COMMISSIONE PARLAMENTARE
PER L'INFANZIA

RESOCONTO STENOGRAFICO

INDAGINE CONOSCITIVA

2.

SEDUTA DI MARTEDÌ 11 DICEMBRE 2001

PRESIDENZA DEL PRESIDENTE **MARIA BURANI PROCACCINI**

COMMISSIONE PARLAMENTARE PER L'INFANZIA

RESOCONTO STENOGRAFICO

INDAGINE CONOSCITIVA

2.

SEDUTA DI MARTEDÌ 11 DICEMBRE 2001

PRESIDENZA DEL PRESIDENTE **MARIA BURANI PROCACCINI**

INDICE

La seduta comincia alle 13,40.

(La Commissione approva il processo verbale della seduta precedente).

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che, se non vi sono obiezioni, la pubblicità dei lavori della seduta sarà assicurata anche mediante l'attivazione dell'impianto audiovisivo a circuito chiuso.

(Così rimane stabilito).

Audizione del dottor Domenico Vulpiani, Dirigente superiore della polizia di Stato, Direttore del servizio della polizia postale e delle comunicazioni.

PRESIDENTE. L'ordine del giorno reca, nell'ambito dell'indagine conoscitiva sull'abuso e lo sfruttamento dei minori, l'audizione del dottor Domenico Vulpiani, dirigente superiore della Polizia di Stato, direttore del servizio della polizia postale e delle comunicazioni. Egli informerà i membri della Commissione sullo stato di avanzamento dell'indagine relativa ai siti pedopornografici, in particolare sulle novità emerse nel corso dell'indagine stessa; costituirà oggetto di particolare interesse, inoltre, il collegamento dell'attività della Commissione con quella della polizia e dei vari ministeri svolta a favore dell'infanzia, anche in vista di possibili iniziative da proporre in sede parlamentare.

Il dottor Vulpiani è accompagnato dal dottor Sergio Staro, vice questore aggiunto della polizia di Stato.

Do subito la parola al dottor Vulpiani, che ringrazio per aver accettato il nostro invito.

DOMENICO VULPIANI, *Dirigente superiore della polizia di Stato, Direttore del servizio della polizia postale e delle comunicazioni.* Vi ringrazio per avermi dato la possibilità di illustrare, in una sede così qualificata come quella di una Commissione parlamentare, il nostro lavoro, in questo momento sottoposto all'attenzione dell'opinione pubblica e delle massime autorità dello Stato. Ho ritenuto opportuno non preparare una relazione scritta, ma predisporre una serie di diapositive che illustrerò ai membri della Commissione.

Abbiamo dato inizio ai lavori investigativi a seguito dell'entrata in vigore della legge n. 269 del 1998 sullo sfruttamento sessuale dei minori, che ci ha consentito di verificare gli approcci investigativi a questi problemi. Tali approcci non potevano essere semplicemente quelli tradizionali perché avevamo a che fare con un problema non più legato ad un particolare territorio ma fortemente delocalizzato, con una extraterritorialità addirittura planetaria, che interessa legislazioni e tecniche investigative in continua evoluzione tecnologica non sempre prevedibile.

Sulla base delle indicazioni fornite tre giorni orsono dal presidente Burani Procaccini, ho organizzato la mia esposizione: vorrei innanzitutto focalizzare l'attenzione su *Internet* e sulla pornografia minorile (senza approfondire troppo questo punto, per non correre il rischio di apparire dispersivo); in secondo luogo mi concentrerò sul commercio elettronico di materiale pedo-pornografico, che è ciò che più interessa perché, almeno apparentemente, sembra maggiormente pericoloso per i

nostri figli e per i minori che navigano in *Internet* e sono vittime di attenzioni sessuali. Vorrei, in seguito, trattare l'argomento della pedofilia *on-line*: i pedofili esistevano anche nel passato ma, con l'avvento di *Internet,* sono usciti allo scoperto perché questo sistema offre possibilità inedite. Traccerò, infine, il quadro dei percorsi investigativi che abbiamo seguito negli ultimi tre anni e che ci hanno consentito di raggiungere alcuni risultati. Come mi è stato richiesto, fornirò la nostra opinione sulla navigazione sicura in *Internet,* secondo ciò che si apprende da notizie provenienti dal mercato e da settori dell'opinione pubblica attenti a questo fenomeno.

Non è mio compito illustrare le possibili modifiche alla legge n. 269 del 1998, che ritengo ancora validissima; credo però necessario innovare alcune tecniche procedurali per consentirci di accelerare i tempi. Non possiamo più procedere con i tradizionali tempi investigativi, che devono essere abbreviati, garantendo una supervisione dell'autorità giudiziaria anche in fase successiva, in maniera da evitare lungaggini che ci impediscono di investigare in modo concreto.

Debbo premettere che uno dei volani fondamentali per la diffusione di *Internet,* nel passaggio dall'impiego militare all'applicazione civile, è stato la pornografia, che si è subito diffusa con il commercio elettronico. Sappiamo bene che la pornografia, quasi ovunque nei paesi occidentali, dove *Internet* sta prendendo piede grazie al progresso tecnologico, viene ritenuta lecita se non coinvolge atti sessuali od osceni compiuti da minori. Noi ci occupiamo, dal punto di vista inquirente (come anche il legislatore ha evidenziato), della pornografia minorile in *Internet:* consideriamo rilevanti a questo scopo le fotografie che ritraggono minori coinvolti in atti sessuali o in pose sgradevoli e non semplicemente bambini nudi, come appaiono nelle foto che molti di noi hanno in casa. È evidente che non bisogna avere un atteggiamento rigidamente repressivo.

Cosa troviamo in *Internet* ? È necessario capire come si sviluppa il fenomeno di cui stiamo discutendo: attraverso l'offerta sui siti *web* o *news group,* che sono luoghi di discussione, oppure mediante le *chat,* che sono i canali più trascurati ma, secondo la nostra esperienza, i più pericolosi. Dal lato della domanda, *Internet* offre la possibilità planetaria di ricercare questo materiale per soddisfare determinate perversioni o curiosità occasionali, che hanno origine nella pornografia cosiddetta normale e si orientano verso la pornografia minorile, secondo una scala di devianza o perversione più dura, meno comprensibile.

Gli scambi avvengono attraverso una navigazione mirata dell'utente che ricerca questi siti, oppure attraverso scambi di posta elettronica tra soggetti con le stesse inclinazioni, oppure ancora, attraverso le *chat* o i *news group.* Esistono pagine *web* ad accesso condizionato (ossia a pagamento) oppure libere; i siti *web,* per la quasi totalità, hanno un accesso condizionato, perché si tratta di una forma di commercio. Nella navigazione, si parte da siti pornografici normali per arrivare, nello stesso sito, a settori pedo-pornografici. Questi siti vivono anche di pubblicità di cui si occupano i vari *provider,* dando origine ad un meccanismo economico perverso: se un *provider* decide di avere siti pornografici, pubblicizzerà altri prodotti sullo stesso sito ed otterrà il guadagno proprio dalla pubblicità, non tanto sul prezzo del sito o della pagina *web.* Il meccanismo poi è semplice: si acquistano immagini e si scaricano. Sappiamo che è reato anche soltanto consultare un sito pornografico nella parte *preview* (di vista generale) o nella parte a pagamento ma, se non c'è flagranza di reato durante la consultazione, il semplice collegamento non costituisce reato; scaricare le immagini, invece, consente alle forze di polizia, successivamente, di acquisire la prova che un determinato *file,* contenente immagini pedo-pornografiche, è stato scaricato: ciò costituisce prova di reato sanzionata ai sensi dell'articolo 600 del codice penale.

Le *news group* sono bacheche elettroniche ed è molto difficile rincorrere i personaggi che vi si affacciano; esse sono canali di conversazione che possono essere

aperti « a grappolo », come un albero, in maniera articolata, con il coinvolgimento di persone che chiamano dall'estero oppure dall'Italia. Le *news group* costituiscono la nostra fonte maggiore di investigazioni positive con le quali riusciamo a catturare i pedofili (almeno quelli italiani: gli altri li lasciamo ai nostri colleghi).

