COMMISSIONE PARLAMENTARE DI INCHIESTA SUI FENOMENI DELLA CONTRAFFAZIONE E DELLA PIRATERIA IN CAMPO COMMERCIALE

RESOCONTO STENOGRAFICO

58.

SEDUTA DI GIOVEDÌ 26 SETTEMBRE 2012

PRESIDENZA DEL VICEPRESIDENTE **LUDOVICO VICO**

INDICE

PAGINA BIANCA

PRESIDENZA DEL VICEPRESIDENTE LUDOVICO VICO

La seduta comincia alle 9,15.

(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 odierna sarà assicurata anche attraverso impianti audiovisivi a circuito chiuso.

Audizione del dottor Antonio Apruzzese, direttore del Servizio Polizia postale e delle comunicazioni.

PRESIDENTE. L'ordine del giorno reca l'audizione del dottor Antonio Apruzzese, direttore del Servizio Polizia postale e delle comunicazioni, il quale è accompagnato dal dottor Carlo Solimene, direttore della Divisione II.

L'audizione odierna si inserisce nel ciclo di approfondimenti che la Commissione sta svolgendo in merito al fenomeno della contraffazione nel settore della pirateria audiovisiva e digitale. Faccio presente ai nostri ospiti che della presente audizione sarà redatto un resoconto stenografico e che, all'occorrenza, i lavori della Commissione possono procedere anche in seduta segreta. Do, quindi, la parola al dottor Apruzzese, che ringrazio ancora della sua presenza.

ANTONIO APRUZZESE, *direttore del Servizio Polizia postale e delle comunicazioni*. Buongiorno a tutti e grazie per l'invito. Siamo fieri e onorati di essere qui e di poter esporre, anche se sommariamente, dal nostro angolo di visuale, cioè dal lato delle Istituzioni che rappresentiamo, il tema in oggetto.

Noi siamo una componente del Ministero dell'interno nell'ambito della Polizia di Stato, con il compito istituzionale, pressoché esclusivo, di contrastare i fenomeni illeciti riguardanti l'utilizzo dei sistemi di telecomunicazione più moderni, ossia Internet e le reti.

Si tratta di un campo che va espandendosi ad una velocità prodigiosa e che stiamo seguendo sempre più da vicino, nel senso che si va verso un'amplificazione sempre più forte della quantità dei contenuti da sottoporre a controllo e visione, aumentando, al contempo, la complessità dei problemi connessi a tale situazione, a fronte dello sviluppo non solo quantitativo ma anche qualitativo delle relative problematiche.

Tutti i fenomeni criminali classici – se così possiamo definirli – si stanno progressivamente trasferendo: è in atto una trasmigrazione epocale verso questo nuovo universo, che ci sta coinvolgendo sempre di più. Stanno nascendo nuove forme di criminalità, assolutamente sconosciute in passato, che presentano alcune caratteristiche che erano prima del tutto ignote al mondo del crimine e del malaffare.

Vi è la possibilità di avere contatti in istantanea, senza alcuna limitazione temporale o spaziale, ossia in tempo reale e senza alcun confine, nonché di creare, in tempi brevissimi, vincoli associativi criminali di qualunque ampiezza, superando ogni schema di confine e di giurisdizione

– questo è un aspetto fondamentale – potendo contare soprattutto sull'anonimato dei contatti.

Il contatto per via digitale consente, infatti, l'anonimizzazione del soggetto da cui si viene contattati, il che ha rappresentato un'altra svolta radicale in questo mondo criminale (per esempio, ciò ha dato la stura a nuove forme di affiliazione, sempre più forti ed ampie, basate proprio sull'anonimizzazione). Nell'ambito delle organizzazioni criminali classiche – si pensi alla mafia e alla 'ndrangheta – ci siamo sempre interrogati sulla possibilità di aggredire tali organizzazioni attraverso meccanismi di « infiltrazione », cioè tramite l'utilizzo dei cosiddetti pentiti. Si è discusso a lungo sulla maggiore permeabilità della mafia siciliana rispetto, per esempio, alla 'ndrangheta calabrese, perché quest'ultima, puntando e contando prevalentemente sul rapporto familiare, se non proprio di sangue, dei diversi affiliati, rendeva praticamente impossibile insinuarsi o sgretolare la struttura omertosa dell'associazione. Un maggiore spiraglio, invece, è stato riscontrato nell'ambito della mafia siciliana, più improntata a schemi richiamanti una struttura « imprenditoriale ». In tale contesto, c'è stata, dunque, la possibilità di agire, come ampiamente dimostrato dalle vicende giudiziarie degli ultimi decenni.

Con l'avvento delle nuove organizzazioni criminali si sta creando una « terza » forma di aggregazione di vincolo criminale, basato veramente sull'anonimizzazione, perché manca la conoscenza fisica dei soggetti. Si tratta di soggetti che si conoscono, si connettono e si frequentano nell'etere – parlavamo prima di « fisicizzazione » delle presenze – ma che, molto spesso, non si conoscono fisicamente. Questo è un aspetto fondamentale e definitivo del nuovo assetto che si sta creando.

Si aggiunga, poi, un altro aspetto, ossia l'espansione enorme, sempre più impensabile, dell'utilizzo della rete Internet e dei soggetti che vi fanno capo. Quando uso il termine impensabile, alludo a un anno fa: già un anno fa non saremmo stati in grado di prevedere ciò che sta succedendo oggi.

Bisogna passare ad alcuni esempi concreti per rendere l'idea delle manifestazioni che spiegano l'esplosione del fenomeno generale. Si pensi a due aspetti, uno « fisico », o meglio, parlando in termini di informatica, di *hardware*, un altro un po' meno fisico. A proposito dell'aspetto fisico, la rivoluzione degli ultimi mesi mostra che il mondo della rete e dell'informatica si sta letteralmente spostando. C'è una trasmigrazione dal mondo dei *computers* veri e propri a quello dei *mobiles* e dei cosiddetti *smartphones*.

