo perchè in questo caso mi sembra necessario, veniva depositata la sentenza relativa al primo troncone dell'indagine condotta dal giudice istruttore Guido Salvini sui fatti eversivi degli anni 1960-1970. Il 12 aprile, presso la redazione di Perugia dell'Ansa giunge una telefonata in cui viene minacciato il giudice Salvini, con numero di

codice ricorrente. Telefonata alla redazione di Udine de «Il Gazzettino»: «Il giudice Salvini non annulla la nostra volontà di riportare ordine nel paese contro i mistificatori di regime quali Prodi. I giudici Salvini e D'Ambrosio non devono avere il tempo per portare avanti le loro menzogne». Poi, il comunicato che ho poc'anzi richiamato, quello che ho definito di una certa complessità strategica.

Inoltre, nel mese di maggio 1995, un comunicato estremamente scarno all'Ansa di Genova, senza sigla Falange armata ma con espressioni ricorrenti e facilmente rintracciabili nei precedenti comunicati, in cui si afferma che Di Pietro non ha nulla da temere. Contestualmente viene formulata una minaccia all'indirizzo del dottor Mancuso a Bologna.

Il 17 giugno l'Ansa di Genova riceve una stringata comunicazione relativa al dottor Saverio Borrelli nel corso della quale vengono indicate, riguardo al magistrato, una opzione politica in alternativa ad una opzione militare. Di nuovo il 23 giugno si ipotizza l'alternativa tra una strada militare ed una politica. Il 27 giugno si dice che: «è troppo lunga e fin troppo coperta la soluzione politica adottata per Saverio Borrelli, per cui opteremo per quella militare».

Per due volte l'8 e il 9 luglio la Falange armata lascia sulla segreteria di una trasmissione radiofonica minacce contro l'onorevole Berlusconi. Il 21 luglio viene minacciato Maurizio Torrealta, giornalista di Rai 3, poi di nuovo l'onorevole Carlo Ripa di Meana.

Il 1° settembre 1995 all'Ansa di Genova nuovamente minacce contro Antonio Di Pietro. Il 13 settembre minacce contro Violante, Arlacchi e D'Alema. Si arriva poi al 29 e 30 settembre ove più telefonate rivendicano appunto le intrusioni telematiche.

Il 9 ottobre - è un fatto recente - giunge una telefonata all'Ansa: una persona si qualifica come l'onorevole Tajani e riferisce di aver ricevuto un messaggio, presso la sede di Forza Italia, contenente minacce all'onorevole Berlusconi. Per accreditare la sua presentazione come onorevole Tajani fornisce un numero di telefono cellulare che effettivamente corrisponde a quello dell'onorevole Tajani che, interpellato sul punto, nega assolutamente di avere ricevuto e comunicato all'Ansa quanto sopra.

Credo che l'opera di contenimento e di insonorizzazione di questa attività che proprio si rivolge sul piano dell'informazione sia indispensabile ma certamente insufficiente. L'adozione di misure tampone certamente non consente di fare processi o di individuare responsabilità processuali. Quindi le indagini sotto questo aspetto continuano e dovrebbero continuare con un'attenzione non altalenante, bensì ben più pressante sul fenomeno con l'uso di tutti gli accorgimenti e i mezzi tecnici che possano da un lato scoraggiare e, dall'altro, effettivamente giungere all'individuazione di autori materiali di singoli interventi, di comunicazioni, di provenienze.

LA VOLPE. Al di là delle minacce, ci sono state delle rivendicazioni?

SAVIOTTI. Non abbiamo mai scoperto chi sono, oltre a Scalone Carmelo, un telefonista. Non sapendo chi sono, non sappiamo che cosa

fanno. Dire non ha mai fatto nulla può voler dire solamente che le rivendicazioni effettuate dalla Falange armata non hanno crismi di autenticità. Tra l'altro è caratteristica anche la mancanza di un qualsiasi sforzo (che pure altri fanno, quando hanno rivolto rivendicazioni non autentiche) di accreditarsi come autentici, salvo quattro occasioni in cui c'è riferimento ad un tipo di proiettile, ad un tipo di esplosivo, ma è cosa estremamente rara rispetto al grande numero di comunicati di rivendicazione. Non c'è neanche un tentativo di autoaccreditarsi come responsabili dell'attentato che si andava rivendicando o minacciando.