L'*e-mail* è di difficile controllo preventivo, perché i messaggi vengono scambiati tra soggetti conosciuti; dovremmo individuare un soggetto sospetto e chiedere il permesso di intercettazione all'autorità giudiziaria: a quel punto, si entra in una fase in cui la Polizia non può operare, se non previa autorizzazione del magistrato.

Vi mostrerò ora alcune diapositive come esempio, non scabroso, accettabili in qualunque consesso, sul modo in cui si presentano le pagine *web*: è la pagina di un cartone animato pedo-pornografico, così come l'abbiamo trovato (censurata nella parte più scabrosa, perché posso assicurare che le immagini di atti sessuali che coinvolgono minori sono ripugnanti).

Le *news group* si presentano in modo che ad ogni riga corrisponde un messaggio: a sinistra dei messaggi noterete la classica *attache,* che indica la presenza di un allegato che può essere costituito da immagini. Noi applichiamo una certa tecnica nel rintracciare alcuni indizi, selezionandoli a partire dall'esperienza pregressa: a volte si vede l'immagine di una Ferrari e poi ci si ritrova in un sito o in un *news group* con immagini pornografiche o di minori. Lavoriamo molto, ma si tratta di un compito difficile perché gli autori delle immagini « scappano »: l'inseguimento è piuttosto complesso ma, a volte, sortisce esiti positivi.

Le *chat server,* in sostanza, costituiscono il settore investigativamente più proficuo. Esse sono organizzate con una struttura ad albero: alcuni canali vengono aperti come posta elettronica. Sono canali dinamici in continua evoluzione, dove si tengono *forum* di discussione su temi di vario tipo, dalla cucina italiana o russa, alla moda, alle automobili; poiché si tratta di canali di facile appuntamento e non costano nulla, sono preferiti dagli adolescenti (oltre ai telefonini e agli SMS). In genere si tratta di *chat* che gli stessi adolescenti organizzano tra loro; in questi casi, sono contrario a creare allarme perché i ragazzi che hanno un discreto livello culturale, che frequentano la scuola ed hanno a disposizione un *computer* sono in grado di difendersi da soli da certi attacchi (il PC è un mezzo molto interessante e non bisogna soffocarne l'uso). Come vedremo, si possono impiegare misure cautelative per la navigazione protetta a vantaggio dei minori più piccoli dei quattordicenni, i quali si difendono bene da soli nella vita: non abbiamo avuto prove di gravi danni.

L'ultimo aspetto riguarda le *e-mail,* che sono conosciute da tutti e che, in genere, coinvolgono due o più persone. Esse vengono usate quando si ha fiducia nell'altro interlocutore o lo si conosce direttamente: quando i nostri operatori rintracciano le *e-mail,* le indagini compiono un passo avanti e riusciamo ad ottenere risultati proficui tramite le intercettazioni telematiche.

Come si presenta una *e-mail* ? È importante la pagina dove figura un numeretto, che corrisponde ad un indirizzo telematico (IP), a cui si risale attraverso il *provider,* che fornisce l'informazione sull'utente che in quel momento ha utilizzato quell'IP. In sostanza, è come risalire attraverso la targa della macchina, al proprietario di una autovettura che è passato con il rosso.

Questa operazione, tuttavia, che fino a poco tempo fa veniva concessa facilmente dai nostri *provider,* a seguito dell'entrata in vigore del decreto antiterrorismo e di una certa interpretazione di una disposizione normativa, non è più così immediata. I *provider,* infatti, non ci vogliono più dare questi dati senza previa autorizzazione del magistrato; si tratta di dati esterni, come nel caso in cui si deve risalire all'intestatario di un numero telefonico. Noi, in quanto polizia e carabinieri, in tutte le indagini tradizionali, otteniamo questi dati senza nessun decreto da parte dell'autorità giudiziaria perché ciò rientra nelle nostre competenze. Se così non fosse,

potremmo chiudere bottega e aspettare che i malviventi vengano a costituirsi per prenderli; né possiamo appesantire l'autorità giudiziaria con la richiesta di acquisizione di dati laddove non si verifica alcuna lesione della *privacy*.

L'elenco telefonico peraltro è disponibile in qualsiasi bar: se invece di consultarlo lì, viene consentito di accedervi per telefono o tramite una banca dati, non ritengo vengano lesi gli interessi sulla *privacy* di alcuno.

Quali sono le caratteristiche del pedofilo? Anzitutto, in base alle nostre esperienze, abbiamo constatato che la rete dei pedofili si estende, ben oltre l'Italia, all'estero, poiché *Internet* non si limita soltanto ad un ambito italiano; quindi ci troviamo di fronte a pedofili che comunicano, si scambiano informazioni e consultano siti sia nel nostro paese sia al di fuori di esso.

Solo pochi giorni fa, abbiamo terminato un'operazione a Venezia che ha comportato, nel territorio nazionale, cinque arresti e ventisei denunciati, questi ultimi con posizioni penalmente meno gravi dei primi, ma anch'essi pedofili. Tutti erano in contatto con un'altra trentina di soggetti tedeschi, probabilmente non totalmente individuabili, ma di cui abbiamo informato la polizia tedesca, fornendole i dati elettronici in nostro possesso (trattandosi di persone operanti sul loro territorio spetta a loro procedere).

Il pedofilo è per natura curioso: clicca su un sito, lo visita e poi scappa. Vi è poi il pedofilo occasionale, che ci telefona – com'è avvenuto di recente – senza nascondere il fatto che stesse consultando un sito pornografico ed afferma di essersi imbattuto in un sito pedopornografico: questa è la tipica segnalazione. Tuttavia, essendo noi « sbirri » per definizione, molto spesso non crediamo a quanto ci viene detto; succede – probabilmente – che un utente entri a visitare un certo sito – non accade in modo casuale – ed in un secondo tempo, magari preoccupato per le nostre indagini tecniche, forse preferisca comunicarlo alla polizia. Questa fattispecie di soggetto ci soddisfa ugualmente, perché per noi il curioso non deve essere etichettato come persona pericolosa. Quindi, non scoraggiamo questo tipo di denunce, inquisendo o « torturando » colui che si espone attraverso la denuncia, perché è meglio ricevere una collaborazione spontanea da parte di tutti gli utenti – molti dei quali spinti da eccessiva curiosità – piuttosto che criminalizzarli e sbatterli alla gogna.

Vi sono ancora il collezionista ed il produttore di immagini pedofile; in queste due ultime fattispecie, si tratta di persone che visitano i siti o si servono delle *chat line* per cercare materiale.

A questo punto, è il caso di aprire una parentesi. Il materiale pornografico che si trova nelle reti commerciali è quasi sempre lo stesso, che si sposta di *server* in *server*, venendo ricopiato: si tratta, in pratica, di una sorta di enorme fotocopia dello stesso materiale che viene ritagliato e montato; a volte, addirittura le immagini vengono costruite con il *computer*.

In realtà, il pedofilo vero non prova molta soddisfazione nel far ciò, perché alla fine, tutte queste immagini le ha già viste e pagate anche ad un prezzo non indifferente (peraltro correndo il rischio di essere individuato attraverso l'utilizzo della carta di credito; per questo non vi ricorre volentieri e preferisce le *chat line).*

Il pedofilo vero, in realtà, cerca immagini nuove, siano esse prodotte amatorialmente o industrialmente, che non compaiono sui siti a pagamento. E dove le può trovare? Presso altri che hanno la stessa inclinazione sessuale e per questo è alla ricerca di persone che condividano come lui tale necessità. Prima dell'avvento di *Internet* questa operazione sarebbe stata impossibile, perché non c'era la possibilità di esporsi mantenendo l'anonimato; *Internet*, in tal senso, ha aperto nuove frontiere: non ha fatto aumentare il numero dei pedofili – intendiamoci – ma ha semplicemente messo in luce un fenomeno che prima non poteva essere individuato.

La produzione di immagini pedopornografiche, può essere di natura domestica,

industriale, digitalizzata o proveniente dalla diffusione sulla rete, di cui ho già parlato.

