COMMISSIONE PARLAMENTARE PER L'INFANZIA

RESOCONTO STENOGRAFICO

INDAGINE CONOSCITIVA

5.

SEDUTA DI GIOVEDÌ 6 NOVEMBRE 2008

PRESIDENZA DEL PRESIDENTE **ALESSANDRA MUSSOLINI**

INDI

DEL VICEPRESIDENTE **GABRIELLA CARLUCCI**

INDICE

PAG.

Sulla pubblicità dei lavori:

Mussolini Alessandra, *Presidente* 3

INDAGINE CONOSCITIVA SULLA TUTELA DEI MINORI NEI MEZZI DI COMUNICAZIONE

Audizione del professor Gianluigi Me, rappresentante del Dipartimento della sicurezza nei sistemi informatici dell'università di Tor Vergata e consulente della Commissione europea per il *Safer internet class:*

Mussolini Alessandra, *Presidente* 3, 6, 8

Carlucci Gabriella, *Presidente* 6, 7, 8, 10

Di Giuseppe Anita (IdV) 8, 10

Me Gianluigi, *Rappresentante del Dipartimento della sicurezza nei sistemi informatici dell'università di Tor Vergata e consulente della Commissione europea per il* Safer internet class 3, 6, 7, 9, 10

PAGINA BIANCA

PRESIDENZA DEL PRESIDENTE ALESSANDRA MUSSOLINI

La seduta comincia alle 9,40.

(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 odierna sarà assicurata anche mediante l'attivazione di impianti audiovisivi a circuito chiuso.

(Così rimane stabilito).

Audizione del professor Gianluigi Me, rappresentante del Dipartimento della sicurezza nei sistemi informatici dell'università di Tor Vergata e consulente della Commissione europea per il *Safer internet class*.

PRESIDENTE. L'ordine del giorno reca, nell'ambito dell'indagine conoscitiva sulla tutela dei minori nei mezzi di comunicazione, l'audizione del professor ingegner Gianluigi Me, rappresentante del Dipartimento della sicurezza nei sistemi informatici dell'università di Tor Vergata e consulente della Commissione europea per il *Safer internet class*.

Do la parola al professor Me.

GIANLUIGI ME, *Rappresentante del Dipartimento della sicurezza nei sistemi informatici dell'università di Tor Vergata e consulente della Commissione europea per il* Safer internet class. Buongiorno a tutti. Il progetto che vi presenterò è diventato un prodotto informatico destinato sì al mercato, ma finalizzato soprattutto ad aiutare i genitori, il cui *gap* tecnologico rispetto ai bambini va sempre più ampliandosi.

Il progetto nasce con una sinergia diversa rispetto a ciò che di solito si riscontra, in ambito accademico o in ambito industriale, perché ad esso collabora una onlus, ECPAT Italia *(End child prostitution, pornography and trafficking)* che ne costituisce il cardine perché i due *partner,* il Consiglio nazionale delle ricerche e l'università di Tor Vergata, avevano bisogno della presenza concreta di un soggetto di elevata competenza in materia, in grado di comprendere gli attuali problemi dei bambini e dei genitori, e nonché livello di conoscenza da parte di questi ultimi del fenomeno che andremo a trattare.

ECPAT ha dunque svolto un ruolo molto importante per adattare con precisione lo strumento alle attuali esigenze dei suoi fruitori.

Il fenomeno di cui parlo sono gli *instant messaging* e i *social network*. *Instant messaging* è una tecnologia che consente alle persone di comunicare in tempo reale attraverso il computer, indipendentemente dal sistema operativo adoperato *(Windows, Linux o Macintosh)* ovvero utilizzando *Skype,* il primo programma che ha consentito di effettuare telefonate gratuitamente.

Microsoft è il più importante e il più diffuso produttore di applicazioni per *instant messaging,* e copre oltre il 90 per cento del mercato.

L'*instant messaging* è un'applicazione che si apre sul proprio computer, come *Word,* o come i programmi di navigazione – *Internet explorer,* ad esempio – che, a

differenza di questi, consente alle persone di mettersi in comunicazione fra di loro, scambiandosi opinioni e informazioni. Questo nuovo modo di interpretare *internet* ha esercitato una particolare attrazione sugli adolescenti, perché è quello che utilizzano con più facilità e più creatività, per scambiarsi opinioni su ogni argomento.