PRESIDENTE. Anzi, addirittura per la Uno bianca hanno prima rivendicato e poi smentito la rivendicazione dopo che i Savi sono stati scoperti.

LA VOLPE. Nel primo caso si tratta di una organizzazione che lancia messaggi terroristici e che non ha mai fatto nulla.

PRESIDENTE. In questo starebbe il carattere nuovo ed informatico di questo tipo di operazioni.

STANZANI GHEDINI. Per il momento solo telefoniche.

PRESIDENTE. Sì, si introducono nel sistema per creare allarme o per condizionare i destinatari delle minacce. Credo che sia questo il tipo di lettura.

SAVIOTTI. Vorrei rappresentare un'idea (che è un po' più che un'idea): se domani il dottor Pansa intraprende una delicatissima operazione di polizia giudiziaria e oggi arriva un comunicato della Falange armata che dice «uccideremo il dottor Pansa», se pure egli non sarà ucciso, il collegamento fra quello che sta per fare o che ha fatto e il segnale che tempestivamente arriva sul suo conto è inevitabile.

STANZANI GHEDINI. Direi che l'obiettivo presumibile siete voi, cioè provocare una dispersione di energie e di attenzioni di chi in fondo è tenuto a tentare di arrivare ad un risultato. Anche questo è un obiettivo.

PANSA. Sicuramente è un effetto.

SAVIOTTI. Francamente e umilmente per il paese spero che io stia perdendo tempo, che mi stiano facendo perdere del tempo.

STANZANI GHEDINI. È una dispersione di energie, è difficile tentare di capire, almeno da quello che è emerso, perchè si tratta anche di messaggi contraddittori. Prima si dice che Di Pietro non ha nulla da temere e poi lo si minaccia.

BRIGANDÌ. Desidero rivolgere una domanda semplicissima. Ho seguito con estrema attenzione le due relazioni e vi è certamente una situazione non chiara. A suo parere, dottor Saviotti, in cosa può sfociare

questa situazione non chiara? Vi sono reali possibilità che lei non stia semplicemente perdendo tempo?

SAVIOTTI. Spero proprio di sì. Se con l'ausilio delle forze di polizia e delle indagini nelle quali siamo impegnati potessi giungere alla conclusione e dire con certezza che tutti i comunicati sono addebitabili a buontemponi o scriteriati, comunque credo che avrei reso un servizio ed avrei onorato il compito investigativo. Comunque vorrei essere sicuro di poterlo dire.

PANSA. Probabilmente il senatore Brigandì si chiede se è pericolosa o no questa Falange armata. Questa è la domanda.

SAVIOTTI. Io vedo sintomi di pericolosità fortissima in queste iniziative recenti, per cui sarebbe quanto mai urgente stabilire se si tratta di ragazzi buontemponi che scimmiottano la sigla Falange armata o no. Su questo piano, la potenzialità del danno concreto, quello che a voi interessa quantificare, è il problema. Vi è un danno sul piano dell'informazione, del discredito, dell'immagine, della minaccia che trasversalmente può riguardare un personaggio, indipendentemente dal contenuto del messaggio: questo è un piano di danno in ordine al quale non posso esprimere certezze ma di cui non ho semplicemente un sentore astratto. È un danno che mi è stato rappresentato da questo o da quel soggetto pubblico investiti di responsabilità istituzionali che hanno intravveduto valenze ulteriori rispetto al messaggio in ordine alla loro situazione personale o istituzionale.

BRIGANDÌ. Quindi siamo in una situazione di pericolo.

SAVIOTTI. Di preoccupazione.

DE PAOLI. Lei, dottor Saviotti, ha parlato - e vorrei averne conferma - del comunicato della Duchessa.

SAVIOTTI. Era una battuta.

DE PAOLI. Comunque lei ha richiamato i falsi comunicati delle Brigate rosse fatti al Ministero dell'interno.

SAVIOTTI. Il fatto è che anche se fossero comunicati veri, oggi li farebbero attraverso *Internet*.

DE PAOLI. Oggi non esistono più le Brigate rosse, però sappiamo perfettamente, anche a seguito dei lavori compiuti dalla Commissione, per quello che è risultato in questi dieci anni, come le Brigate rosse siano state utilizzate da parte dei Servizi segreti.