È dell'altro ieri la notizia secondo cui, per la prima volta, è stato segnato il momento del sorpasso del volume di traffico da SMS – che ormai la nostra generazione, bene o male, era arrivata a padroneggiare – da parte dell'utilizzo totale delle *mail*, non più inviate da casa attraverso il *computer*, bensì da apparati mobili. Si stima che, in media, ci possano essere due o tre apparati per ogni italiano, per non parlare delle schede telefoniche che li fanno funzionare. Comprenderete benissimo, quindi, che i numeri si dilatano enormemente.

A questo aspetto prettamente « meccanico », fisico, si aggiunge un'altra rivoluzione che ha sovvertito completamente il mondo di Internet, nonché il nostro modo di affrontare queste tematiche e problematiche. Noi ci siamo arrivati, per esempio, con il discorso della pedopornografia, di cui il dottor Solimene è un profondo conoscitore perché tratta specificamente questo delicatissimo problema.

Il problema della pedopornografia, fino ad alcuni anni fa, era concentrato sui siti: i cosiddetti siti pedopornografici. Il legislatore italiano è riuscito a varare delle norme che tutti ci invidiano, introducendo il principio delle *blacklist*, con le quali siamo riusciti a superare un ostacolo che sembrava insormontabile. Finché i siti pedopornografici erano in Italia, potevamo giocare con il nostro sistema giudiziario e quindi chiuderli o oscurarli. Il problema, però, sorgeva quando i siti, come più spesso avviene, erano all'estero. In tal caso, dovevamo andare a chiedere

ad altri ma non sempre le giurisdizioni erano combinate, ciò creando una serie di problemi enormi.

Si è dunque introdotto un principio rivoluzionario, che l'Italia, per prima fra tutti, ha adottato come norma. È stata varata, infatti, una legge che consente di obbligare tutti i *providers* italiani a non fare entrare nel circuito italiano le immagini di questi siti. Fornendo una spiegazione un po' più tecnica: se ci si connette dall'Italia e si vuole entrare nel sito australiano, si deve passare attraverso il *provider* italiano, che poi indirizza all'altro. Il *provider* italiano ha però l'obbligo di non far andare l'utente su tale sito: è il cosiddetto sistema della *blacklist*, mediante oscuramento (sto facendo cenno a questi concetti perché vi sono dei forti richiami al meccanismo inerente alla discussione che dobbiamo affrontare oggi).

Ricordo bene quando l'allora Ministro dell'interno ci introdusse a questa normativa, avvertendoci del fatto che il legislatore ci aveva messo in mano uno strumento fortissimo, che non aveva eguali nel mondo, invitandoci ad utilizzarlo con la massima attenzione. Lascio a tutti voi comprendere in quale delicatissimo meccanismo ci si era addentrati: uno strumento estremamente delicato.

A questo panorama si aggiunga, nell'evoluzione del fenomeno, il fatto che è subentrata la rivoluzione della rivoluzione: mentre dai siti si è passati alle *chat* – anche in quell'ambito abbiamo faticato non poco per affrontare i fenomeni di pedopornografia –, oggi siamo arrivati al discorso sui *social networks*, che hanno significato la rivoluzione della rivoluzione.

Si tratta di un altro Internet. Molto francamente, ormai, il meccanismo delle *blacklist* continua ad essere utilizzato, ma i nostri ragazzi non « girano » più sui siti, bensì sui *social networks*, che sono un'evoluzione di Internet.

Oggi si parla tanto, per esempio, della problematica del *cloud computing*. Una delle rivoluzioni del domani annunciate riguarda la possibilità di non conservare più enormi contenuti multimediali sui nostri *computers*, bensì di mandarli su una « nuvola » lontana, cioè su un *server* lontano magari mille miglia. Questa, che sembra una rivoluzione copernicana e di là da venire, in realtà, con i *social networks* è stata già realizzata. Come ripeto, i nostri ragazzi sono i primi ad aver afferrato immediatamente tale concetto rivoluzionario. Quando si parla di *Facebook* o di *Twitter*, in realtà, questi sono diventati nuvole, basi, magazzini enormi di dati. Credo che chiunque abbia dei figli a casa, vedendoli quotidianamente, perennemente attaccati a questi *social networks* sappia tutto ciò. Ormai, i nostri ragazzi vanno in giro con degli apparati per cui non devono più restare fisicamente a casa, quindi, noi stessi abbiamo minori possibilità di controllare che cosa fanno: essi stanno connessi in ogni momento, sono capaci di parlarti e, mentre parlano, di guardare il loro aggeggio. In quel momento, però, essi entrano nelle varie banche dati e « girano » per tutto il mondo.

Questo è il panorama in cui ci si muove oggi: un panorama che, ogni giorno, porta ad innovazioni che non sono prevedibili e questa è l'assoluta novità di questo fenomeno, che è in perenne evoluzione.

Ovviamente, le problematiche che riguardano la contraffazione, la pirateria, la violazione dei princìpi di base che regolano la tutela del diritto d'autore, sono fortemente toccate da tutta questa nuova strumentazione, da questo nuovo mondo che sta bussando in maniera sempre più continua alle nostre porte, che ci invade sempre di più con sorprese e scoperte sempre nuove.

Nella nostra attività di presidio, contrasto e controllo di questo mondo estremamente complesso, ci troviamo ad essere – non ho esitazioni a definirci in questo modo – alla stregua di testimoni di fronte a queste nuove forme di illecito che riguardano il diritto d'autore e la contraffazione in generale.

Qual è grossomodo la situazione, lo stato dell'arte? Fondamentalmente, si tratta di una tematica di difficilissima regolamentazione, perché anche in questo campo andiamo a cozzare – parlo per

estrema sintesi – contro il problema di fondo delle giurisdizioni. Il fenomeno in esame non è – non può tecnicamente essere e sempre meno sarà – in tutto il suo contesto un fenomeno solo italiano, quindi sottoposto solo alla giurisdizione, alla legge e alla potestà sanzionatoria e normativa della nazione Italia. Ciò crea dei problemi enormi, perché si fa molto presto a pensare di vietare, chiudere ed agire, quando poi, tecnicamente e fisicamente, per andare a chiudere o ad oscurare un sito che si trova in un altro Stato, bisogna chiedere tutto ciò alle autorità di quello Stato. Vi è, dunque, questa problematica.