Più avanti vi mostrerò alcune delle principali minacce cui si può andare incontro con l'*instant messaging*. Questa applicazione, che consente a due o più persone di comunicare via *internet*, è strettamente collegata, dal punto di vista concettuale, al fenomeno delle *social networks*, « reti sociali » che servono a condividere interessi, idee e opinioni e soprattutto a placare la voglia di protagonismo di chi desidera pubblicizzarsi su *internet*.

Sebbene questi due fenomeni siano assolutamente distinti dal punto di vista tecnologico, in alcune ipotesi criminose appaiono in realtà strettamente collegati, perché la *social network* permette di socializzare e l'*instant messaging* consente invece di astrarsi da questa rete sociale e di iniziare a comunicare direttamente, come quando si fa conoscenza in discoteca e poi si va a parlare fuori, in privato. In questo modo viene a costituirsi una sorta di « filiera » del crimine.

Partecipo a questa audizione in veste di docente dell'università di Tor Vergata e non ho voluto far aggiungere, nella mia presentazione, un altro mio titolo: sono maggiore dei Carabinieri, responsabile dei corsi di *cyber-crime;* la mia relazione parla di una filiera del crimine, e deriva soprattutto dalla mia esperienza di carabiniere (ma oggi non sono qui in questa veste).

Il problema è che il *social network* e l'*instant messaging* vengono utilizzati nell'assenza, da parte dei genitori, di una competenza nel controllare cosa facciano i bambini sulla rete. Ci sono moltissimi casi di bambini vittime di ricatto, del cosiddetto *grooming*, ovvero di violenza sessuale, con conseguenti denunce alla polizia giudiziaria; abbiamo diversi esempi, il *carnet* è decisamente nutrito. Questa filiera può anche condurre ad altri esiti come il bullismo *on-line*, la pornografia, i contenuti violenti, eccetera.

Ci siamo concentrati su *Windows live Messenger* perché è l'applicazione di messaggistica istantanea più importante. Vorrei darvi alcuni esempi di quanto sia facile, in questa filiera di *social network e instant messaging*, perdersi o subire dei danni alla propria persona o carriera. Anche gli adulti che desiderano apparire su *internet* pubblicano molto spesso dati relativi alla propria *privacy*, che frequentemente vengono memorizzati da aziende interessate al loro *recruitment*, cioè ad un eventuale ingaggio, prima ancora che l'interessato abbia tenuto un colloquio. Se dunque gli adulti non sono in grado di gestire in sicurezza i *social network* e gli *instant messaging*, ci si può rendere conto di quale minaccia questi strumenti possano costituire per gli adolescenti.

Vi riporto un altro esempio che riguarda proprio degli adolescenti. Una signora inglese, circa un anno fa, aveva avuto contezza del fatto che il figlio avesse degli scambi poco chiari con alcune persone attraverso *instant messaging*. La signora, le cui conoscenze tecnologiche erano abbastanza avanzate anche se non professionistiche, grazie all'installazione di un *software* sul computer del figlio tredicenne, è riuscita a far catturare il pedofilo, un americano residente dall'altra parte dell'oceano. Questo *software* si chiama *Keylogger;* non mi dilungo a parlarne, ma è una piccola parte di ciò che abbiamo fatto noi. Grazie a questo *software* e alla collaborazione della polizia inglese e americana, quell'uomo adesso è stato fortunatamente assicurato alla giustizia.

Questo strumento è dunque un ausilio utile per capire qual è, per così dire, la seconda metà della realtà del bambino, ossia, quella che può essere controllata a vista è la realtà di tutti i giorni, e infatti si chiede al bambino chi sono gli amici con cui esce; quella che non può essere con-

trollata a vista è la realtà virtuale, e questo *software* fornisce un aiuto per poterla controllare meglio.