PRESIDENTE. Il dottor Saviotti ha fatto riferimento al falso comunicato della Duchessa che certamente non proveniva dalle Brigate rosse.

DE PAOLI. Esattamente quello che ho detto io, è stato fatto al Ministero dell'interno. Vorrei sapere se in questo paese molto bello architettonicamente ma con degli apparati di sicurezza che agiscono contro quello che invece dovrebbero difendere... Anche il comunicato che riguarda il Presidente della Repubblica è fatto non certo da un ragazzotto anarchico che per sbaglio è riuscito ad entrare in un sistema; chiaramente è gente che lavora all'interno dello Stato, che ha determinate informazioni e che le fa sapere. Può esistere ancora, a livello di Falange armata, qualcosa all'interno dei corpi deviati dello Stato?

SAVIOTTI. Il sentore non l'ho avuto io, lo ha avuto e lo ha manifestato l'ambasciatore Fulci. Veramente il termine appropriato è «sentore» tant'è che nelle sue dichiarazioni, più volte compulsate dal mio ufficio e da altri inquirenti, non ha mai dato la sensazione di poter agganciare a qualche episodio concreto, a qualche indizio che orienti soggettivamente le responsabilità quello che oggi appunto chiamiamo sentore. Tuttavia era un sentore che proveniva da un ambasciatore dello Stato al quale è stata riconfermata la fiducia da più Governi successivamente, che ci rappresenta oggi credo ancora – all'Onu e che forse ci rappresenterà nel Consiglio di sicurezza. Quindi è un sentore qualificato. Ripeto come ho già detto nell'ultima occasione: un sentore è un sentore e non consente neppure l'iscrizione nel registro degli indagati. Nella precedente occasione confermai questa circostanza: i soggetti indicati dall'ambasciatore Fulci non sono stati mai iscritti nel registro degli indagati.

LA VOLPE. Lei perchè non li ha iscritti?

SAVIOTTI. Io e il mio ufficio – ma credo che in genere questo dovrebbe essere l'orientamento e credo che in effetti lo sia dovunque – riteniamo che l'iscrizione nel registro degli indagati non possa avvenire sulla base di sentori. La notizia di reato non comporta prove di per sè ma è sicuramente qualcosa di più di un sentore, di una preoccupazione, di una deduzione.

PRESIDENTE. Mi scuso con il senatore De Paoli per averlo interrotto: non avevo capito il senso della sua domanda.

ZANI. Volevo sapere se nel caso del comunicato alla Adn-Kronos e in quest'ultimo caso, quello del 29 e 30 settembre (sono le cose più significative e potenzialmente più pericolose) è stato indicato il numero di codice, di identificazione oppure no.

Seconda questione: i codici sono più di uno?

Terza questione: avete condotto uno studio sulle sedi, i luoghi da dove spesso vengono inviati i messaggi?

SAVIOTTI. Cominciamo dall'ultima domanda. L'Ucigos, attraverso il raccordo con tutto il bagaglio informativo dei carabinieri, dei Ros e

delle Digos interessate, ha realizzato una base dati amplissima contenente tutte le informazioni possibili di carattere storico, di cronaca sui comunicati della Falange, gli orari, il loro ruolo. Ovviamente i comunicati di maggiore interesse raggiungono l'Ansa, l'Adn-Kronos se non addirittura le redazioni di alcuni giornali, con ricorrenza delle sedi di Roma, Milano, Bologna e Genova. Queste sono le sedi maggiormente interessate dai comunicati, che ripeto arrivano ad Ansa, Adn-Kronos e talvolta alle redazioni di giornali come «la Repubblica» ed altri. In questo contesto è stata realizzata una raccolta e una individuazione dei numeri di codice, che sono diversi. Due o tre codici sono quelli di maggiore interesse e sono ricorrenti nel filone di comunicati che abbiamo individuato come unitario o come strategicamente riconducibile ad un'unica linea. In queste ultime rivendicazioni e negli stessi attacchi informatici non sono stati inseriti i numeri di codice. In uno dei comunicati che ha interloquito sulla vicenda abbiamo un riferimento testuale che consideriamo significativo per riagganciare questo comunicato ad altri precedenti.

GUALTERI. Desidero parlare della questione dell'accreditamento attraverso il codice. Inizialmente c'è un comunicato in cui la Falange indica i codici per essere creduta oppure questa individuazione della ricorrenza di alcuni codici avviene con l'analisi dei comunicati?