È inutile aggiungere che esiste una normativa, che è stata approntata ormai da alcuni anni, innestata sulla vecchissima norma – mi pare che risalga al 1941 – in tema di tutela del diritto d'autore, la quale è stata di volta in volta novellata prevedendo alcune fenomenologie nuove.

In effetti, c'è stato un primo ritocco che ha riguardato il diritto d'autore classico, ossia la divulgazione, la riproduzione e la vendita di prodotti coperti dal diritto d'autore anche per via multimediale e digitale. Parliamo dei casi delle tecnologie connesse alla produzione musicale (che è poi quella che più colpisce l'immaginario collettivo), di quella video e di quella del *software* (quindi, dei programmi che fanno girare i *computers*).

È stato quindi introdotto dal nostro legislatore un principio che regola la punibilità di queste condotte, che consiste nel subordinare ogni ipotesi punitiva al famoso « fine di lucro ». Non spetta certamente a me ricordare il motivo di questa clausola, che è intervenuta a seguito di alcune pronunce della Corte di Cassazione: è una fenomenologia estremamente complessa e complicata. Si scontrano, infatti, due interessi contrapposti: da un lato, quelli delle grandi *major*, cioè delle grandi aziende mondiali che gestiscono il mondo della produzione di questi contenuti: dall'altro, gli interessi degli utenti. Ovviamente, in tale quadro di interessi c'è anche una fortissima componente italiana, per esempio da parte dell'industria dell'editoria e del mondo musicale, che cerca di far valere i suoi sacrosanti diritti e di tutelare – forse – anche la ragion d'essere di alcune aziende.

Noi siamo parte organica della Commissione tecnica presso il dipartimento dell'editoria (presso la Presidenza del Consiglio), che si occupa del contrasto della pirateria digitale e, quindi, siamo stati testimoni del grido d'allarme che ci è arrivato da questi soggetti, i quali ci hanno fatto comprendere che se le cose continueranno così, potrebbero esserci fortissime ripercussioni sulla vita stessa, per esempio, di molte aziende italiane, che sopravvivono grazie al settore musicale. Ci sono, insomma, fortissimi interessi in gioco.

D'altro canto, c'è poi la realtà cui facevo cenno prima, cioè quella di Internet e dei sistemi di diffusione e divulgazione di questi prodotti, una realtà legata al modo in cui avviene l'accesso da parte del pubblico ai medesimi. Sappiamo tutti bene che la maggior parte dei fruitori di tali prodotti sono giovani, i quali ormai hanno perso – verifichiamo ciò nella nostra attività quotidiana – la consapevolezza non tanto dell'illiceità di ciò che stanno facendo, bensì del fatto stesso che, nel momento in cui si va a prendere un film o una canzone, scaricandoli e poi ricaricandoli sul proprio iPad o iPod, si acquisisce un disco, che dovrebbe invece trovarsi presso la bacheca di un negozio, oppure un libro che, analogamente, dovrebbe essere in vendita nelle librerie. Questo è uno dei punti fondamentali del discorso.

Peraltro, comprendo benissimo le difficoltà di contemperare, a livello normativo, questi due contrapposti interessi: andare ad emanare norme di forte criminalizzazione, per esempio stabilendo che sia punibile chiunque scarica una canzone, così, su due piedi, significherebbe avviare indagini, inchieste e processi penali dirompenti su un pubblico che, forse, non si rende neanche conto di ciò che sta facendo. Questa, purtroppo, è una delle realtà.

La portata della norma del 1941 è stata, successivamente, espansa un po'. È stata infatti aggiornata con la previsione della duplicazione del *software*, nonché di quelle attività che servono, per esempio, a rimuovere gli ostacoli tecnici che il produttore pone per evitare fenomeni di ruberie digitali. Si pensi ai videogiochi che i ragazzi utilizzano più frequentemente e che sono coperti da criteri tecnici di criptazione. A tale riguardo, i nostri ragazzi utilizzano ormai il termine di « craccare », per eludere tali criteri tecnici: essi hanno imparato benissimo come si fa. Anche tale fenomeno, comunque, è punito.

Analogamente, è stato introdotto un altro aspetto riguardante la diffusione, per esempio, di programmi televisivi a pagamento (se prima questo era un fenomeno marginale, adesso sta diventando sempre più ampio). Se prima si trattava di un aspetto molto limitato, oggi non è più così: basti pensare alla possibilità di accedere alla maggior parte degli avvenimenti sportivi nazionali e mondiali, che è subordinata alla possibilità di accedere a circuiti di diffusione televisiva a pagamento. Tali circuiti, ovviamente, per potersi assicurare una logica forma di introito, devono avere un meccanismo di copertura, ossia i sistemi di criptazione dei programmi televisivi. Citando un nome commerciale – non per fare pubblicità – basti pensare a Sky. Esiste una normativa che punisce questi fenomeni e, con particolare riferimento a quanto ho appena detto, su questo specifico fronte siamo impegnati in maniera molto forte, essendo riusciti ad introdurre alcuni paletti. Questi sono gli aspetti fondamentali.

Concludendo il discorso sull'analisi di carattere globale, un altro riferimento indispensabile va fatto alla situazione attuale: che cosa bolle in pentola ? Nella Commissione presso la Presidenza del Consiglio dei ministri si è capito che uno dei sistemi, una delle forme di aggressione di questo tipo di illecito, più che andare a colpire gli innumerevoli terminali, cioè la diffusione capillare – quindi, i fruitori finali, cioè i ragazzini che vanno a scaricare – consiste nell'intervenire sulle cosiddette – chiamiamole con il loro nome tecnico – piattaforme multimediali, sulle quali sono fisicamente allocati i prodotti multimediali, cui tutti i ragazzi attingono (continuo a parlare di ragazzi, perché sono loro i principali fruitori).

