PRESIDENZA DEL PRESIDENTE MARIO VALDUCCI

La seduta comincia alle 14,40.

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

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che la pubblicità dei lavori della seduta odierna sarà assicurata anche attraverso l'attivazione di impianti audiovisivi a circuito chiuso, la trasmissione televisiva sul canale satellitare della Camera dei deputati e la trasmissione diretta sulla *web*-tv della Camera dei deputati.

Audizione del Sottosegretario di Stato per lo sviluppo economico Massimo Vari.

PRESIDENTE. L'ordine del giorno reca, nell'ambito dell'indagine conoscitiva sulla sicurezza informatica delle reti, l'audizione del sottosegretario di Stato per lo sviluppo economico, professor Massimo Vari, al quale do subito la parola.

MASSIMO VARI, *Sottosegretario di Stato per lo sviluppo economico*. L'importanza di Internet e delle nuove piattaforme digitali per l'evoluzione del sistema economico e sociale rappresenta un dato di comune esperienza. Questo significa che garantirne la sicurezza è un'esigenza per tradurre l'opportunità che ne deriva in crescita sostenibile e innovazione e per costruire un ambiente digitale che offra a tutti i cittadini nuove possibilità e prospettive. Il numero di minacce e violazioni della sicurezza ha già provocato notevoli danni economici, riducendo la fiducia degli utenti nell'utilizzo dei nuovi servizi e delle nuove tecnologie e ostacolando lo sviluppo del commercio elettronico che, invece, è molto importante anche a livello europeo.

Vorrei inquadrare, sia pur rapidamente, il mio intervento proprio in tale ambito di riferimento perché il contesto europeo è quello nel quale, in questi anni, sono state assunte iniziative che chiamano in causa gli Stati, non solo come destinatari di regole, ma anche come parte attiva di programmi e di azioni congiunte.

Le violazioni della sicurezza, come descritte nella Comunicazione della Commissione europea n. 163 del 2011, si possono sinteticamente suddividere, sulla base degli obiettivi che si prefiggono, in tre aree: sfruttamento, come le « minacce persistenti avanzate » a fini di spionaggio economico e politico e furti di identità; perturbazione, come gli attacchi finalizzati all'interruzione del servizio originati da più fonti, o lo *spamming* mediante *botnet*; distruzione, scenario che, per nostra fortuna, non si è ancora concretizzato, ma che, in considerazione dell'interdipendenza delle infrastrutture critiche (reti elettriche, sistemi idrici intelligenti, reti di comunicazione elettronica e così via) non si può escludere per il futuro.

Nella consapevolezza dell'importanza della condivisione, anche a livello sovranazionale e internazionale, delle problematiche poste dalla sicurezza delle reti, devo dire che già dal 2004 l'Unione Europea si è dotata di un'Agenzia per la sicurezza delle reti e dell'informazione (European Network and Information Security Agency, ENISA) che agisce come

piattaforma di scambio di informazioni e *best practice* fra le istituzioni europee, le autorità nazionali e le imprese.

L'ENISA funge da punto di riferimento, con il compito di analizzare i rischi attuali ed emergenti e di contribuire non solo ad assicurare un elevato livello di sicurezza delle reti e dell'informazione nell'Unione, ma anche a sviluppare una cultura in materia di sicurezza delle reti e dell'informazione, a vantaggio dei cittadini, dei consumatori, delle imprese e delle organizzazioni del settore pubblico dell'Unione europea, con riflessi anche sul buon funzionamento del mercato interno.

Nella Comunicazione della Commissione europea n. 149 del 2009 sulla protezione delle infrastrutture critiche informatizzate, è stato previsto il Piano di azione « Critical Information Infrastructure Protection », con l'obiettivo di rafforzare la preparazione e la resilienza delle infrastrutture di comunicazione fondamentali. Tra le iniziative del Piano, vorrei sottolineare l'importanza del Forum europeo degli Stati membri, istituito nel 2009 e sostenuto dall'Agenzia europea, che agisce come punto di confronto e di discussione fra i Paesi dell'Unione, e della *partnership* pubblico-privata per la resilienza.

Un significativo ulteriore passo avanti nell'ambito della sicurezza delle reti e dei servizi di comunicazione elettronica è stato compiuto sempre nel 2009, con la direttiva 2009/140/CE, il cui articolo 13 è intervenuto in materia di sicurezza e integrità delle reti, chiamando in causa gli Stati membri, ai quali è affidato il compito di individuare adeguate misure di sicurezza che gli operatori e i fornitori di servizi di comunicazione elettronica dovranno attuare, con l'obbligo di notificare eventuali incidenti che abbiano avuto un impatto significativo sull'utenza.

Vorrei rammentare ancora la Comunicazione della Commissione sull'agenda digitale europea del 26 agosto 2010, che, nell'ottica del conseguimento degli obiettivi della strategia Europa 2020, ha individuato alcune azioni, tra le quali la costituzione di *Computer Emergency Response Team*, i cosiddetti CERT nazionali, per la prevenzione e la gestione degli incidenti informatici, e la partecipazione alle esercitazioni coordinate dall'ENISA.