Inoltre, quanti sono stati i comunicati scartati che, non avendo un numero di codice o non essendo stati da voi individuati, rappresentano la massa di scarto della mania telefonica. Non credo che non ci siano stati altri che hanno dichiarato di essere la Falange armata. Vorrei sapere qual è la differenza tra i comunicati che voi tendete ad accreditare attraverso il numero di codice e quelli non accreditati numericamente e esattamente di che percentuale si tratta.

SAVIOTTI. Una percentuale non è stata fatta, cercheremo di farla; comunque il rapporto tra comunicati di interesse e quelli di ordine sparso (c'è un approccio molto prudente nell'attribuzione di significatività) è approssimativamente di due a dieci. Pertanto un quinto dei comunicati può interessare il contenuto per una ipotesi di continuità.

Per quanto riguarda i numeri di codice, nessun comunicato preannuncia il numero di codice. Nel contesto di un comunicato qualsiasi, che rivolge minacce o ha un determinato obiettivo, la dizione Falange armata è caratterizzata dalla scansione del numero di codice, normalmente a sei cifre, che corrisponde magari a quelli precedenti o che ritroveremo nei comunicati successivi. In questo contesto abbiamo trovato due numeri di codice, uno che inizia con Scalone e che continua fino al 1995.

GUALTIERI. Sono tra coloro che considera preoccupante il fatto che da molto tempo la Falange armata prosegua con questi comunicati. Se si considera da quanti anni dura, cioè da cinque o sei anni, si rileva una persistenza molto grave. Inoltre con le intercettazioni non si è mai riusciti, se non nel caso di Scalone, ad individuarli, ad andare oltre con le indagini. Questo dimostra che quando ci domandiamo perchè lo fanno, nel lungo periodo ci si accorge del perchè lo fanno. Essi hanno

un obiettivo ben preciso. Non dico che coloro che ricevono la minaccia entrano tutti nel terrore, ma alcuni sì. La persona che ha indicato prima il giudice è talmente terrorizzata che non viene in Italia o per farlo deve essere protetta dai blindati. In alcune persone nasce questo problema, per cui la persistenza del fenomeno ha un suo significato. Non è l'evento occasionale o l'opera di persone cattive che vogliono divertirsi: è un problema che crea effettivamente preoccupazione, che rientra in quelle attività di destabilizzazione del nostro sistema. Adesso la preoccupazione aumenta con l'avvio del terrorismo informatico, perchè questa attività è diventata molto più grave. Ritengo che questo fenomeno debba essere valutato con grande attenzione, dal momento che non si tratta di cosa di poco conto.

Negli Stati Uniti e in Inghilterra sapete che ci sono due grandi sistemi di protezione; hanno creato due grandi enti di protezione delle comunicazioni: in America l'Nsa, in Inghilterra il Gran Quartiere delle comunicazioni che hanno strutture cinque volte più grandi della Cia per numero e per potenza finanziaria. Noi abbiamo un sistema di protezione delle comunicazioni che diventi la vera difesa di uno Stato moderno?

PANSA. Per quanto concerne la struttura investigativa nei confronti dei crimini informatici direi che esiste già una distinzione di compiti.

GUALTIERI. Ho dimenticato di dire che il sistema bancario ha creato una sua struttura di tutela generale del sistema bancario italiano: se non sbaglio, c'è un servizio centralizzato di sicurezza del sistema bancario.

PANSA. Si tratta di *Security Net*, è una rete telematica di informazioni di cui facciamo parte anche noi come ufficio.

Probabilmente bisogna distinguere più di un piano. Lei, per esempio, parla dell'Nsa che è un centro di ascolto e di protezione delle comunicazioni anche nei contenuti, non soltanto negli strumenti. È un'agenzia particolare degli Stati Uniti che, da quanto è a mia conoscenza, fino a pochi anni fa non veniva neanche nominata e se agenti federali ne parlavano venivano licenziati.

Per quanto concerne la struttura investigativa c'è stata una distribuzione dei compiti. Nel marzo del 1991 il Consiglio generale di sicurezza decise di affidare il compito alla Polizia di Stato, mentre altri compiti vennero affidati all'Arma dei carabinieri e alla Guardia di finanza.