Per esempio, ci sono stati alcuni tentativi, anche in ambito europeo, da parte di altri Stati – per esempio, la Francia – di trovare scorciatoie molto forti, imponendo o tentando di imporre – poi c'è stata una marcia indietro – ai famosi *providers* di prestare collaborazioni attive agli organismi istituzionali, chiedendo loro di fornire le coordinate di tutte le piattaforme e degli accessi che venivano presso di esse effettuati: è come imporre, da domani, a Telecom di comunicare tutti gli accessi che passano attraverso il proprio sistema e che vengono effettuati presso una delle più comuni piattaforme di *file sharing* – così le chiamano tecnicamente i ragazzi – cioè veri e propri banchi virtuali in cui si vanno a prendere i film o le canzoni. Effettuata tale operazione, si rileva poi una lista di indirizzi informatici, si va a casa del soggetto e lo si accusa, il giorno tale, di aver scaricato un determinato film. Di qui, si parte poi con i procedimenti sanzionatori.

Questa è l'esperienza che hanno provato ad attuare i francesi e che hanno provato ad introdurre anche in America e in Germania. Gli esperimenti, però, non hanno avuto gran seguito.

In Italia questa strada non è mai stata intrapresa, anche perché occorrerebbe poi armonizzarla con le normative in tema di *privacy*. È indubbio, infatti, che quando parliamo della divulgazione di questo tipo di dati, andiamo a toccare anche altri interessi diretti delle persone, quindi, il diritto stesso alla riservatezza.

Il cammino italiano, di cui siamo stati spettatori diretti nell'ambito della Commissione presso la Presidenza del Consiglio, è stato quello di tentare di avviare una prima fase conciliativa con i *providers* e, poi, una fase più impositiva, più coercitiva. Se un produttore di musica – porto un esempio banalissimo – scopre che c'è una piattaforma in Italia sulla quale ven-

gono collocate canzoni che vengono vendute o cedute gratis, si muove prima costui come privato, intentando un'ingiunzione tramite il Garante delle comunicazioni e chiedendo che tale contenuto venga rimosso. Nel caso in cui il *provider* non ottemperi, si potrà chiedere, quindi, un provvedimento coercitivo, sempre tramite l'Agcom, che blocchi e inibisca i transiti telematici.

PRESIDENTE. Temporalmente che cosa accade ?

ANTONIO APRUZZESE, *direttore del Servizio Polizia postale e delle comunicazioni*. Non parliamo neanche di progetti, bensì di idee e spunti che sono ancora oggetto di valutazione. Il problema vero è che, finché parliamo dell'Italia, il discorso può passare. In altre parole, si può concretamente pensare ad una soluzione di questo genere, con il meccanismo dell'ingiunzione e, in caso di inottemperanza, della procedura sanzionatoria sul soggetto italiano. Il discorso è diverso quando siamo all'estero: che cosa succede ? Poiché siamo all'estero nel 90 per cento dei casi, qui si apre una grande pagina. Si è compreso che non è possibile mandare ingiunzioni all'estero, così è stata lanciata l'idea – aggiungo che si tratta di lavori in corso – da qualcuno, nel caso di non ottemperanza all'estero, di ricorrere all'arma « atomica » (così la chiamo io), cioè quella di cui parlavo prima a proposito di pedopornografia: la *blacklist*. Questa è un'arma atomica: se parliamo del mondo della comunicazione, è un'arma atomica. Dobbiamo stare attentissimi (abbiamo l'esempio dalla Cina e dei Paesi arabi, dove ci si sveglia la mattina e si decide che, magari da domani, su Internet non entra più nessuno, oppure che si chiudono dieci finestre). Queste sono le poste in gioco oggi, questo è lo stato dell'arte sul piano di ciò che sta maturando.

Avrei in mente di concludere con un riferimento ad alcune situazioni, per poi magari lasciare spazio alle domande. Se, però, ci fossero subito richieste di intervento, posso fermarmi.

PRESIDENTE. Prosegua pure.

ANTONIO APRUZZESE, *direttore del Servizio Polizia postale e delle comunicazioni*. Questa è, dunque, la complessa situazione di oggi, che è oggetto di esame e di valutazione. Sono valutazioni che comportano riflessioni molto profonde, perché vanno a toccare tematiche, interessi e diritti delicatissimi che, soprattutto, ci impongono di affrontare un mondo nuovo, al quale, sinceramente, siamo decisamente poco abituati. Si tratta di scenari che si sono aperti all'improvviso e che ci hanno trasportato e proiettato in un mondo diverso. Chiunque vanti, per esempio, una formazione giuridica classica, di fronte a queste nuove problematiche che si stanno prefigurando vacilla veramente.

Poiché finora abbiamo parlato di aspetti legati, più o meno, a ciò che si deve fare per agire sul fenomeno, svolgo un accenno concreto ad un'attività che ci sta vedendo fortemente interessati e che riguarda, da un lato, la prevenzione e, dall'altro, la repressione. La nostra attività, infatti, consiste di due momenti: un momento di intervento, quando il guaio è provocato, e un momento in cui si cerca di evitare che il guaio venga provocato.

L'aspetto repressivo e alcuni contenuti molto positivi che stanno emergendo riguardano il sistema delle televisioni che si avvalgono di sistemi di criptazione. Quando abbiamo cominciato, ci sembrava di lavorare su una nicchia, su un fenomeno minimo. Adesso, ci stiamo accorgendo invece che è un fenomeno esteso: si parla apertamente di concorrenza tra Sky e la RAI, per comprenderci. C'è un mercato enorme, con realtà veramente consistenti. Poiché, però, in questo caso siamo completamente nel mondo della rete, di Internet, ci siamo dovuti spremere le meningi per arrivare a formulare alcune idee, che poi si sono tramutate in strumenti investigativi pratici.