Ho portato alcuni estratti di un'indagine condotta nel febbraio 2008 da *Save the children* insieme alla Doxa. Nei fascicoli che vi ho consegnato stamane ho riportato un'altra indagine, datata maggio 2008 e fatta da Microsoft e Nextplora. Vi illustro soltanto la prima perché ha una grafica migliore, ma entrambe dicono le stesse cose, e i numeri sono sostanzialmente analoghi.

Vi mostro questi numeri per darvi contezza della natura dei dati che i bambini, o meglio, gli adolescenti, forniscono in *instant messaging*. Ad esempio, molti ragazzi inseriscono i propri dati anagrafici veri e non uno pseudonimo e addirittura il 3,2 per cento inserisce il proprio numero di telefono cellulare, cercando dunque sostanzialmente un contatto reale.

Vorrei focalizzare l'attenzione su un punto preciso, ovvero la foto fatta con gli amici, che, insieme alla foto personale, viene utilizzata spesso per attivare un contatto personale, e che spesso è l'amo che innesca la commissione di un crimine non ancora previsto in Italia e che in Gran Bretagna è chiamato *grooming*.

Il *grooming* è una tecnica di manipolazione psicologica per cui l'abusante, o il potenziale abusante, cerca di collezionare il maggior numero di foto per arrivare ad una situazione di predominio strategico sul bambino o sull'adolescente e poterlo poi ricattare, senza il timore che faccia ricorso ai genitori o alla polizia giudiziaria.

Come potete vedere dai dati, il fenomeno non è trascurabile e, soprattutto, è fortemente asimmetrico, perché da una parte c'è un adolescente che, in certo qual modo si dimostra del tutto ingenuo in quanto fornisce dati autentici; dall'altra c'è l'abusante, che ha la certezza di conservare l'anonimato nei suoi confronti. Questa forte asimmetria è in qualche maniera peggiorata dal fatto che gli adolescenti credono di poter utilizzare questa tecnologia in piena consapevolezza. In realtà, sebbene si dimostrino piuttosto scaltri nell'uso delle varie funzioni del *software*, non riescono a percepire le minacce che ne possono derivare.

Oltre a stare in contatto con gli amici, si può riscontrare una forte spinta a utilizzare queste tecnologie per fare nuove conoscenze e trascorrere il tempo con loro. Situazioni queste ad elevato rischio. Va precisato che il nostro discorso concerne l'aspetto criminale della vicenda; vi è anche una sfera, su cui non ho competenza, di carattere educativo, nel senso che i bambini possono contattare persone che, pur non avendo intenzioni violente, hanno magari idee non condivisibili, che sfuggono al controllo dei genitori, privi delle necessarie cognizioni tecniche. Alcune delle relazioni che vengono realmente allacciate terminano con l'incontro, che è una delle cose più pericolose che possano accadere, soprattutto per gli adolescenti.

Ritorno sul fenomeno del *grooming*, per fare una precisazione. Nella stragrande maggioranza dei casi, soprattutto negli ultimi due anni, il potenziale abusante non è un adulto ma un adolescente più grande, ad esempio un diciassettenne nei confronti di un tredicenne. Il problema, quindi, non si ha soltanto dalla parte della vittima ma anche dalla parte del potenziale abusante, nel senso che, se il *groomer* ha solo 16 anni, la tutela giuridica del minore impone alcuni obblighi.

Abbiamo dunque cercato di mostrare quali siano le dimensioni e i « colori » del problema che abbiamo affrontato.

Aggiungo che *instant messaging* è altresì un vettore di attacco per i sistemi informatici, nel senso che i virus e i *worm* sono molto diffusi in questo ambiente. Pertanto, un superiore controllo di questo strumento consentirebbe non solo di vigilare sulla « realtà virtuale », ma anche di prevenire eventuali attacchi e minacce al computer.