Già dal 1989 da parte della Polizia di Stato era stato affrontato il problema nei seguenti termini: innanzi tutto, si è costituita una struttura investigativa centrale e cioè la sezione criminalità informatica del Servizio centrale operativo; poi il fenomeno si è diffuso e sono state create delle antenne sul territorio attraverso i quattordici centri interprovinciali con personale specializzato. Poichè noi non possiamo specializzare una quantità enorme di persone in questo settore, la materia criminalità informatica è stata introdotta nei corsi di formazione per funzionari e ispettori, cioè a tutti gli investigatori della Polizia di Stato. Quindi, dal punto di vista investigativo, allo stato

l'approccio è in questi termini: cultura di base nei corsi di formazione, strutture specializzate centralizzate con antenne sul territorio.

Devo poi riferire di un'intervista rilasciata dal Capo della Polizia su «Polizia moderna» alcuni mesi fa, e cioè che vi è l'idea di riconvertire una struttura della Polizia di Stato nella difesa delle comunicazioni in generale, adeguandosi anche con una modificazione normativa. Noi abbiamo già la Polizia postale che difende e tutela la corrispondenza: è nata per tutelare la corrispondenza epistolare, ma oggi, *ope legis*, corrispondenza è considerata anche quella telematica, le telecomunicazioni, per cui l'idea è quella di trasformare questa struttura della Polizia postale in una Polizia delle telecomunicazioni. Si tratta di un'intervista del Capo della Polizia, per cui più di questo non sono in grado di dire: non so se sia un progetto avviato, a mio avviso è molto intelligente e interessante, sia perchè non crea nuove strutture (secondo me già sono troppe), sia perchè non crea strutture che si ripetono nei vari Corpi di polizia, ma opera una distribuzione dei compiti che dovrebbe essere secondo me la strada da perseguire anche in altri settori, una scelta fondamentale.

Per quanto riguarda il concetto generale di sicurezza delle comunicazioni, esiste presso la Presidenza del Consiglio una struttura che fa capo al Sismi, per il controllo della sicurezza, che stabilisce cioè i canoni e i limiti dei sistemi di sicurezza, ma non abbiamo un'agenzia, una struttura che faccia, allo stato, controllo delle comunicazioni se non nei limiti delle comunicazioni di proprio interesse che ogni struttura può fare; non esiste un'agenzia che svolga un controllo sulle comunicazioni. Non abbiamo neanche un sistema per stabilire gli *standard* medi di sicurezza che devono avere le forme di comunicazione. Noi imponiamo ai giornalisti e ai direttori di giornali l'obbligo della registrazione, mentre abbiamo i giornali telematici di cui vi sono milioni e milioni di copie, ma per essi non c'è l'obbligo della registrazione. C'è una certa anarchia nelle norme, quindi quella del controllore è un'ipotesi azzardatissima. I Bbs sono dei giornali telematici: non capisco perchè un giornale di carta, di cui si possono diffondere 500-600.000 copie deve avere tutta una serie di obblighi di registrazione e di identificazione, mentre un Bbs a cui si accede e automaticamente moltiplica le copie fino ad arrivare a milioni, è libero da qualsiasi forma di controllo preventivo.

LA VOLPE. *Internet* sta sconvolgendo tutte le regole perchè questo potrebbe valere per l'Italia, ma per le cose che pubblico all'estero? *Internet* sta scardinando il diritto d'autore e, in questo modo, anche tutto il sistema.

PANSA. Il problema è anche delle comunicazioni. Noi abbiamo una forma di riconoscimento della stampa estera ed ho fatto un esempio, quello di un BBS, ma ce ne sono anche altri. C'è quindi libertà nelle comunicazioni. Ho detto che si tratta di un principio di alta democrazia: *Internet* significa rendere a bassissimo costo accessibile l'informatica e i contenuti delle banche dati a tutti. Se si ha una struttura da un milione, si può parlare con il mondo, e questo avviene sia abitando vicino alla biblioteca nazionale, sia sul cocuzzolo di una montagna nella parte più sperduta d'Italia.