I sistemi televisivi criptati sono basati sull'invio di trasmissioni televisive criptate, cui vengono applicate codici informatici che occorre conoscere: serve, insomma, una « chiave » per aprire il pacchetto che

ci invia Sky. Si tratta di un pacchetto con un codice informatico. Tutto è basato sull'informatica. Tuttavia, abbiamo scoperto che ci sono vere e proprie organizzazioni criminali che intercettano questi codici, se ne appropriano e, tramite un sofisticatissimo sistema, li cedono in forma commerciale a terzi, proponendo l'analogo « pacchetto » a costi estremamente ridotti rispetto a quelli reali, quindi, offrendo la possibilità di eludere i sistemi di criptazione. Si è creato un vero e proprio mercato, su cui siamo potuti intervenire. Il sistema è sofisticatissimo ed è talmente strutturato da prevedere due opzioni: la possibilità di potere avere un *decoder*, cioè un apparecchio fisico a casa, o di ricevere, via Internet dall'organizzazione, le « chiavi » per poter combinare i dati ed accedere ai servizi offerti. In che modo si fa tutto ciò ? Di certo, non lo si fa *una tantum*, nel senso che si entra oggi nell'apparato e poi è tutto concluso. Gli organizzatori hanno la possibilità di concedere accessi limitati e temporanei, ragion per cui possono permettere all'utente di vedere una partita o due, per un giorno o due giorni, nonché di stipulare abbonamenti annuali. È tutto un discorso che gira sull'informatica.

Effettuando una complessa attività – la primavera scorsa abbiamo trascorso tutte le sere in cui c'erano le partite della cosiddetta Coppa dei campioni – io sono ancora abituato a chiamarla così – a lavorare. In quelle giornate, infatti, si aveva il maggior traffico nell'utilizzo di questi sistemi di trasmissione televisiva criptata e, studiando tali flussi di traffico, siamo riusciti ad individuare alcune centrali da cui venivano diramati i relativi segnali. Abbiamo cominciato a sporgere denunce e ad aprire indagini in alcuni grandi centri italiani, sia al Nord, sia al Sud, ottenendo ottimi risultati. Nell'arco di due anni siamo arrivati ben oltre le centinaia di denunce, tuttavia, non andiamo a denunciare – svolgo una precisazione doverosa –, non si va a « sparare » con il fucile addosso a chi compra il servizio, il quale, poi, magari, sarà responsabile forse civilmente, con un altro tipo di sanzione. In realtà, andiamo a perseguire penalmente chi fa di tutto ciò un'attività di lucro organizzato, cioè un'attività criminale, perché si crea un sistema di ruberia organizzata, di malaffare, di crimine vero e proprio. Questo è ciò che di concreto siamo riusciti a produrre. Si tratta di una strada su cui stiamo andando avanti con l'appoggio di tutte le società interessate.

L'altro aspetto, il più importante di tutti, è quello che riguarda la prevenzione. In merito, vi devo una piccola e ultima spiegazione, perché la prevenzione è l'aspetto che rende di più. Andare a lavorare sui guai causati è sempre faticoso e costoso, mentre cercare di prevenire è senz'altro meglio.

Dal momento che i fruitori di questi sistemi, quelli che vengono ad affrontare questo mondo, sono i giovani, abbiamo da tempo avviato un discorso sistematico con vari Ministeri (con quello dell'istruzione, con l'allora Ministro per la gioventù) attraverso contatti standardizzati e istituzionalizzati con le realtà giovanili, soprattutto nelle scuole e con le scuole. All'inizio, eravamo partiti con le problematiche di uso di Internet sicuro, per difendere i ragazzi dai pericoli che ci sono sul *web*, essendo quindi orientati verso le realtà più conosciute, per esempio, quelle riguardanti gli abusi sui minori, cioè quelle situazioni di fatto più preoccupanti.

Tuttavia, ciò ha rappresentato per noi una palestra fondamentale, perché ci ha consentito di compiere una grande scoperta, proprio in materia di comunicazione. Abbiamo visto, piuttosto casualmente, che riuscivamo ad ottenere risultati sorprendenti in termini di contatto e dialogo con i ragazzi laddove impiegavamo i nostri agenti più giovani, mandandoli ad avere i contatti direttamente con loro.

All'inizio, eravamo noi funzionari ad andare nelle scuole, ma io stesso mi sono accorto prestissimo che si ripeteva la forma di contatto che tutti noi abbiamo con i nostri figli. Quando, infatti, c'è un certo *gap* generazionale, è molto più difficile fare presa. Quando, invece, mandiamo il ragazzo ventenne, la musica cambia. Ho personalmente assistito, al-

cune volte da dietro le quinte, a questi contatti con i ragazzi e mentre quando ci siamo trovati noi a chiedere loro se mai fossero andati di nascosto su *Facebook* e se si fossero creati un falso profilo, nessuno si alzava o parlava, quando invece, andava il nostro ragazzo a spiegare loro i vari giochini possibili su *Facebook*, si sono aperte le quinte ed è stata una rivoluzione. È stata una rivoluzione che poi ci ha consentito di far passare, attraverso un canale che ormai si era aperto, numerosi messaggi. Purtroppo, ci stiamo facendo carico dell'inoltro di messaggi relativi alla cosiddetta educazione alla legalità. A margine e al di là delle problematiche di abuso e di pericolo (penso a quando ammoniamo i ragazzi a non attraversare la strada, altrimenti si possono far male), stiamo cominciando a spiegare a questi ragazzi tutta la questione, facendogliela comunicare dai loro « coetanei », o da chi è più vicino a loro in termini di età: loro guardano al « maghetto », il quale però spiega loro anche a quali rischi si va incontro andando a scaricare un film.