Il modo più sicuro per fare utilizzare questi strumenti ai bambini o agli adolescenti è quello di farlo accompagnati dai genitori che garantisce piena consapevolezza e responsabilizzazione sull'uti-

lizzo del mezzo. Tuttavia, la presenza dei genitori ha senso se hanno qualcosa da insegnare o hanno almeno la stessa padronanza dello strumento, altrimenti la semplice presenza non è molto utile ed è poco pratica perché, se da un lato non possiamo creare un bambino *digital divided*, cioè che non sa utilizzare determinate tecnologie, dall'altro non possiamo pretendere che la famiglia stia tutto il giorno in compagnia del bambino che naviga. È un sistema poco pratico e difficilmente si trova un *trade off*. O meglio: il *trade off* in questo caso ricade in uno di quei punti rossi di cui ho parlato nella relazione e che sono tutti punti di pericolo. I filtri, poi, in questi casi non servono proprio.

Responsabilizzare il minore varia da caso a caso. Lasciare il minore da solo durante l'attività in *internet*, incosciente dei pericoli, è ciò che avviene più di frequente ed è una cosa molto pericolosa.

PRESIDENTE. Quindi non ci si salva.

GIANLUIGI ME, *Rappresentante del Dipartimento della sicurezza nei sistemi informatici dell'università di Tor Vergata e consulente della Commissione europea per il* Safer internet class. Le strategie adottate fino ad ora sono state di impartire *awareness* a genitori e figli, cioè consapevolezza.

I frutti di queste azioni, però, si vedono non dopo tre o sei mesi, ma dopo diversi anni, considerando anche che la tecnologia marcia più in fretta rispetto a queste iniziative.

La Commissione europea ha stanziato dieci giorni fa 55 milioni di euro per il triennio 2009-2011, per finanziare progetti di questo tipo. Sulla dispensa sono riportati gli indirizzi di alcuni siti di interesse, per mostrare la centralità del problema anche in sede europea.

Il nostro obiettivo è di consentire ai genitori di controllare l'attività su *Windows live Messenger*. Questo *software*, è stato fatto in modo tale che sia completo, cioè che possa raccogliere tutte le informazioni scambiate; soprattutto, deve essere semplice, nel senso che noi ci rivolgiamo a persone che non hanno un buon rapporto con la tecnologia, quindi l'interfaccia deve essere assolutamente semplice e intuitiva.

Abbiamo avuto per questo aspetto un grande sostegno da ECPAT, perché ha sostenitori di tutte le età per cui abbiamo potuto constatare che il programma era abbastanza intuitivo anche per persone di 75-80 anni.

Il programma, quindi, deve essere adattabile alle esigenze di controllo del genitore: questo vuol dire che se io non voglio che mio figlio parli con un altro bambino o con un'altra persona, posso semplicemente spingere un tasto e se mio figlio parla con la persona che a me non piace, nel momento in cui lancio il *software* la prima cosa che fa è presentarmi tutti gli eventi per i quali ho chiesto di ricevere un allarme. Ad esempio, mi dice che mio figlio alla data ora ha parlato con questo tizio e che si sono detti queste cose.

Il programma è proattivo nel senso che la sua attività consiste nel presentare gli oggetti che il genitore ritiene di maggiore interesse; è rapido, perché lo abbiamo progettato in modo tale che in tre *click* al massimo si raggiunge l'informazione desiderata ed è accessibile remotamente e in tempo reale. Questo significa che se il bambino naviga con *Windows live Messenger* e parla con i suoi amici, nel momento in cui finisce e chiude il programma, al genitore, ovunque si trovi nel mondo, basta una connessione ad *internet* e un PC – o uno *smartphone* – per essere in grado di accedere ai contenuti della *chat* in tempo reale, cioè in circa 5-10 minuti.

GABRIELLA CARLUCCI. Come avviene la connessione ? Il genitore a cosa si deve collegare ?

GIANLUIGI ME, *Rappresentante del Dipartimento della sicurezza nei sistemi informatici dell'università di Tor Vergata e consulente della Commissione europea per il* Safer internet class. Il genitore apre

semplicemente la finestra del proprio *Virtual Parent,* che può essere caricato su una chiavetta USB, un oggetto che oggi è molto diffuso, lo scarica in un *laptop* e apre l'applicazione. Ha un prezzo estremamente popolare e accessibile a tutti. È sufficiente aprire l'applicazione perché lei sa già dove andare, cosa andare a vedere e cosa scaricare.