Con il termine produzione domestica, intendiamo la produzione di materiale da parte di tutti coloro che sono vicini al minore. Le persone individuate come pedofili svolgono le professioni più svariate: dal poliziotto – e chiamo in causa per prima la mia categoria così da non offendere nessuno – come nell'ultimo caso, dove abbiamo arrestato un agente della stradale, al sacerdote, al professore di scuola, all'insegnante di musica, all'allenatore di calcio, allo zio, al parente più stretto. Non scopriamo nulla di nuovo: i minori sono insidiati all'interno della cerchia che frequentano più da vicino. Si tratta quindi di operatori sociali o membri della famiglia. Molto più raro è il caso del minore che venga adescato occasionalmente da un pedofilo di passaggio. Il minore, in realtà, viene sempre seguito, almeno fino a 12-13 anni da qualcuno della famiglia, e proprio quando viene affidato ad altri, per esempio il vicino, spesso a ciò segue un epilogo tragico.

Noi scopriamo tutto questo solo *a posteriori*, quando andiamo a sequestrare il materiale (si tratta molto spesso di fotografie del bambino o di riprese eseguite dal soggetto che abbiamo individuato, magari attraverso *Internet*). Quest'ultimo, quindi, ci serve, più che altro, come indicatore, poiché ci fornisce la possibilità di individuare soggetti sospetti, i quali probabilmente non sanno che visitando siti pedopornografici in rete, si corre il rischio di essere individuati.

Desidero ora fare qualche breve cenno al meccanismo di funzionamento di questi siti. Innanzitutto, la richiesta che più spesso ci viene rivolta riguarda la loro eventuale chiusura. Per aprire un sito, pornografico o meno che sia, si comincia con la creazione di un dominio, cioè di un sito *web* appartenente ad una persona, che può essere aperto attraverso *Internet* da qualunque paese del mondo, rimanendo comodamente a casa propria, fornendo anche false identità dal momento che in alcuni paesi non viene eseguita alcuna verifica: basta che – non importa in che modo – si paghi ed arrivino i soldi.

L'ubicazione fisica del *server*, a volte, non corrisponde neppure al paese in cui il dominio è registrato. Si può infatti utilizzare un *server* in un terzo paese, diverso da quello in cui esiste il dominio che, in altre parole, è come la camera di commercio per le società. Per quanto attiene al *server*, invece, si affitta, materialmente, uno spazio da un *provider*, nell'ambito del quale si apre il sito contenente le immagini. Queste ultime possono essere assolutamente normali, celando, in genere, al loro interno, immagini pedopornografiche. In questo modo, si acquista, in pratica un diritto. Gli americani, che sono stati i primi a diffondere *Internet*, trasformandolo dall'impiego militare a quello civile, sono stati precursori in tal senso.

Pertanto, la gran parte di domini e di *server* sono attualmente allocati – parlo esclusivamente di questi due, perché su di essi possiedo dati certi – negli Stati Uniti.

Vorrei ora chiarire quanto ho appena esposto. Attraverso l'immagine grafica, il gestore del sito si collega ad *Internet*, magari attraverso un *provider* italiano, entra nella rete e si rende anonimo (esistono programmi appositi per mantenere l'anonimato). Va in un altro paese, contatta una società gestore di domini e comunica che desidera registrare un dominio a suo nome, pagando una certa cifra, con carta di credito o simili. Infine, apre il *server* in un terzo paese ancora o nello stesso paese, purché distinto da quello del dominio.

Si capisce, quindi, che risulta della massima importanza la collaborazione internazionale al fine di ricostruire tale percorso. Possiamo anche avvalerci di programmi che permettono di ricostruire il percorso – come meglio vedremo in seguito –, tuttavia, se non c'è collaborazione, perlomeno da parte del primo *provider*, non sempre riusciamo ad arrivare all'identità del gestore del sito.

Altre volte è necessario fare il percorso all'inverso, e cioè, dal *server* risalire al dominio, per poi arrivare al paese (nel-

l'esempio di prima l'Italia). Molto spesso però proprio in questo percorso a ritroso, siamo costretti a fermarci perché non otteniamo la collaborazione delle polizie straniere o dei *webmaster* che restano coinvolti in tale opera di tracciamento.

Con riferimento al commercio elettronico, esso funziona sostanzialmente sulla base di una transazione finanziaria attraverso carte di credito, le quali, a volte, sono estero su estero e comunque, più spesso ancora risultano clonate e quindi non riferibili ad un titolare identificabile. Inoltre, nella maggior parte dei casi, le carte di credito non specificano l'entità della spesa, perché questa fonte di commercio elettronico permette guadagni enormi, pur sembrando la visione di immagini a basso costo. È, infatti, sulla quantità dei collegamenti che avviene il profitto e la curiosità sessuale è molto diffusa, anche quella eterosessuale e quest'ultima permette ulteriori guadagni. Non è quindi solo la pedopornografia a garantire profitti, bensì la grande quantità di collegamenti sui siti pornografici in genere, che avvengono durante le ore di ufficio, al di fuori della famiglia, oppure in orari notturni, quando non si è osservati (magari dalle proprie mogli).

Ricordo a tale proposito le immagini di Pamela Anderson, la famosa bagnina della serie televisiva; vi lascio immaginare quanti collegamenti sono stati effettuati sul suo sito – ricordo che all'inizio la visione di quelle immagini era addirittura gratuita – e ciò produce in generale un effetto volano, con una moltiplicazione delle richieste, tutte nella stessa direzione. Non è raro che siamo chiamati da enti pubblici o privati che lamentano all'improvviso un aumento spropositato delle bollette telefoniche, dovuto, in realtà, ai frequenti collegamenti degli impiegati stessi dell'azienda che di tanto in tanto vanno, per così dire, a fare un viaggetto su *Internet*.

La criminalità organizzata, come è evidente, di fronte all'esigenza di creare nuovo materiale e produrre nuovi film pornografici, non poteva rimanere al di fuori di tutto ciò e per questo si è organizzata, entrando in un mercato in cui i guadagni continuano a lievitare.

Qual è, tuttavia, il fattore che rende veramente proficuo e favorevole questo mercato? È l'anonimato, il fatto cioè che l'acquirente possa rimanere anonimo, non comparendo sulla sua carta di credito l'indicazione di ogni spesa effettuata (nel caso specifico, per esempio, « sexy shop – Amsterdam »).

Tale anonimato è stato introdotto, in realtà, per proteggere categorie non eterosessuali, per esempio gli omosessuali, ma questa è l'altra faccia della medaglia: per proteggere loro da un lato, la coperta si è rivelata troppo corta dall'altro! Naturalmente, il mercato si adegua alle esigenze degli utenti: per questi ultimi la riservatezza è fondamentale e il mercato l'ha subito garantita. Sono state infatti create società terze per mezzo delle quali il cliente può, in sostanza, visitare un sito pornografico, non pagando direttamente quest'ultimo, ma un intermediario.

Da un lato, il sito pornografico non riconosce il visitatore perché il pagamento è fatto a terzi, dall'altro, la carta di credito non permette di risalire al cliente vero in quanto non viene specificata la reale natura di quanto venduto dal terzo utente intermediario.

Per chiarire meglio, l'utente che possiede una carta di credito procede ad una transazione finanziaria con una banca; quest'ultima, a sua volta, soddisfa il pagamento del sito dove sono le immagini che il cliente ha scaricato: il detentore è quella banca *on line*. Su *Internet*, questi passaggi possono moltiplicarsi e questo vale per tutte le transazioni, non solo quelle pedopornografiche, ma anche per quelle pornografiche in genere.

Quindi, quando troviamo tale massa di transazioni, non sapendo cosa è stato venduto, non possiamo neanche conoscere ciò che è stato pagato, né eventualmente, sapere se è stato scaricato materiale pedopornografico presente nel sito, che, ad esempio, potrebbe essere all'estero.

Questa è l'immagine più semplice, ma pensatela composta e scomposta: l'utente è

a Roma, il sito nel Wisconsin e la banca a Bruxelles: il mondo virtuale non ha confini ed il commercio non segue leggi politiche, bensì economiche, che prescindono da qualsiasi condizionamento, soprattutto nell'attuale fase di grande espansione liberista: più ampio è il mercato, maggiori sono le possibilità di agire.