SAVIOTTI. Se un Bbs gestisce il messaggio di Saviotti a Pansa è giusto che nessuno controlli questo messaggio; però in un Bbs ci può essere anche la situazione per cui io apro uno spazio e chiunque vuole ci appoggia eventuali informazioni, notizie, segreti, diffamazioni, minacce e così via. Confondere la tutela della segretezza della *prima forma di corrispondenza con* la tutela della *segretezza della seconda* forma è quanto di più equivoco e pericoloso ci possa essere. Se io espongo una ventina di informazioni ci deve essere una figura, a mio modesto avviso, assimilabile al direttore responsabile dei giornali che, se nei suoi annunci pubblica minacce deve garantire quanto meno l'informazione sulla provenienza. La tutela dell'anonimato presso un Bbs arriva al punto che chi mette in mostra presso quella vetrina ha garantita la tutela dell'anonimato del messaggio che ha inviato. Questa è una scelta *ovviamente politica, di democrazia e di cultura*, però è gravida di conseguenze e forse una maggiore consapevolezza nel momento in cui si lotta per normare questo settore o per *non farlo sicuramente* è necessaria.

LA VOLPE. Questo non è stato fatto in nessun paese: come è possibile?

PRESIDENTE. Stiamo segnalando un'arretratezza generale.

LA VOLPE. La nuova tecnologia non lo consente, nessun paese ci riesce.

SAVIOTTI. Però negli Stati Uniti istituiscono ed hanno delle risorse e mezzi per cui in chiave magari solo repressiva delle intercettazioni telematiche in tempo reale a inseguimento riescono a realizzarle.

PRESIDENTE. Se io pubblico una notizia diffamatrice nei tuoi confronti, tu hai una serie di mezzi possibili di tutela.

Se invece questa notizia diffamatrice è diffusa per via telematica, non vi sono mezzi di tutela. È chiaro che si tratta di una discrasia alla quale occorrerà porre rimedio.

SAVIOTTI. Questo sul piano della telematica. Sul piano dei sistemi informatici e della sicurezza volevo segnalare che mentre nel caso di un'automobile se la casa costruttrice installa un *air bag* vi è una istituzione pubblica che lo omologa, verifica se è *sufficientemente sicuro e ne* fa conoscere all'utente le caratteristiche, per il *software* questo non è possibile: è sul mercato più libero e l'utente non sa che livello di sicurezza ha, da chi è stato abilitato, che barriere ci sono, quante volte è stato violato. Non c'è alcuna competenza ordinamentale rivolta alla tutela intrinseca della banca dati.

PRESIDENTE. Questa è la storia del mondo. Nascono sempre prima i fenomeni e poi le regole dei fenomeni. Più i fenomeni sono nuovi, più c'è questa sensazione di arretratezza, di incontrollabilità. Il

problema è adeguare i sistemi normativi alle realtà nuove. Finora ci siamo abbastanza riusciti.

PANSA. Esiste questo concetto. La legge n. 517, che disciplina i crimini informatici, prevede che l'accesso abusivo è sanzionato se il sistema è protetto da misure di sicurezza. Non specifica la misura della protezione, per cui l'interpretazione della norma è vaga. Il disegno di legge sulla *privacy* prevede *standard* per la gestione delle banche dati che raccolgono informazioni sui cittadini. Uno degli obblighi previsti è che gli *standard* siano rispettati: è previsto anche che un gruppo di tecnici rediga l'elenco di questi *standard* e che provveda al suo aggiornamento attraverso decreto ministeriale ogni due anni.

MAGRONE. Vorrei collegarmi a quella espressione, che non condivido, cioè all'ipotesi che il giudice Saviotti stia perdendo tempo. Premetto che non la condivido, dico invece che questa indagine e questa attenzione non solo deve continuare ma deve anche intensificarsi. Perchè dico questo? Perchè sono colpito, dal mio punto di vista, da quella parte della sua relazione nella quale mette in evidenza come alcune cose si sanno mentre altre non si sanno, alcuni messaggi sono noti altri non lo sono. Tant'è che il Presidente giustamente ha imposto la segretazione di alcuni passaggi della sua esposizione.

Mi chiedo perchè di alcuni messaggi si sa mentre di altri non si sa, quale è la causa storica - non la ragione metafisica - per cui è accaduto che alcuni sappiano e altri non sappiano di questi messaggi?