GABRIELLA CARLUCCI. Ci vuole solo la chiavetta.

GIANLUIGI ME, *Rappresentante del Dipartimento della sicurezza nei sistemi informatici dell'università di Tor Vergata e consulente della Commissione europea per il* Safer internet class. Serve soltanto la chiavetta con il *software* caricato; poi il genitore, da qualsiasi computer, da qualsiasi parte del mondo si può collegare. Questo può essere fatto anche a computer *target,* ovvero a computer spento, perché il programma sposta i dati da un'altra parte. Questa caratteristica consente anche di scindere l'attività di navigazione dall'attività di controllo. Uno dei problemi che abbiamo esaminato prima è il fatto che i genitori dovrebbero stare accanto ai loro figli durante la navigazione; in questo modo, invece, i ragazzi possono navigare da soli ma, in realtà, non sono soli, perché c'è un *Virtual Parent,* cioè un genitore virtuale che li controlla.

Questa non è la sede ideale per spiegare come funziona il programma, perché sarebbe un discorso troppo tecnico. Questo *software* segue in maniera nascosta la navigazione, registra tutta l'attività su MSN, ricostruisce e organizza i dati, identifica le situazioni tendenzialmente sospette e presenta in modo semplice e flessibile le informazioni. Inoltre, consente la consultazione remota locale con una semplice interfaccia.

Una domanda che spesso mi viene posta riguarda la legalità di questo tipo di controllo. Se sia giusto o meno farlo, dipende solamente dal genitore; la cosa importante è capire che l'interferenza nella vita privata del figlio di minore età è indispensabile per la tutela della sua integrità fisica e morale. Nel momento in cui si verifica una minaccia a questa integrità, il nostro ordinamento giuridico consente ai genitori di interferire e di intromettersi nella corrispondenza privata, mentre in ogni altra ipotesi si applica l'articolo 616 del codice penale. Da questo punto di vista, si può dare assolutamente una rassicurazione sulla sua legalità.

È evidente – ma questo è assolutamente ancillare rispetto a questa discussione – che io con questo *software* posso fare di tutto, posso controllare il bambino, ma anche chiunque altro. È evidente che la legittimità di questo *software* sta nel suo utilizzo, nel senso che chi lo usa deve essere consapevole di quello che sta facendo.

Virtual Parent non è un filtro, e non vuole censurare l'attività di un minore. Attualmente, tutte le strategie finora utilizzate sono state di censura. John Gilmore, uno dei padri fondatori di *internet*, già trent'anni fa diceva che la comunità di *internet* percepisce la censura come una minaccia e perciò la aggira, e questo è quello che regolarmente avviene.

Il nostro prodotto non censura niente; l'unica cosa che vogliamo fare è dare visibilità a ciò che accade. È proattivo, flessibile, *real time*, completo, utilizzabile nuovamente e adatto all'uso per un pubblico non esperto.

Vi mostro alcuni *screenshot* per darvi l'idea di come appaiono, ad esempio, i cartellini dei contatti. L'*alert box* è il segnale di allerta di cui parlavo prima, che avvisa che si sono verificati degli eventi da segnalare. Questa è una vista temporale, sequenziale, e queste sono tutte le varie viste proprio per fare in modo che entro tre *click* tutti abbiano l'informazione voluta. Poi ci sono delle funzioni statistiche, in modo che si possa capire anche che tipo di uso si fa di questo oggetto: se si scarica prevalentemente musica, se si scaricano video, se si parla soltanto, ed è utile anche per capire la natura della conversazione.

Concludendo, *Virtual Parent* è rivolto ai genitori con poca familiarità con *Windows*

live Messenger e con poco tempo a disposizione. Non sostituisce assolutamente l'attività di educazione, ma è uno strumento di supporto per l'educazione dei minori ad un comportamento consapevole su *internet*.

Chiudo con una frase di Seneca: « Non esiste vento favorevole per il marinaio che non sa dove andare ». Pertanto, non aspettiamoci che *Virtual Parent* sostituisca l'attività del genitore: sicuramente la può aiutare, e molto, ma chi decide dell'educazione del figlio è il genitore e non un *software*.