A volte le operazione sono compiute estero su estero, come nelle transazioni e nel riciclaggio, che precedentemente avvenivano tra banca e banca. Per la mente umana era abbastanza facile seguirne le tracce, ma oggi, sebbene l'operatore sia bravissimo, non siamo più in grado di farlo. Stiamo studiando programmi per velocizzare la ricerca su *Internet* di tutti i dati utili riguardanti le transazioni finanziarie e le ricerche dei siti. Sarebbe utile, inoltre, che i gestori telefonici concedessero le loro informazioni con maggiore elasticità, in quanto la polizia, essendo tenuta al segreto, non lederebbe alcuna *privacy*. Non capisco, infatti, perché gli organi investigativi, che rappresentano lo Stato e le istituzioni, non possano esaminare il tabulato telefonico della Telecom, quando essa stessa, invece, può farlo nelle vesti di operatore commerciale.

Sono stato a capo della DIGOS di Roma per cinque anni, fino al febbraio scorso; quando mi sono occupato del caso D'Antona ho individuato il telefonista grazie ai tabulati: utilizzando potenti *computer*, infatti, siamo risaliti alle comunicazioni inviate prima e dopo il fatto. Ci siamo avvalsi della collaborazione importante (trattandosi di un caso di terrorismo) dei gestori dei servizi telefonici, anche se i tempi si sono allungati moltissimo. Infatti, solo « inginocchiandomi » siamo stati in grado di avere i dati su supporto magnetico, altrimenti avremmo dovuto riportare manualmente migliaia di dati cartacei, impiegando molti mesi di lavoro. Per evitare tutto ciò, lo Stato dovrebbe eventualmente pagare il prezzo di questi servizi alle società private, perché velocizzare i tempi dell'indagine informatica oggi risulta essenziale: i file di *log* ed *IP* cambiano velocemente e possono sparire dal sito.

La polizia delle comunicazioni esiste da tempo, come postale all'inizio e, successivamente, come unione di vari uffici, dei quali faceva parte il primo ufficio di polizia di informatica, costituito nel 1992 e « santificato » da un decreto ministeriale, che ha stabilito le articolazioni centrali e periferiche (esistono circa 75 sezioni con 2 mila uomini in tutto il territorio nazionale). La sua competenza è relativa ai crimini del settore investigativo della polizia informatica. Quando è entrata in vigore la legge n. 269 del 1998, l'esperienza del nostro personale, che aveva precedentemente già lavorato in questo settore, ha rappresentato un grande vantaggio. La polizia delle comunicazioni ha assorbito anche il NOPT, che era un organismo esclusivamente con funzioni di polizia informatica e che poi si è sviluppato all'interno del servizio, seguendo le nuove frontiere della polizia informatica.

I due approcci investigativi adottati per la lotta alla pedofilia *on line* esaminano l'offerta dei siti *web*, per ricostruire così un percorso a partire dalle carte di credito, e la domanda, che viaggia nelle *chat*, per cercare di individuare il pedofilo. Il primo dei due approcci è cominciato a settembre con un monitoraggio di ventiquattro ore (mentre prima era a campione), anche per la sollecitazione di vari organismi, anche esterni, come l'associazione Arcobaleno, che accusavano la polizia di non essere pronta. Comunque, l'esistenza di molti siti pedopornografici, con un materiale difficile da accettare per l'uomo comune, non significava che la polizia delle comunicazioni non stesse lavorando. Essi erano noti, ma – essendo all'estero – non potevano essere chiusi, a meno che la polizia dell'altro Stato non lo avesse consentito. Quando troviamo siti sospetti o contenenti certe immagini, verifichiamo l'esistenza del dominio e la sua registrazione e, attraverso *Internet*, proseguiamo nelle indagini. Infatti, molti dati – sebbene falsi – debbono essere registrati ed è importante verificarlo per risalire, attraverso il supporto fisico della linea telefonica, al *computer* in Italia. Tuttavia, diverse volte l'indagine risulta interdetta

dall'assenza di comunicazioni da parte della polizia straniera competente. Resta il fatto che, sebbene nel virtuale tutto sia modificabile, non è possibile fare altrettanto per l'utenza telefonica domestica o di ufficio, che permette di ottenere il numero dal quale è stato attivato il *computer*.

L'altro aspetto da verificare è la localizzazione del *server*; nei primi tempi essi erano allocati in Italia, ma – dopo le prime scoperte – il loro contenuto è stato trasferito, attraverso *Internet*, in altri paesi affittando un'*host mail*. Naturalmente, per localizzare il *server* abbiamo dovuto studiare programmi e comunicare con le altre polizie straniere per compiere i tracciamenti telematici, che di solito avvengono attraverso l'invio di un pacchetto di dati segnati al fine di ricostruire il messaggio ed arrivare così all'obiettivo finale. Essi sono dotati di due targhe – una anteriore ed una posteriore – rintracciabili nel momento in cui quella anteriore si collega al numero di origine dell'offerta, permettendo il ritrovamento del *server*. Ovviamente, non conosco perfettamente i particolari tecnici, ma è importante capire che la verifica compiuta per ogni sito ha lo scopo di trovare il dominio, il *server* ed, attraverso la carta di credito, il pagamento.

Con il monitoraggio effettuato dal 1998 ad oggi, sono stati esaminati 20 mila siti, segnalando all'estero per 4 mila di essi tutto ciò che fosse estero su estero, e sono state avviate 2 mila e 21 indagini in tutto il territorio nazionale, delle quali molte non sono state concluse, perché, riguardando l'offerta, sono risultate le più difficili.

Inoltre, dall'inizio del 2001 sono stati monitorati 14 mila siti, dei quali 9 mila e 140 per nostra iniziativa. Dal settembre 2001 è stato realizzato un controllo per ventiquattrore ore attraverso una banca dati itinerante, consultata e alimentata da ogni parte del paese, avviando una forte sinergia tra gli uffici che lavorano e comunicano telematicamente, e sono state sfruttate le potenzialità di *Internet* mediante una serie di studi di fattibilità. Alla fine, si è appurato che durante l'anno in corso i siti, che non hanno il *server* in Italia, ma sono riconducibili a persone italiane, risultano essere soltanto quattro. Da analisi di un campione di circa mille siti, l'80 per cento della localizzazione dei *server* e dei domini è negli Stati Uniti. Ovviamente, ce ne siamo interessati, ma in questo momento l'FBI ha problemi con i *custom*, che sono i nostri referenti, ed inoltre ha questioni più serie da seguire; comunque, va dato atto che il servizio americano ha dato la propria disponibilità per concretizzare alcune difficili operazioni sulle quali stiamo già lavorando con le procure di Milano e di Salerno.

Apparentemente più difficile, invece, potrebbe sembrare operare dal lato della domanda, ma in realtà non è così perché si lavora sotto copertura, fingendosi pedofili ed indagando nelle *chat*. Grazie alla legge n. 269 del 1998 è possibile compiere acquisti simulati e creare siti « esca », che risultano però poco utili nell'indagine, contrariamente al rapporto a due.

L'*iter* investigativo per scovare il pedofilo si svolge secondo questi canoni. La persona indagata si nasconde dietro dei *nickname*, compie degli *account* falsi, ed è convinta così di poter sfuggire alle indagini, ma dimentica che il suo collegamento telefonico opera su una *chat* italiana, per cui, avendo a che fare con soggetti italiani, l'indagine viene per forza di cose ricondotta al nostro paese. A questo punto i nostri rapporti sono con i *server* e con magistrati italiani ed è più facile, dopo aver individuato il soggetto attraverso i controlli telefonici, telematici e con i pedinamenti, concludere il ciclo investigativo. In sede processuale la prova interessante è rappresentata dai dati forniti, attraverso un decreto di acquisizione, dal *provider*, con i quali si identifica il soggetto e si termina l'indagine: più veloce è il circuito, più facile è ottenere risultati.

Come potete notare, il *trend è* crescente anche se nel 2001 sembra essersi verificato un calo; in realtà, ciò è da attribuire al fatto che alcune operazioni in corso si chiuderanno nel 2002.

I pedofili si nascondono sempre di più, ma abbiamo affinato le tecniche e continuiamo a riscuotere successo. Esiste una progressione di utilizzazione di *Internet*, ma non tutti i pedofili lo usano, perché non tutti sono in grado di farlo (bisogna essere giovani o possedere un certo grado di cultura). Considerando anche solo questo spicchio di attività, i dati sono piuttosto allarmanti e denotano, soprattutto dal numero di persone sottoposte alle indagini (che hanno tutte questa devianza sessuale), una grande quantità di casi: non sono aumentati con il tempo, ma escono allo scoperto.