Ci sono anche alcune realtà che possono, forse, aiutare molto da questo punto di vista, per esempio, laddove si riescono a creare meccanismi standardizzati di accesso ai prodotti, introducendo anche alcuni princìpi. Su alcuni contenuti multimediali esiste già questa previsione. Non per parlare in termini commerciali, ma *I-Tunes* dispone di alcune applicazioni che consentono di accedere a contenuti musicali a bassissimo prezzo: ci si scarica la canzone pagando. Si tratta di pagamenti minimi, però, ciò è importante perché si educano i ragazzi al principio che si sta andando a prendere qualcosa che appartiene ad altri. È un lavoro duro, ma essendo un lavoro rivolto al terminale, cioè all'utenza, speriamo che possa essere una strada per l'avvenire, per il domani. Ho così esaurito il quadro di insieme. Vi ringrazio per l'attenzione e sono a disposizione per ogni chiarimento.

PRESIDENTE. La ringraziamo noi per la sua illustrazione. Do la parola ai colleghi che intendono intervenire per porre quesiti o formulare osservazioni.

GIOVANNI SANGA. Direttore, la ringrazio per il contributo che ci ha fornito. Dopo il suo intervento mi sento un po' più disarmato di prima, nel senso che non mi sento più troppo rassicurato (ovviamente, ciò non dipende da lei). La mia è solo una constatazione. Ormai, dobbiamo renderci conto del fatto che gli strumenti legislativi sono del tutto inadeguati all'evoluzione della tecnologia. La riflessione che volevo svolgere riguarda il quadro che lei ci presenta oggi, ma che non sappiamo quale sarà nei prossimi anni, posto che in questo settore il cambiamento, l'evoluzione corrono molto di più rispetto agli altri settori della quotidianità e della vita, con tutti i riflessi che ciò comporta anche sul piano che più ci interessa per quanto riguarda gli aspetti commerciali, delle irregolarità, della violazione dei diritti d'autore e della contraffazione.

La mia considerazione, quindi, è che se dobbiamo certamente proseguire sulla via tracciata, cercando di recuperare tutti gli sforzi possibili per fornire alcune risposte, tuttavia, realisticamente, potremo agire in piccoli segmenti: siamo di fronte ad un mondo ormai talmente variegato e universale su cui ritengo che difficilmente riusciremo ad incidere in modo più significativo.

DEBORAH BERGAMINI. Vorrei porre due domande. La mia considerazione di partenza si riallaccia a quanto affermava poc'anzi il collega Sanga. Se c'è un ambito nel quale i tradizionali « ritardi » della legislazione, rispetto alle necessità e alle urgenze, diventano macroscopici, è proprio quello dello sviluppo della criminalità nella rete, non solo perché questo è un fenomeno che si evolve con una rapidità che non penso abbia precedenti nella storia della modernità, ma anche perché, a differenza di altri ambiti, il fenomeno mette addirittura in questione il ruolo che deve avere lo Stato con le sue Istituzioni. Esiste, infatti, un dibattito mondiale – immagino che lo sappiate – che ha pro-

vocato uno scontro vero e proprio tra chi ritiene che la rete debba crescere liberamente e non debba minimamente, a rischio di effettuare censure di qualunque tipo, essere toccata dalle leggi dello Stato e chi, invece, sostiene che dobbiamo regolare tale realtà, altrimenti Internet diventerà una discarica dei peggiori vizi dell'umanità, ciò sancendone il suo stesso fallimento. Questo è un tema sul quale ogni riflessione non penso sia mai sufficiente. Passo ora alle mie due domande.

La prima domanda si riferisce alla sicurezza della rete. Nella Commissione trasporti della Camera, di cui faccio parte, stiamo svolgendo un'indagine sulla sicurezza informatica delle reti e abbiamo raccolto informazioni a dire poco allarmanti. Esiste, infatti, un fenomeno recente che ci preoccupa moltissimo: quello dei *virus* dormienti: in totale liceità io acquisto un *computer*, senza sapere che al suo interno c'è un *virus* dormiente, il quale, a un certo punto, si attiva – sto schematizzando – trasformandomi, a mia insaputa, in un *hacker* o comunque in un diffusore di reati nella rete. Si tratta di un meccanismo virale pericolosissimo che, secondo le letture che ho svolto, mi sembra sia particolarmente sviluppato in Cina (ancora una volta, la Cina è un Paese del quale ci occupiamo molto in questa Commissione).

Il fenomeno pone, ovviamente, anche alcune questioni che riguardano i profili di legge. Se, infatti, sono inconsapevole del fatto che attraverso il mio *computer* sto svolgendo una funzione virale che produce un reato, come posso difendermi ed essere difeso ?

La seconda domanda è la seguente: secondo lei, dottor Apruzzese, perché l'Italia è nella *watch list*, insieme – se non sbaglio – alla Gran Bretagna, per quanto riguarda l'utilizzazione illecita di materiale coperto dal diritto d'autore ? È una questione culturale, di leggi che non sono sufficienti o, forse, di una disciplina sul diritto d'autore che non è attuale ? In quest'ultimo caso, mi è difficile pensare ciò dal momento che stiamo parlando di un fenomeno globale. Vorrei capire perché non riusciamo ad arginare questo fenomeno: perché siamo uno dei Paesi che scarica di più in modo illecito nonostante le forti campagne di sensibilizzazione ?

LUCIANO ROSSI. Ringrazio il dottor Apruzzese per la sua presenza. Nell'associarmi alle domande che la collega Bergamini le ha posto, una curiosità mi sorge spontanea. Nella struttura, nell'amministrazione, vi sentite attenzionati come merita un tema tanto delicato ? Strumenti, mezzi, formazione sono assicurati alla vostra azione, oppure registrate qualche ritardo, come spesso accade, nell'ambito di queste situazioni che, certamente, come la collega Bergamini ricordava poco fa, ci vedono impegnati sempre in momenti di gravità estrema ?

PRESIDENTE. Se non ci sono altri interventi da parte dei colleghi, vorrei formulare anche io alcune domande. Nel caso di indagine, se i *servers* e le sedi legali sono posizionati all'estero, soprattutto in Paesi non comunitari, quali sono i margini del vostro agire ?