PRESIDENTE. Noi abbiamo fatto tante audizioni sul problema dell'allarme globalizzato nei sistemi di comunicazione interconnessi e sull'estrema tecnicalità che possiedono i nostri ragazzi rispetto agli adulti: senza parlare di settantenni, in questo campo anche i quarantenni sono alcune volte poco esperti. Abbiamo visto che soprattutto le donne usano *Messenger,* mostrando le proprie foto.

Io mi auguro che ci si possa incontrare nuovamente per favorire, magari organizzando una conferenza stampa, la diffusione del *software Virtual Parent*, una realtà virtuale – in effetti non così virtuale, dato che è come se ci fosse un tutore che, tuttavia, non può in nessun caso sostituire il genitore – che costituisce uno strumento a libera scelta, che si può o meno utilizzare per tentare di avere maggiore consapevolezza e controllo del *mare magnum* di comportamenti pericolosi che provengono addirittura dagli stessi adolescenti; non è solo l'adulto il mostro che raggiunge i bambini, ma gli stessi adolescenti possono in certi casi essere gli adescatori.

Inoltre, il *grooming* è inserito all'interno della modifica della legge contro la pedofilia e se ne sta discutendo in Commissione giustizia alla Camera. Io mi auguro che si possano fornire ai genitori non solo le conoscenze sui progressi della tecnologia del computer, ma anche gli strumenti in grado di fronteggiare e controllare questi sistemi.

ANITA DI GIUSEPPE. Desidero ringraziare il professore Gianluigi Me. Ritengo che le audizioni siano veramente utili perché ci consentono di conoscere meglio i fatti. Ringrazio Dio di avere figli grandi perché, oltre a un mondo reale che è tanto difficile da vivere, adesso si aggiunge anche il mondo virtuale.

Le chiedo se questo *software* sia stato promosso, cioè quanti genitori ne conoscano l'esistenza. Finalmente c'è qualcosa che può contrastare il problema e può vigilare sui nostri ragazzi, ma quanti genitori ne sono a conoscenza ?

PRESIDENZA DEL VICEPRESIDENTE GABRIELLA CARLUCCI

PRESIDENTE. Desidero intromettermi in questa discussione perché noi, maggioranza e opposizione, dobbiamo fare uno sforzo per far conoscere questi strumenti.

Non so se le persone che erano presenti ieri si sono rese conto non solo dell'importanza delle informazioni, ma anche della mole di lavoro raccolta dalla Società di pediatria e della devastante influenza dei *media*, in particolare della pubblicità e della televisione, sui nostri figli.

Questi sono documenti che circolano da tempo. Io, che mi occupo di questo problema perché lo sento un problema della nostra società – perché i nostri figli sono la società del futuro – credo che si debba attivare l'attenzione della gente, in particolare dei genitori, con tutti i mezzi possibili in particolare attraverso i *media*.

Di qui a poco presenteremo gli atti, in conferenza stampa e tutti i documenti che abbiamo raccolto nell'ambito di questa indagine conoscitiva. Presenteremo anche questo strumento che abbiamo a disposizione: non ci sono leggi che possano obbligare i genitori a comperare il *Virtual Parent,* però è uno strumento che dobbiamo divulgare e mettere a disposizione dei genitori, farlo conoscere attraverso tutti i canali possibili della comunicazione, perché riguarda problemi ormai conosciuti da tutti.

Il problema dell'adescamento attraverso *internet* è noto a tutti; la polizia

postale, la Guardia di finanza e i Carabinieri da anni lavorano su questo tema, oltre al fatto che certi messaggi che vengono scambiati, al di là di essere attrattivi per i pedofili, spesso sono fuorvianti e distorsivi della realtà.

Noi ci troviamo di fronte a una generazione di ragazzi che vivono spesso in un mondo virtuale, non solo per opera della televisione, ma anche per quello che vedono in *internet* o che si scambiano con il cellulare, per cui bisogna controllare in continuazione quale sia il loro vero rapporto con la realtà e spiegare loro che determinate cose non si possono fare.