Non vorrei abusare della pazienza dei membri della Commissione, ma vi sono altri problemi da affrontare.

PRESIDENTE. Al contrario, la sua esposizione è interessantissima.

DOMENICO VULPIANI, *Dirigente superiore della polizia di Stato, Direttore del servizio della polizia postale e delle comunicazioni*. Esistono alcuni problemi, uno dei quali riguarda le barriere delle giurisdizioni; ad esempio, la questione della localizzazione dei siti non coinvolge solo la giurisdizione per affrontare la quale è dunque necessaria una collaborazione internazionale. Si tratta di intendenze che dobbiamo portare avanti in gruppo, come istituzioni, anche nei riguardi di paesi stranieri, stringendo rapporti più saldi per perseguire lo stesso fine.

La collaborazione internazionale, in questa materia, avviene lungo tre canali: attraverso il G8, dove abbiamo un punto di contatto 24 ore su 24 – servizio che svolgiamo noi – esteso agli otto paesi (con referenti diretti della polizia), tramite l'Interpol e l'Europol.

Siamo impegnati nella realizzazione di un importante progetto per la costituzione di una banca dati a livello europeo, inserita nell'ambito di Interpol (che potrà essere aperta anche ad altri). Si tratta di un progetto costoso, sul quale abbiamo ricevuto la collaborazione di paesi importanti e la destinazione di fondi europei: se riuscissimo ad ottenere tali finanziamenti compiremmo un grande passo avanti, anche sotto il profilo tecnico-investigativo. Inghilterra e Germania sono i nostri *partner*: noi siamo stati i promotori, ma abbiamo preferito che capofila del progetto fosse l'Inghilterra (dove esiste una consistente spinta politica su tale problema), paese che riesce ad essere molto ascoltato a livello europeo. È stata, dunque, una scelta dettata dall'opportunità, ma noi tentiamo di imprimere una spinta all'intero processo; anche la Germania è fortemente motivata. Naturalmente, esistono gelosie da parte di altri paesi: la Francia, ad esempio, vorrebbe adottare un sistema di origine francese; Inghilterra, Germania ed Italia sono nazioni autorevoli e forse riusciremo ad ottenere le risorse necessarie.

Le problematiche del *database* che stiamo realizzando a livello europeo corrispondono, in parte, alle nostre: modalità di alimentazione (esiste un problema relativo al segreto istruttorio), modalità di consultazione e ubicazione presso organizzazioni internazionali. In origine, eravamo disposti ad ospitarlo ma, in seguito alla nascita di alcuni problemi, abbiamo preferito cedere il passo in modo da ottenere l'appoggio di Europol o di Interpol (lo ospiteranno, forse, i francesi); si tratta di compromessi, l'importante è che il progetto si realizzi.

Esistono, in secondo luogo, problemi tecnici di realizzazione e di gestione: su questi aspetti, abbiamo compiuto un grande passo avanti perché, almeno per la parte italiana, 19 compartimenti sono collegati al mio servizio, in una banca dati che non è a raggiera, ma circolante, dove l'informazione appunto circola in tempo reale; i dati inseriti a Milano sono visibili a Palermo dopo un secondo. Si tratta di un fatto importantissimo, che rende lo strumento vivo e funzionale lungo l'arco delle ventiquattro ore: la polizia delle comunicazioni lo estenderà a tutte le indagini informatiche.

Vorrei esaminare il tema della navigazione protetta per i minori, su cui mi era stato chiesto di intervenire. Non creerei troppo allarme, ma esistono tre tipi di tecniche che abbiamo rintracciato sul

mercato: una navigazione vietata a determinati siti (il *provider* indica su quali siti è possibile navigare, indirizzando il minore, soprattutto i più piccoli che non hanno grandi capacità); una navigazione limitata solo a siti consentiti *(white list)*; una navigazione più allargata, escludendo solamente i siti vietati *(black list)*. In quest'ultimo caso si può navigare ovunque tranne che nei siti pornografici e tale scelta può essere compiuta dai familiari.

Quali sono i limiti di questa opzione? Seguendo una qualsiasi navigazione, si può finire su siti gestiti da un altro *provider* e la protezione familiare può essere eliminata se il ragazzo è sufficientemente scaltro, posto che le parole chiave sono sempre le stesse. Tutte le protezioni, molte volte, non sono sufficienti; ad esempio, in un particolare sito dei Pokémon, si trovavano i cartoni animati atteggiati in pose sessuali: tutti i bambini vogliono vedere i Pokémon e così si è ideato un tale sito. L'estrema dinamicità del sistema costituisce la ragione per cui esso è di difficile rincorsa per il *provider*, per le famiglie: la fantasia dei soggetti criminali che usano *Internet* è grandissima, supera qualsiasi immaginazione. I sistemi di protezione sono estremamente aggirabili: ci si può collegare ad *Internet* con un nuovo *account*, gratuitamente, da casa propria ed è difficile per un familiare, non abile quanto i figli, accorgersene.

È possibile dividere i minori in due fasce: per la prima, è possibile utilizzare questi sistemi di protezione, mentre per l'altra, ripeto, non ci preoccupano tanto i siti pornografici, quanto le *chat*. Cito come esempio il film *Viola*, ispirato ad un adescamento « al contrario »: attraverso una *chat*, un bambino si fingeva adulto e corteggiava una donna, la quale si invaghiva telematicamente di lui, per poi scoprire – il bambino non si presentava agli appuntamenti – che si trattava di un bambino di nove o dieci anni, classico filibustiere che l'aveva indotta in questo errore.

La legge n. 269 del 1998 non considera alcuni comportamenti: non possiamo infatti arrestare coloro che accedono a siti pornografici a titolo gratuito, cioè coloro i quali scambiano immagini pornografiche. La pena è fino a tre anni e dunque la legislatura vigente non ci consente l'arresto, neppure facoltativo (ed è facoltativo fino a cinque anni); potrebbe essere rivista la pena edittale, innalzandola a cinque anni. Un altro problema riguarda la detenzione: possiamo trovare una grande quantità di materiale, ma non possiamo provare che l'abbia distribuito più di una persona (in questo caso si tratterebbe di distribuzione, con l'ipotesi di una pena di cinque anni). Il soggetto infatti che detiene grande quantità di materiale può essere più colpevole di chi ha scambiato solo una immagine. Inoltre, viene colpita la produzione commerciale – gravemente, in modo giusto: il passo successivo investigativo che ancora non riusciamo a compiere, ma sul quale dobbiamo insistere, riguarda le immagini provenienti dall'estero – mentre il caso della produzione domestica rientra nella detenzione: si può trattare di filmini riguardanti il vicino di casa, la nipotina o tutti i bambini. Credo che il magistrato debba « forzare la mano » e trasformare la distribuzione in scambio (magari non ha distribuito, ma consegnato il materiale, semplicemente all'agente sotto copertura). In realtà, la distribuzione domestica è una fattispecie che andrebbe sanzionata diversamente.

Vorrei sottolineare un aspetto, emerso sulla base dell'esperienza concreta e che riguarda il problema della *privacy*. La direttiva CE 97/66 è stata recepita con il decreto legislativo del 13 maggio 1998, n. 171: essa prescrive che i fornitori di servizi di connettività, di telecomunicazioni in genere, i gestori di servizi telefonici fissi (dalla Telecom a Virgilio) ed i *provider* sono tenuti a cancellare, al termine della chiamata, tutte le transazioni delle comunicazioni che sono avvenute. Ciò può consentire di mantenere soltanto a fini commerciali i dati; infatti, soprattutto i gestori telefonici li mantengono perché devono fatturare, mentre i *provider* non hanno nessuna esigenza di fatturazione, essendo il servizio gratis; di fatto vengono conservate per semplice conces-

sione. La stessa direttiva CE, in un altro articolo indicava che il singolo contraente poteva derogare a questa disposizione a carattere generale per ragioni di pubblica sicurezza e di indagini giudiziarie. La sicurezza pubblica è un fatto più ampio: bisognerebbe studiare il modo per procedere ad eventuali modifiche così da consentire la conservazione dei dati di accesso, anche quelli a carattere libero, mantenendo pure l'anonimato, ma fornendoci la possibilità di unire il dato anonimo ad un numero telefonico.

CARLA CASTELLANI. È quanto prevedeva la risoluzione che approvammo nella scorsa legislatura.