Inoltre, qual è il livello di cooperazione tra le forze di polizia ? Lei dà per scontato che esiste quella europea, ma si tratta di capire come si comporta quella extraeuropea: quale possibilità avete di intercettare le cosiddette comunicazioni postali – passatemi il termine – sul modello di *Skype* ?

Infine, il vostro lavoro e la vostra esperienza ci consentono di essere ricettori in questo momento anche di suggerimenti legislativi, urgenti o a medio termine, che impegnerebbero maggiormente questa Commissione per la natura dell'indagine che sta svolgendo. Vorrei ascoltare la sua opinione in merito a ciò. Do quindi la parola al nostro ospite per la sua replica.

ANTONIO APRUZZESE, *direttore del Servizio Polizia postale e delle comunicazioni*. Penso che l'argomento che unifica tutte le questioni che sono state poste sia la problematica riguardante la cooperazione, che è determinante e fondamentale in questo contesto, perché – mi riconnetto

alle questioni sollevate all'avvio della discussione – questo è un mondo che ci ha posto davanti alla necessità urgente ed immediata di rivedere e riconsiderare tutti i nostri criteri e concetti di rapporti tra Stati, quindi, anche di cooperazione sia in termini giudiziari, sia di aiuti di polizia.

Cerco di rispondere alle varie domande poste. Cominciando dall'onorevole Sanga, il quadro normativo che ho tracciato è un dato di fatto. Ho fatto cenno anche a ciò che bolle in pentola e non ancora a livello normativo o di produzione normativa vera e propria. Noi abbiamo la sensazione che si stia ancora riflettendo molto proprio sugli atteggiamenti da assumere e da tradurre in norme. Penso che l'operazione più difficile in questo campo consista nel trovare il giusto punto di contemperamento tra i contrapposti interessi: è un tema delicatissimo. Mentre è facile pensare di punire, per esempio, il furto di energia elettrica, perché si tratta di un dato più o meno condiviso da tutti, quando ci sono sotto interessi delicati, come in questa storia, le scelte sono molto difficili.

Si aggiunga che il quadro di valutazione, il quadro da cui trarre gli elementi di decisione e su cui si deve andare ad intervenire, è in continuo rimodellamento, quindi, le scelte non sono facili.

La cooperazione internazionale è decisiva, ma non è ancora al massimo: sicuramente, non è al passo con lo sviluppo della cooperazione internazionale criminale. Le organizzazioni criminali, oggi, sono tutte transnazionali. Oggi, è questo lo schema classico di organizzazione criminale. Oggi, si attaccano i *computers* per sottrarre dati sensibili, tra cui i dati riguardanti l'identità digitale, per avere la possibilità di entrare nei conti bancari e via dicendo. Per far ciò, c'è bisogno di una complessa filiera, nella quale vi è chi fabbrica i *virus* informatici, chi li diffonde, chi li produce, chi li commercia, chi li distribuisce in un dato modo. Vi è poi l'organizzazione di coloro che devono utilizzare tali strumenti per andare a rubare il denaro. Poi, c'è l'altra fase, ancora più complessa per le organizzazioni criminali, cioè quella della monetizzazione, perché questi sistemi consentono di rubare soldi virtuali, ma poi i soldi devono essere trasformati in denaro reale.

Per esempio, sappiamo ormai tutti per comune esperienza che i più migliori produttori e inventori di *virus* sono in Russia e in Cina. È una notizia quasi conclamata. Russi e cinesi producono questi *virus* e poi ci sono organizzazioni, per esempio russe o di altri Paesi dell'Est europeo, che si occupano della distribuzione sul territorio mondiale, quindi, anche di quello italiano.

C'è infine il bisogno di creare una rete nei diversi Paesi in cui si va a colpire, poniamo l'Italia, perché si devono monetizzare concretamente i denari. Per tale scopo, occorre fare ricorso a manovalanza locale, che deve andare ad attivare carte prepagate intestate a personaggi compiacenti, quindi, creando dei meccanismi di monetizzazione, oppure appoggiandosi ai circuiti di *transfer* internazionale, come Western Union o Money Transfer, i quali consentono di trasferire all'estero le somme di denaro concrete e materialmente introitate.

Si tratta di vere e proprie organizzazioni transnazionali, che vengono allestite e create in un battibaleno, proprio perché si utilizza Internet. Pertanto, quando andiamo a parlare di meccanismo sanzionatorio, vi è il bisogno che io mi capisca subito – non tanto in senso linguistico, quanto sul piano operativo –, per esempio, con il collega di Mosca: il giudice italiano deve avere un appoggio dal giudice di Mosca e contemporaneamente da quello di Bucarest.

Siamo di fronte a delle rivoluzioni a cui il nostro sistema non era assolutamente preparato. Si stanno creando dei circuiti di magistrati specializzati, dei canali particolari tra magistrati. Con alcuni Paesi abbiamo affinato contatti forti e creato un punto di contatto internazionale, proprio presso il nostro ufficio, per questo tipo di crimine, riuscendo a stabilire un contatto diretto, che è aperto sempre, con 54-56 nazioni. Siamo partiti dall'ambito del G8 e ci siamo allargati, però, sono attività che richiedono uno sforzo enorme. Il problema

è che poi bisogna sempre confrontarsi con realtà che non sono più le nostre, con mondi diversi, quindi, con la necessità di introdurre la possibilità di comprendersi e di condividere con altre realtà istituzionali di Stato alcuni princìpi, compresi quelli in materia di contraffazione e di pirateria. È questo il vero nocciolo del problema.

In risposta all'onorevole Bergamini, tratto ora il problema dei *virus* dormienti e quello della *blacklist*. Noi siamo stati in Commissione trasporti per sottoporre alcune problematiche e criticità riguardanti la sicurezza delle reti. Quello dei *virus* dormienti è un problema enorme, vero e reale, ma è anche connesso a un'altra diavoleria – mi si perdoni il termine – che noi tecnicamente definiamo un po' come la peste del secolo: il *botnet*, un acronimo anglosassone che sta per *robot network*, un nome che sta diventando tristemente famoso.