Di qui a poco audiremo anche la società AESVI (Associazione editori software videoludico italiana), società italiana che controlla i videogiochi e che ha portato in Europa le istanze dell'Italia sulla modifica del PEGI *(Pan-European Game Information)*, che è un sistema di controllo e di classificazione dei videogiochi. Gli italiani hanno dimostrato la maggior sensibilità verso il problema dell'utilizzo di videogiochi non adatti ai bambini, che invece vengono tranquillamente venduti loro. Si tratta di videogiochi vietati ai minori di diciotto anni, che circolano e vengono venduti a bambini molto più piccoli e che, anche in quel caso, oltre ad avere un contenuto violento, hanno anche un contenuto distorsivo della realtà.

Pertanto, come maggioranza ma anche come opposizione, in maniera *bipartisan* in questo Parlamento e in questa Commissione, dobbiamo fare uno sforzo per attivare tutti i canali della comunicazione su questo problema. Mi auguro che lo si faccia e rivolgo il mio invito a tutte le forze di questa Commissione affinché ci si attivi in tal senso.

Oggi non erano presenti molte persone, ma gli atti di questa nostra audizione restano. Vi chiediamo di farci avere anche la presentazione video su supporto informatico, in modo che rimanga agli atti della Commissione infanzia e che i genitori o i deputati più attivi del punto di vista tecnologico la possano vedere nel medesimo formato che ci è stato mostrato oggi.

Ribadisco la nostra precisa volontà non solo di divulgare le informazioni, ma anche di dare seguito, con concrete proposte di legge, a tutto quello che abbiamo appreso in questa audizione.

GIANLUIGI ME, *Rappresentante del Dipartimento della sicurezza nei sistemi informatici dell'università di Tor Vergata e consulente della Commissione europea per il* Safer internet class. Concordo in pieno con l'onorevole Carlucci. La mia impressione, ovvero di colui che osserva il fenomeno e che, purtroppo, ha dovuto anche mettere le mani su computer che contengono cose veramente orribili, è che non ci sia sufficiente conoscenza e consapevolezza del problema.

Faccio un esempio banale: nella lista delle raccomandazioni che una mamma fa a suo figlio, che più o meno sono sempre le stesse, non se ne trova una su questi temi. Questo, secondo me, non è indice di una scarsa attenzione dei genitori al problema, ma di una loro scarsa consapevolezza dei pericoli che possono scaturire dall'uso di certi strumenti.

Abbiamo parlato di crimine, ma vi assicuro che su *Messenger* molti adolescenti si scambiano informazioni che riguardano anche il piccolo spaccio o che non hanno niente a che vedere con la violenza, ma che comunque è utile che un genitore conosca per capire che cosa il proprio figlio stia facendo.

Spesso gli adolescenti, soprattutto quelli più furbi, percorrono questi territori proprio perché sanno che lì non sono molto controllabili. Il problema è che i genitori non recepiscono che questo rappresenta quello che noi chiamiamo tecnicamente canale subliminale, cioè un canale che non si vede ma che esiste e permette una comunicazione molto nascosta e abbastanza sicura.

A mio avviso, un'azione positiva consiste proprio nell'*awareness*: bisogna dire chiaramente ai genitori che i problemi possono essere molto gravi e che loro non controllano abbastanza.

ANITA DI GIUSEPPE. Molti magari non controllano perché non sanno usare il PC.

GIANLUIGI ME, *Rappresentante del Dipartimento della sicurezza nei sistemi informatici dell'università di Tor Vergata e consulente della Commissione europea per il* Safer internet class. La mia esperienza mi porta ad affermare che molti non si rendono neanche conto del problema, nel senso che confondono *internet* con il *web,* la pornografia con la pedofilia: in questo mostruoso « minestrone », si sentono in qualche modo al sicuro, mentre non è affatto così.

PRESIDENTE. Ringrazio il professore Gianluigi Me e dichiaro conclusa l'audizione.

La seduta termina alle 10,20.

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

DOTT. GUGLIELMO ROMANO

Licenziato per la stampa
il 17 dicembre 2008.

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

PAGINA BIANCA

€ 0,35

Stampato su carta riciclata ecologica



16STC0001610