In secondo luogo mi ha colpito - fra i messaggi di cui si sapeva e quelli di cui abbiamo saputo ora - l'elenco dei destinatari, per usare una parola brutale l'oggetto dell'attenzione. In particolare la loro disomogeneità, un campionario di persone di altissimo livello comunque (quasi tutti credo) però disomogeneo quanto al significato che si può attribuire.

Come elemento di contributo per capire la logica di queste - chiamiamole così - minacce, noto che una cosa è minacciare Berlusconi, altro è minacciare Violante, una cosa è minacciare Pellegrino, altro è minacciare altre persone.

Questa disomogeneità dei destinatari delle minacce messa insieme al fatto che alcuni sanno ed altri non sanno a me dà - chiedo il loro conforto - una stranissima sensazione, cioè che un altro tipo di significato queste minacce possono averlo nella estenuazione del conflitto politico a seconda dei momenti: ora mi giova che dica questo a Tizio, ora mi giova che dica questo a Caio.

Il collega La Volpe chiedeva: «Cosa hanno fatto in concreto?». Mi voglio spiegare con un esempio. Perchè, per esempio, di Contrada si è saputo subito che era coinvolto nella vicenda della pretesa associazione mentre non si è saputo subito che era indagato per l'omicidio del giudice Borsellino. Questo meccanismo di che cosa si sa e di che cosa non si sa, il filtro, la regia di questo tipo di messaggi che vengano dall'opinione pubblica, se li applichiamo ai problemi che stiamo affrontando, emerge un'impressione - ma lo dico chiedendo conforto, mi domando se sia un'ipotesi fantastica la mia - che si tratti non di terrorismo nell'accezione sanguinaria classica tradizionale, bensì di terrorismo

nell'accezione della estenuazione del conflitto politico portata alle estreme conseguenze.

Vi è anche un'altra ipotesi, e concludo: che operazioni di questo genere siano fatte in modo che tutti si accodino e usino lo stesso sistema.

Mi permetto di sottoporre a voi queste mie valutazioni. A me preme molto sapere cosa ne pensate a proposito di questa ipotesi; un'ipotesi che non è riscontrabile soltanto qui ma anche, ad esempio, per le informazioni di garanzia: alcune si sanno ed altre non si sanno, dipende, non è un fatto meccanico e obiettivo, c'è sempre una regia molto attenta a quelle che si devono sapere e a quelle che non si devono sapere.

Chiedo dunque al giudice Saviotti quale è la lettura che il pubblico ministero, allo stato e senza pretendere conclusioni, dà circa la disomogeneità dei destinatari o dei prospettati attentati. Io ne ho tentata una: una battaglia politica che con il terrorismo sanguinario e storico potrebbe non avere connessione.

SAVIOTTI. Il mio ufficio ragiona in questi termini: c'erano notizie di reato e delle minacce rivolte a Tizio e a Caio. Sulle notizie di reato si svolgono delle indagini. Nel momento in cui apprendo la notizia di reato diffido le persone da cui vengono le informazioni e chi ha ricevuto la telefonata dal diffondere quello che diventa intrinsecamente il primo segreto dell'indagine. Questa è stata l'impostazione dell'ufficio, ovviamente particolarmente marcata con questo ulteriore fine, molto difficile da non confessare, di insonorizzare la notizia. Il pubblico ministero ha tra i suoi compiti anche quello di evitare che il reato sia portato ad ulteriori conseguenze: se le ulteriori conseguenze possono provenire dalla diffusione sui *mass media* di un comunicato, credo che sia legittimo oltre che opportuno limitare questa ulteriore conseguenza. Ho parlato di comunicati del 1995 perchè da quella data il mio ufficio ha assunto questa linea di comportamento; nel 1995 le Forze di polizia si sono attivamente mosse per attuare queste direttive. Su circa centoquaranta o centocinquanta comunicati a me risulta che ne siano sfuggiti pochissimi, soltanto due o tre, eccezion fatta per l'episodio del 29 e 30 settembre dove vi è stata una modalità di diffusione e una rivendicazione tale da sfuggire a qualsiasi tipo di controllo sul circuito informativo dell'indagine. Visto che c'è un'indagine sugli attacchi e sulle aggressioni informatiche, cerco di mantenere il segreto sull'indagine. Le modalità di rivendicazione sono state tali che è stato praticamente impossibile mantenere il segreto. I giornalisti mi telefonavano per dire che avevano saputo una certa notizia.