In realtà, i *virus* dormienti generano un altro fenomeno: quando il *virus* dormiente si è attivato nel suo *computer*, tale *computer* non è più governabile da lei, bensì da qualcun altro. Se io riesco a mandare questo *virus* in cento, duecento, mille *computers*, come organizzazione criminale posso gestire cinquanta, cento, mille, un milione di *computers* senza che tutti i proprietari di quei *computers* lo sappiano o se ne accorgano. A prescindere dalla pericolosità, un'unica macchina informatica con mille terminali può diventare più potente dei più potenti calcolatori ed elaboratori oggi in uso. Per esempio, se questa macchina decidesse un giorno di connettersi al sito *x*, tale sito si sbriciolerebbe (giusto per capire di che cosa può essere capace una macchina di questo genere).

Al di là di questo, la questione genera delle problematiche enormi perché, a livello investigativo, quando scopriamo il malfatto, l'indagine mi porta ad un determinato *computer*. Comprendere che il malcapitato proprietario del *computer* non c'entra nulla, porta a dovere avviare un discorso giuridico completamente diverso, immaginando altre soluzioni. Infatti, Inevitabilmente, a casa sua, poi, la polizia arriva con un mandato di perquisizione. Adesso, stiamo cominciando a variare completamente il nostro tiro e a pensare anche a forme nuove di contatto con colui che, teoricamente, potrebbe non essere un reo, chiedendone la collaborazione spontanea. Si pensa, cioè, ad avvertire il soggetto del fatto che una strana strada porta proprio a casa sua e a domandare il permesso per l'accesso al suo *computer*, evitando la perquisizione cruda. Come ripeto, però, è un *work in progress* e stiamo cercando, giorno per giorno, di inventarci questi percorsi.

La problematica della *blacklist* è estesa al mondo della contraffazione e della pirateria. Per essere ancora più concreti, ribadisco un esempio tratto dalla realtà. Se c'è una piattaforma digitale su cui vi è del materiale audiovisivo in violazione del diritto d'autore cui attingono utenti e clienti italiani, applicando la normativa all'eccesso e portandola alle estreme conseguenze, dovremmo poter imporre a tutti i *providers* italiani di non consentire che, dall'Italia, ci si possa connettere a quel dato *provider*. Si tratta, però, di scelte forti, anche per un'altra ragione, posto che si farebbe passare il principio della possibilità di limitare determinare tipi di attività. Da ciò nasce il problema epocale che lei poneva: lasciamo la rete com'è o interveniamo ? Mentre si è raggiunto un *general agreement* in materia di tematiche delicatissime, come la pedopornografia, su cui anche i cinesi adesso ci forniscono delle risposte, perché l'abuso dei ragazzi, facendo riferimento ai diritti classici, è un discorso che riguarda il diritto naturale, su altre tematiche la concordanza non è chiarissima.

Riguardo al rapporto tra noi e le Istituzioni e al fatto di sentirci o meno coperti, risponderei tranquillamente in senso affermativo, anche perché il Parlamento italiano ci ha fornito e ci fornisce un appoggio straordinario, nel senso che ci offre un canale proprio di aiuto finanziario per questo tipo di attività e, quindi, per l'acquisto del materiale, che è fondamentale per noi.

Il nostro problema vero è che, ormai, il nostro sguardo va oltre la realtà nazionale: il nostro problema non sta nel rapporto col Ministero dell'interno. Quando devo parlare con il collega rumeno, devo capire in che lingua parlargli. Ciò vale non solo per noi, ma anche per i magistrati. Questa è l'amara realtà di oggi.

Tornando ora alla domanda che mi poneva il presidente, ossia alla stabilità o meno di *Skype* e ai sistemi criptati di fonia o che girano su sistemi di base dati. Premesso che tutto ciò che riguarda questo fenomeno ci vede interessati come ufficiali di polizia giudiziaria, quindi, nell'ambito dell'attività giudiziaria ordinaria, coordinata e disciplinata dall'autorità giudiziaria, l'unica in Italia che può intervenire in materia di comunicazioni a livello di intercettazione, al momento non è possibile tecnicamente svolgere quel tipo di intercettazioni. *Skype* è stata un po' la scoperta vincente di tutti: ci consente di effettuare telefonate gratis, in quanto consente di far transitare il traffico di fonia attraverso un sistema di scambio dati su Internet. Per poter effettuare queste telefonate si deve possedere una connessione Internet e ciò deve valere sia per chi compie, sia per chi riceve la telefonata.

In realtà, trasferiamo i dati di telefonia su un canale di dati. Tale canale di dati è gestito da alcune società – *Skype* è una di queste – che, però, impiegano sistemi multipli di criptazione e di inoltro dei dati. Poiché sono società non italiane, al momento, non è possibile accedervi. Questa è una risposta estremamente tecnica.

PRESIDENTE. La ringraziamo moltissimo, dottore. Il contributo che ci ha reso è importantissimo per la nuova fase del lavoro della Commissione. Io mi permetto di affermare che non escludo, d'accordo con i commissari, di risentirla ancora, eventualmente anche sulla base di alcuni quesiti precisi, al fine di ottenere altre informazioni. Ad un certo punto della sua esposizione, invece del verbo « ricollegare », lei ha usato l'espressione « riconnettersi », con ciò rendendo precisamente il senso del lavoro che svolge.

Nel ringraziarla di nuovo, dichiaro conclusa l'audizione.

La seduta termina alle 10,25.

IL CONSIGLIERE CAPO DEL SERVIZIO RESOCONTI ESTENSORE DEL PROCESSO VERBALE

DOTT. VALENTINO FRANCONI

Licenziato per la stampa il 4 dicembre 2012.

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

PAGINA BIANCA

€ 1,00

16STC0021490