CARLA MAZZUCA. E che prevedeva anche la mozione che abbiamo approvato recentemente.

DOMENICO VULPIANI, *Dirigente superiore della polizia di Stato, Direttore del servizio della polizia postale e delle comunicazioni.* A questo proposito preciso che esiste un gruppo interministeriale che sta studiando il problema, di cui facciamo parte come rappresentanti del Ministero dell'interno; ne fanno parte altresì rappresentanti del Ministero della giustizia, del Ministero delle comunicazioni e del Ministero dell'interno ed altri soggetti privati, interessati alla parte economica ed al fatto che venga approvato al più presto il listino prezzi. Non c'è una disposizione legislativa a monte che disponga il rispetto di obblighi per i privati. Un disegno di legge, che il Ministero della giustizia dovrà presentare, riguarderà gli obblighi sia per i gestori telefonici, sia per *Internet.*

Si tratta di un gruppo interministeriale che si riunisce presso il Ministero delle comunicazioni: un rappresentante del ministero presiede questo gruppo, ai cui lavori abbiamo partecipato più volte.

L'altro aspetto interessante è l'approvazione della convenzione sui crimini informatici, parte della quale è dedicata proprio alla pornografia e alla sua produzione. In quest'ambito normativo, l'Italia è all'avanguardia, poiché la legge n. 269 del 1998 aveva già anticipato molti punti in materia.

Il dottor Staro – insieme al dottor Sarzana, del Ministero della giustizia – è stato il rappresentante della delegazione tecnica per l'Italia e ha seguito tutti i lavori che si sono svolti sul tema negli ultimi due anni. Egli è stato uno dei fautori principali della convenzione, la quale rappresenta certamente un passo significativo, anche se, per quanto riguarda specificamente l'Italia, con le norme del 1996 e del 1998 e con alcuni altri decreti legislativi si trova già abbastanza all'avanguardia; l'adeguamento infatti cui il nostro paese deve sottoporsi, rispetto alle norme vigenti, è minimo e tuttavia va fatto.

Inoltre, in base alla convenzione, per velocizzare i tempi di raccolta dati, i paesi contraenti si impegnano, in caso di richiesta da parte di uno Stato che sta svolgendo un'indagine nei campi della criminalità informatica e quindi anche della pedofilia *on line*, a chiedere al paese che detiene il *server* di obbligare il *provider* a « congelare » i dati per almeno tre mesi, nell'attesa della rogatoria internazionale, ancora necessaria. Attraverso il « congelamento » di tali dati per il tempo suddetto, diventa così possibile risalire e ricostruire i percorsi.

CARLA MAZZUCA. Tre mesi è un tempo utile o sarebbe meglio un anno, come prospettato in altra sede ?

SERGIO STARO, *Vice questore aggiunto della polizia di Stato.* Il termine di tre mesi rappresenta il tempo minimo previsto dalla convenzione, eventualmente rinnovabile per analogo periodo; in ogni caso, la convenzione va oltre, laddove prevede che il termine non debba essere comunque inferiore al tempo necessario perché la richiesta rogatoriale venga inoltrata e giunga al paese che detiene i dati e che ne deve dare esecuzione.

CARLA MAZZUCA. La convenzione è già stata sottoscritta dal nostro paese ?

DOMENICO VULPIANI, *Dirigente superiore della polizia di Stato, Direttore del servizio della polizia postale e delle comunicazioni.* Sì, è stata sottoscritta dall'Italia, insieme ad altri 29 paesi, il 23 novembre a Budapest.

PRESIDENTE. Ne ha parlato recentemente il giudice Priore.

DOMENICO VULPIANI, *Dirigente superiore della polizia di Stato, Direttore del servizio della polizia postale e delle comunicazioni.* Immagino che si sia ora in attesa di ratifica, per lo meno per quella parte che non può essere recepita direttamente dal nostro ordinamento (suppongo che per fare ciò sia necessario un atto di recepimento da parte del Parlamento italiano).

Tale convenzione è rivolta a diverse legislazioni già vigenti; per quanto ci riguarda, essa si riferisce, per esempio, ai crimini informatici, laddove noi abbiamo già una legislazione piuttosto avanzata che prevede tale fattispecie e che andrebbe solo adeguata; si riferisce alla legge sulla pornografia minorile in *Internet* e, anche sotto questo aspetto, da noi sono già vigenti leggi in materia; si riferisce inoltre al diritto d'autore e, anche in quest'ambito, nel 2000 è stata approvata una legge piuttosto avanzata. Quindi non sorgono particolari problemi dal punto di vista normativo; si tratta, più semplicemente, di prevedere un raccordo fra tutte queste norme ed adottare ogni misura tesa ad incentivare la collaborazione internazionale.

Tale convenzione è importante, perché paesi che prima non avevano adottato una legislazione di questo tipo (molto spesso le stesse forze di polizia erano ostacolate nel processo di collaborazione con noi, per il fatto che non esistendo la legge non potevamo ottenere dati), ora sono costretti a recepirla. La convenzione è stata firmata anche dagli Stati Uniti, i quali partecipavano insieme al Giappone in qualità di osservatori e hanno seguito molto attentamente il procedere dei lavori. Tuttavia, ricordo che prima dell'11 settembre, essi avevano sollecitato contatti informali da parte nostra, manifestando perplessità riguardo al fatto che noi europei rispettiamo norme molto più severe nell'attività investigativa. Essi, d'altronde, devono fare i conti anche con problemi di natura economica e non va dimenticato che in America il partito dell'economia molto spesso tende a prevalere sugli interessi della sicurezza.

Dopo l'11 settembre, gli Stati Uniti hanno, invece, cambiato completamente atteggiamento. *Internet*, infatti, non viene usato solo dai pedofili. Il fenomeno del riciclaggio, per esempio, è ampiamente favorito dall'uso della rete; più recentemente, Al Qaeda ha dimostrato di saper usare molto bene tale strumento. Quindi, potere investigare in *Internet* in modo più incisivo, avendo a disposizione strumenti giuridici che ci consentano di migliorare la nostra azione dall'interno è un interesse che gli Stati Uniti condividono con noi.

L'altra questione su cui desidero soffermarmi è quella dei dati esterni. Vengono fatte molte eccezioni sulla *privacy*. Il decreto antiterrorismo, approvato recentemente, prevede intercettazioni preventive – in sostanza, queste vengono sempre effettuate sotto il controllo dell'autorità giudiziaria, non al fine di acquisire la prova del reato, bensì allo scopo di scoprire eventuali reati nel campo antiterrorismo – le quali erano state abbandonate nel 1990 e potevano essere compiute soltanto per le associazioni mafiose o per i traffici di armi e di droga. Con il decreto antiterrorismo, esse sono state praticamente ripristinate. Giustamente, si è avuta anche l'accortezza di rendere più celeri le indagini per il tracciamento telematico, oltre che telefonico. Sposando quella che era una tesi della Corte di cassazione in materia – secondo cui erano dati esterni quelli riferiti al traffico telefonico – non è necessario passare per il GIP, ma è pur sempre richiesto un decreto del pubblico ministero per l'esecuzione.

Ritengo che ciò debba essere valido nell'ambito telefonico, dove i dati, per esigenze di fatturazione, vengono conservati anche cinque-dieci anni. Per quanto

riguarda il campo dell'informatica, al contrario, è necessario fare uno sforzo ulteriore, soprattutto quando siamo già in costanza di reato: se, per esempio, viene intercettata per via telematica una minaccia a Bush e si è riusciti a risalire all'IP, al *provider*, questi può rifiutarsi di rispondere alla richiesta di collaborazione se non è stato emanato un decreto del magistrato. Però, gli operatori di polizia non possono incontrare ostacoli simili soltanto per acquisire un indirizzo telematico: è come disporre dell'indirizzo anagrafico. Se per ragioni di servizio, devo verificare, per esempio, l'indirizzo anagrafico di qualcuno, mi reco all'anagrafe, lascio la richiesta scritta, motivandola con ragioni istituzionali e ottengo l'informazione. Allo stesso modo, ritengo debba funzionare nel caso di richiesta di indirizzo telematico, per cui non dovrebbe essere previsto l'ulteriore passaggio dell'autorizzazione dell'autorità giudiziaria, ferma restando la necessità di impedire abusi in tal senso.