PRESIDENTE. In pratica è successo che la procura ha imposto sia alle agenzie sia ai destinatari delle minacce di tenere il segreto. Questo è avvenuto quasi nella totalità dei casi ma a volte questo non è avvenuto e noi ne siamo stati anche testimoni. Ad esempio il ministro Mancuso, nell'ambito di una polemica che si stava svolgendo in questa Commissione, disse che era stato minacciato dalla Falange armata e così si è saputo. Normalmente in quest'ultima fase non si è avuta notizia perchè sia le agenzie sia i destinatari delle minacce hanno ottemperato alla disposizione della procura di Roma e non

hanno reso noto il fatto che una persona era stata minacciata o di essere stata minacciata.

SAVIOTTI. Le ipotesi alternative sono tante: se sono dei buontemponi vuole dire che sto perdendo tempo. Attualmente le letture investigative sono assai aride, devono essere necessariamente prudenti. Questo aspetto induce a delle considerazioni che al momento non hanno alcuno spessore indiziario.

LA VOLPE. Quando svolgevo un'altra attività fui sollecitato a dare la notizia da parte di chi aveva ricevuto una minaccia da parte della Falange armata. Dinanzi al mio rifiuto, dicendo che forse non era il caso di amplificare la notizia, mi fu detto «Tu ti assumi questa responsabilità». E questa frase fu pronunciata da un autorevolissimo personaggio della Repubblica. C'è forse questo obiettivo nei comunicati della Falange armata: creare uno stato d'animo per cui o per ragioni pubblicitarie o per ragioni autoreferenziali o per ragioni diverse l'interessato è portato ad insistere perchè la notizia venga data, e questo è paradossale. Vorrei recare questa testimonianza per arricchire quanto affermava il collega Magrone. La domanda che desidero rivolgere è la seguente: tornando alla famosa denuncia dell'ambasciatore Fulci, se le sue denunce non costituiscano prove, non recano sufficienti elementi per poter svolgere le indagini, come è stato ascoltato l'ambasciatore Fulci, sulla base di quali elementi lui ha fatto certe affermazioni? I conti non tornano, si dice che non ci sono le prove ma se non ci sono vuol dire che la cosa è manifestamente infondata ed è inutile cercare responsabilità presso altri organi. Bisogna allora risalire a chi ha circuitato queste informazioni.

SAVIOTTI. L'ambasciatore Fulci è stato sentito più volte da me e dal mio ufficio oltre ad essere stato ascoltato in altre autorevoli sedi per comprendere alcune cose. La differenza tra le rivelazioni dell'ambasciatore Fulci che riguardavano la contabilità del Sisde e quelle che riguardavano il fenomeno Falange armata sta proprio nello spessore degli elementi che portava in un caso o nell'altro. In un caso parlava di verifiche di contabilità, di dubbi su certi circuiti finanziari, di cose verificabili; nel secondo caso ha parlato e più volte ribadito che si trattava di sue deduzioni, di valutazioni tratte sintomaticamente dalla sua conoscenza complessiva della realtà, nè da un «riferito» nè da un elemento concreto. La valutazione, per quanto autorevole, non costituisce prova, indizio, notizia e quindi neanche notizia di reato soggettivamente orientata per attenersi ad una valutazione di prudenza.

PRESIDENTE. Penso che possiamo ritenere conclusa questa audizione. Ringrazio il dottor Pansa e il dottor Saviotti per il tempo che ci hanno dedicato. In conclusione penso, con riferimento al problema generale della pirateria informatica, che si tratti di un fenomeno nuovo, molto grave al quale occorre pensare anche in sede legislativa rispetto alle misure da adottare.

Quanto alla Falange armata, troverei errato un atteggiamento di enfatizzazione ma anche pericoloso un atteggiamento di minimizzazione. Questa è gente che lavora da cinque anni con determinate finalità, de-

cisa ad assumere determinati rischi giudiziari nel momento in cui venisse individuata. Non è pensabile che è gente che faccia tutto questo per perdere o far perdere tempo. Aggiungo che, se si osservano determinate scadenze temporali con cui vengono avanzate le minacce, si può osservare che è gente ben informata e spesso sa che il destinatario si trova in una fase delicata: di qui il proposito di lanciargli un messaggio.

Dichiaro conclusa l'audizione.

La seduta termina alle ore 20,30.