PRESIDENTE. Quindi lei è favorevole alla previsione di obblighi a carico dei *provider* ?

DOMENICO VULPIANI, *Dirigente superiore della polizia di Stato, Direttore del servizio della polizia postale e delle comunicazioni.* Sì, deve esserci un obbligo a carico dei *provider* di conservare i dati, ma soprattutto di fornirli senza la richiesta di passaggi superflui. Bisogna superare il passaggio dell'autorizzazione da parte dell'autorità giudiziaria, magari prevedendo che intervenga una successiva ratifica, oppure si potrebbero « congelare » i dati in attesa che arrivi il provvedimento; tuttavia, anche in tal caso, avremmo comunque la necessità di ottenere questi dati prima di poter procedere. Ad esemplificazione di quanto appena detto, cito un caso che si è verificato 20 giorni fa, a Roma: una ragazza in stato di depressione ha inviato una *e-mail* che è stata ricevuta da un anonimo cittadino, nella quale la prima minacciava di suicidarsi. Grazie anche alla collaborazione immediata del *provider* – il quale, prima del decreto antiterrorismo, era scontato che fornisse questi dati – che ci ha fornito il numero telefonico, siamo potuti risalire all'indirizzo della ragazza. Abbiamo inviato una « volante » ed appena in tempo siamo riusciti a salvarla; in questo caso si è trattato di evitare un gesto insano, ma in altre situazioni può darsi che si debba tempestivamente rintracciare il colpevole di qualche messaggio prima che sparisca dal mondo di *Internet*. Non vedo, quindi, perché la richiesta di tali dati, che fino a pochi giorni fa veniva soddisfatta direttamente, possa, adesso, venirci rifiutata dai *provider* in base al decreto antiterrorismo, il quale, d'altronde, vale per le intercettazioni preventive (ed in quest'ultimo caso capisco la necessità di una tutela giudiziaria).

Io però mi riferisco a fattispecie di reato che sono già avvenute e che si collegano ad una determinata persona. In tal caso, ribadisco la necessità per gli organi di polizia, di investigare subito, ferma restando la possibilità, poi, di riferire all'autorità giudiziaria.

Concludo questo mio intervento accennando alla questione del mantenimento dei *file* di *log*, per i quali il termine deve essere di almeno sei mesi; non chiediamo dieci anni, come da più parti sollecitato, anche perché le transazioni in *Internet* sono di mole enorme e non sarebbe possibile, anche materialmente, mantenerli per così lungo tempo: si bloccherebbe il sistema. Il termine di sei mesi, tuttavia, mi sembra ragionevole e richiederebbe solo lievi modifiche di carattere tecnico alle basi di raccolta dati.

In secondo luogo, chiediamo l'accesso immediato ai dati esterni (come ribadito dalla Corte di cassazione), ferma restando l'eventuale ratifica dell'autorizzazione giudiziaria, che può essere informata contemporaneamente, mediante avviso orale, con un'informativa, per esempio, alla procura competente o, ancora, in caso di difficoltà ad individuare quest'ultima, con un informativa successiva alla procura che risulterebbe competente proprio a seguito dell'individuazione sul territorio dell'IP da cui è partito il reato.

PRESIDENTE. Ringrazio il dottor Vulpiani per la sua relazione.

È confortante conoscere i progressi compiuti dalla polizia nel settore delle comunicazioni. I membri della Commissione hanno constatato *in progress* lo sviluppo e l'approfondimento del vostro lavoro.

Lei ritiene utile qualche obbligo normativo per i *provider*, ma la dottoressa Manacorda, invece, affermava l'impossibilità di farlo; tuttavia, ritengo che per l'Italia si potrebbe prevedere.

DOMENICO VULPIANI, *Dirigente superiore della polizia di Stato, Direttore del servizio della polizia postale e delle comunicazioni*. Lo stabilisce anche la convenzione.

PRESIDENTE. Perfetto.

Ho capito che l'intermediazione tra chi inserisce il materiale pornografico e la carta di credito avviene attraverso società di intermediazione, che però sono bancarie.

DOMENICO VULPIANI, *Dirigente superiore della polizia di Stato, Direttore del servizio della polizia postale e delle comunicazioni*. Possono essere bancarie o di natura finanziaria ma molte volte si nascondono. Sulle transazioni finanziarie – per combattere il riciclaggio – esistono norme che obbligano le banca a conservare alcuni dati: bisognerebbe, però, imporre la collaborazione di tipo tecnologico per le transazioni via *Internet* sulle carte di credito.

Abbiamo avuto la collaborazione dei servizi interbancari italiani – anche a livello di VISA europea – per determinate indagini (per noi nuove ed esplorative) e stanno giungendo risultati sul piano investigativo, ma non posso addentrarmi di più per il segreto istruttorio.

Posso dire che un percorso investigativo – nonostante le società di intermediazione bancaria siano quasi tutte allocate all'estero, come i siti –, con la collaborazione di ABI e dei servizi interbancari, si sta avviando e che alcune banche già conservano queste informazioni.

Il problema dei *provider* è costituito dagli accessi liberi e gratuiti, che permettono di non fatturare. Se, però, c'è un interesse economico, per varie ragioni (ad esempio tributarie), i dati sono conservati. L'importante, allora, è garantire velocemente l'accesso alle informazioni degli istituti bancari in caso di reato. Naturalmente, la polizia non vuole sottrarsi a determinate garanzie e non vuole essere un « grande fratello », ma nemmeno vuole esserne condizionata, semmai il contrario !

PRESIDENTE. Ringrazio nuovamente il dottor Vulpiani.

Do ora la parola ai colleghi per i loro interventi.

CARLA MAZZUCA. Ringrazio il dottor Vulpiani per la sua chiarezza e l'esaustività della sua relazione. Il gruppo della Margherita concorda con la necessità di predisporre le opportune modifiche indicate e la sua relazione ci è stata utile per avere quelle informazioni, tecnologicamente corrette, necessarie per non incorrere in errori e all'ottimizzazione degli interventi da effettuare.

La presidente ed alcuni di noi andranno a Yokohama per partecipare alle discussioni riguardanti lo sfruttamento sessuale dei minori, temi contenuti nella convenzione sulla cybercriminalità adottata dal Consiglio d'Europa.

Il mese scorso avevo proposto – non sapendo della convenzione – uno strumento internazionale dello stesso tipo. Infatti, l'articolo 9 della convenzione prevede i reati riferiti alla pornografia infantile, coprendo quelli di sfruttamento sessuale dei minori.

DOMENICO VULPIANI, *Dirigente superiore della polizia di Stato, Direttore del servizio della polizia postale e delle comunicazioni*. Sostanzialmente, ricalca la nostra legge n. 269 del 1998.

CARLA MAZZUCA. Ma non possiamo parlare soltanto della nostra situazione; lei ha dimostrato, infatti, che possiamo essere perfetti nel prevedere norme e reati, ma

molto spesso i crimini non sono compiuti in Italia. È, quindi, molto importante che la convenzione sia firmata dal più ampio numero possibile di paesi e questo potrebbe essere l'obiettivo di un'azione italiana di forte pressione in occasione di questo consesso internazionale, che vedrà probabilmente presenti circa 180 paesi. Sarebbe eccezionale se l'eventuale adozione della convenzione del Consiglio d'Europa avvenisse per un'opera di promozione dell'Italia, senza per questo – naturalmente – impossessarsene.

DOMENICO VULPIANI, *Dirigente superiore della polizia di Stato, Direttore del servizio della polizia postale e delle comunicazioni.* Con il consenso del presidente, vorrei cedere la parola al dottor Staro, che ha partecipato ai lavori della convenzione come membro della delegazione tecnica ed è stato anche testimone della firma dei 29 paesi, durante la cerimonia svoltasi presso il Parlamento ungherese il 23 novembre scorso.

SERGIO STARO, *Vice questore aggiunto della polizia di Stato.* Il 23 novembre 2001, presso il Parlamento di Budapest, c'è stata la cerimonia ufficiale di apertura della sottoscrizione della convenzione.

Lei ha citato – giustamente – dei numeri riguardanti il bacino di utenza dei paesi aderenti al Consiglio d'Europa, che è abbastanza ampio. L'analisi di tali dati dimostra l'importanza di questo strumento pattizio di carattere internazionale.

Vale la pena di sottolineare che quasi tutti i quindici componenti dell'Unione europea hanno sottoscritto l'atto, tranne la Danimarca ed il Lussemburgo. Al blocco europeo si sono aggiunti quattro paesi osservatori (un *record* per le convenzioni del Consiglio d'Europa), rappresentanti i quattro angoli del mondo: Stati Uniti e Canada (padroni della tecnologia nel *cyber space*), Sudafrica e Giappone, a testimonianza della globalità della rete e dei crimini informatici. A questi paesi se ne aggiungeranno altri che presto saranno nell'Unione europea, determinando perciò un contesto internazionale molto forte.

La convenzione (lei richiamava il giusto principio che l'atto sia seguito da strumenti formali di ratifica di un maggiore numero di Stati), però, non introduce per l'Italia principi estremamente innovativi: fortunatamente, siamo rappresentati nel G8 ed abbiamo adottato recenti disposizioni normative, usate come riferimento, tentando poi di andare oltre. Non credo, quindi, che siano estremamente radicali ed innovativi i cambiamenti necessari per la nostra legge, qualora si recepisse l'atto.

I pilastri della convenzione sul *cyber crime* possono essere divisi in tre parti. La prima riguarda l'armonizzazione delle norme di diritto sostanziale; infatti, con la convenzione si stabilisce un cosiddetto minimo comune denominatore giuridico dei *cyber crime*. Si tratta di un grandissimo risultato, perché non tutti i paesi aderenti conoscevano i crimini informatici, così come sono stati delineati attraverso la nostra legge n. 547 ed anche precedentemente. Comunque, la nostra legislazione è parallela ad altre, come la francese, l'inglese o quella degli Stati Uniti.

La seconda parte è costituita dalle disposizioni di diritto processuale, armonizzate soprattutto per la possibilità di accedere ai trattati di mutua assistenza giudiziaria e legale per l'estradizione e la cooperazione tra i giudici al fine di giungere non solo alla reale individuazione del responsabile, ma anche alla possibilità di sostenere un processo. L'importanza di queste misure, richiamate dalla convenzione sul *cyber crime*, è che il *cyber space* è un ambiente globalizzato, senza frontiere e senza confini; per tale motivo è evidentemente necessario sancire il principio dell'inesistenza dei confini fra i paesi – ovviamente – aderenti, qualora sia presente la volontà di combattere contro il crimine informatico.

La terza parte è costituita dal pilastro della cooperazione di polizia. Praticamente, si è constatato che qualsiasi indagine informatica per definizione tecnologica e per ubicazione (il direttore richiamava i concetti di *server* e di dominio, che spesso spostano le indagini cominciate in Italia in altri paesi) successivamente di-

venta transnazionale. La cooperazione, allora, diventa un passo imprescindibile per il buon esito delle indagini, ma anche per la semplice possibilità di continuarle.

Tra le misure necessarie di cooperazione voglio citare solamente la più significativa, congegnata allo scopo di prevedere uno scambio celere di informazioni. La convenzione prevede che tutti paesi aderenti dovranno organizzare degli uffici specialistici in grado di operare ed investigare sui crimini informatici, che saranno dotati di un punto di contatto nazionale per le emergenze provocate da questi crimini.

In Italia il servizio di polizia postale e delle comunicazioni già da tempo ha maturato una sua esperienza all'interno del G8, quali soci fondatori della rete dei punti di contatto sull'*high tech crime*, mentre altri paesi, che ignoravano tale sistema, saranno motivati ad approntare questo ufficio specialistico e ad aderire alla rete; alla fine, si avrà la possibilità di interloquire direttamente in modo celere con i *partner* di altri paesi: qualora tutti paesi del mondo aderissero alla convenzione, realizzeremmo ovviamente il principio dell'abbattimento delle frontiere.

DOMENICO VULPIANI, *Dirigente superiore della polizia di Stato, Direttore del servizio della polizia postale e delle comunicazioni*. Una precisazione sui costi della nostra attività. Il Ministero dell'interno ha investito molto su questa specializzazione, nel quadro dei finanziamenti ripartiti per tutta la sicurezza pubblica, attraverso l'adozione di *hardware* e *software*. Ovviamente, le risorse non sono illimitate e devono tener conto di altre esigenze e di altri uffici investigativi. Quindi, molto importante sarebbe trovare nuove risorse a livello sia italiano sia europeo.

Formare, infatti, un tecnico o un navigatore sotto copertura significa dare una formazione psicologica che opera nella fase preventiva, in quella attiva e dopo la conclusione dell'indagine: la continua visione di tali immagini non può non colpire ed incidere sulla psiche dei nostri agenti. Inoltre, è necessario dotare il personale utilizzato di un'adeguata formazione tecnica per poter « navigare » senza farsi riconoscere. La rete poi deve essere sicura e la banca dati nascosta: si sfruttano le potenzialità di *Internet*, ma se ne deve essere anche protetti, per cui si stanno avviando rapporti con soggetti privati: in cambio di nostri consigli sulla sicurezza, ci danno una formazione gratuita. Tali forme di collaborazione, a cui sono interessate le imprese private per la loro espansione economica, che si compie anche attraverso *Internet*, dovrebbero essere incentivate con convenzioni, appostando risorse anche al di fuori del bilancio dello Stato: la sicurezza informatica attualmente non è più un bene riguardante solo lo Stato.

Per quanto riguarda i costi operativi, fino adesso abbiamo usato i fondi di giustizia, ma non sono illimitati. Le procure, a volte, non hanno la possibilità di avviare un'indagine, se non hanno i fondi necessari: l'affitto di una macchina per compiere intercettazioni telematiche – per esempio – ha un prezzo molto alto e, quindi, si può fare solo per indagini terroristiche e riguardanti la pedofilia. Anche in questo caso si tratta di una questione di selezione di interventi.

Ho contattato una società di intelligenza artificiale per vedere se sia possibile – usando programmi intelligenti – compiere determinate operazioni, che mentalmente non riusciamo più a fare, così da consentire l'eliminazione di ciò che non serve al raggiungimento del nostro fine. Si tratta di esperimenti costosi e le società private lo fanno per le nostre iniziative, ma qualcuno le dovrà pagare.

Sul piano normativo, abbiamo scoperto che esistono immagini alterate, digitalizzate, non reali, ma costruite con il *computer*. Per chiarire, faccio riferimento a quelle pubblicità, ad esempio, in cui le persone camminano sul soffitto, sfidando la legge di gravità. Sono immagini costruite con i *computer* e lo stesso si può fare per i minori, sottoposti ad atti di brutalità e di tortura, che molte volte non sono reali, oppure presenti in cartoni animati a sfondo sessuale. Tali immagini

digitalizzate – probabilmente – potrebbero sfuggire ad una sanzione penale nell'attuale codifica.

Quindi sarebbe opportuno prevedere un adeguamento normativo anche rispetto a queste immagini, introducendo una norma che consenta la nostra azione ed eviti scappatoie a chi afferma che si tratta di immagini digitalizzate, che il bambino non esiste e lo dimostra; magari si tratta di fotografie scattate su una spiaggia a bambini nudi, ricostruite al *computer*, trasformate in immagini che riproducono atti sessuali veri e propri e poi commercializzate. Questo problema potrebbe essere considerato in vista di un'eventuale modifica della legge n. 269 del 1998.

PRESIDENTE. La ringrazio per la sua esposizione che è stata esauriente ed accurata; ritengo che le considerazioni da lei svolte siano molto importanti, in relazione alla verifica dell'attuazione data all'ottima legge n. 269 del 1998.

Ringrazio nuovamente il dottor Vulpiani ed i suoi collaboratori, anche per il lavoro che svolgono: probabilmente, sarà nuovamente richiesta la loro presenza in Commissione.

Dichiaro conclusa l'audizione.

La seduta termina alle 15,15.

IL CONSIGLIERE CAPO DEL SERVIZIO RESOCONTI
ESTENSORE DEL PROCESSO VERBALE
DELLA CAMERA DEI DEPUTATI

DOTT. VINCENZO ARISTA

Licenziato per la stampa
il 14 gennaio 2002.

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

Lire 1000 = € 0,52

Stampato su carta riciclata ecologica

14STC0001330