In questo contesto, la Commissione ha presentato una proposta relativa al nuovo mandato per rafforzare e ammodernare l'Agenzia europea per la sicurezza delle reti e dell'informazione. La proposta, che non è stata ancora approvata, consentirebbe all'Agenzia di supportare con maggiore efficacia l'Unione europea, gli Stati membri e il settore privato nello sviluppo delle loro potenzialità nel prevenire, individuare e combattere i problemi di sicurezza informatica.

Inoltre, merita di essere ricordata anche la più recente Comunicazione della Commissione europea sulla « Critical Information Infrastructure Protection » del 2011, che si sofferma essenzialmente sulla dimensione mondiale delle sfide e sull'importanza di un rafforzamento della cooperazione tra gli Stati membri e il settore privato a livello nazionale, europeo e internazionale. Questa comunicazione è stata oggetto di un confronto e di un ampio dibattito nell'ambito della Conferenza ministeriale sulla protezione delle infrastrutture informatizzate che si è svolta a Balatonfüred, in Ungheria, nei giorni 14 e 15 aprile 2011, le cui indicazioni sono state recepite nelle conclusioni del Consiglio dei Ministri dell'Unione europea del 27 maggio 2011.

In tale documento, il Consiglio dell'Unione europea invita gli Stati a intraprendere diverse azioni, tra le quali, oltre alla costituzione di CERT nazionali, l'adozione di una strategia di sicurezza informatica nazionale, l'elaborazione di piani di emergenza nazionali per il caso di incidenti informatici, l'organizzazione di esercitazioni nazionali e la partecipazione a esercitazioni europee.

Nel documento del Consiglio dell'Unione europea, gli Stati membri sono altresì invitati a cooperare fra loro e nell'ambito dell'European Forum for Member States, come pure con l'European public-private Partnership for Resilience, rispettivamente per l'individuazione delle infrastrutture critiche europee e per il

sostegno alla cooperazione con il settore privato a livello sia nazionale sia europeo.

Quanto al periodo 2010-2011, tra le principali iniziative di ENISA e della Commissione europea con l'obiettivo di rafforzare la protezione delle infrastrutture informatiche critiche, ricordo la prima esercitazione paneuropea « Cyber Europe 2010 », l'esercitazione congiunta Unione europea-Stati Uniti « Cyber Atlantic 2011 » e la seconda esercitazione paneuropea « Cyber Europe 2012 », alle quali ha partecipato anche l'Italia e, in particolare, il Ministero dello sviluppo economico.

Veniamo, ora, alla situazione nazionale, ovvero alla strategia nazionale per la *cyber security*. Attualmente, in campo nazionale, vi sono diverse istituzioni che operano in relazione a differenti aspetti della *cyber security*: la Presidenza del Consiglio, tramite il Dipartimento informazioni per la sicurezza, ai fini della valutazione della minaccia, e l'Ufficio del Consigliere militare dello stesso Presidente del Consiglio; il Ministero dell'interno, per la tutela dell'ordine e della sicurezza pubblica, il contrasto al crimine informatico e per la difesa civile; il Ministero della difesa, per la difesa dello Stato e la sicurezza delle reti e dei sistemi propri del suo ambito; il Ministero dello sviluppo economico, per la sicurezza delle reti e la tutela delle comunicazioni elettroniche; il Ministero degli affari esteri, per le attività internazionali.

In questa materia così complessa, in cui opera una pluralità di soggetti istituzionali, il primo passo essenziale per rafforzare la sicurezza delle reti in Italia è la definizione di una strategia nazionale di *cyber security,* che sia in grado di fungere da guida per l'individuazione delle azioni da intraprendere, da parte sia della Pubblica Amministrazione, sia degli operatori privati, anche con il coinvolgimento dei cittadini.

Ricordo che si tratta di un'esigenza sottolineata anche dal COPASIR, in un importante documento del luglio del 2010, al quale mi limito a rinviare poiché la Commissione ne sarà pienamente a conoscenza. Dico soltanto che questo documento raccomanda al governo di dotarsi di un impianto strategico e organizzativo che assicuri una *leadership* adeguata e predisponga chiare linee politiche, per il contrasto alle minacce e per il coordinamento fra gli attori interessati; obiettivo che, secondo il COPASIR, potrebbe essere raggiunto assegnando questi compiti a una struttura di coordinamento presso la Presidenza del Consiglio dei Ministri o presso un'autorità delegata. Per gli aspetti di maggiore dettaglio, rinvio, comunque, a questo documento.

Ricordo ancora che, al fine di definire uno strumento operativo nazionale in grado di affrontare la minaccia cibernetica, è stato costituito presso la Presidenza del Consiglio un gruppo di studio per la sicurezza dell'utilizzo dello spazio cibernetico, con l'obiettivo di effettuare la ricognizione delle strutture esistenti presso le varie amministrazioni; individuare, sia pure a fini meramente di studio, gli assetti organizzativi realizzati in altri Paesi, con particolare riguardo a quelli facenti parte dell'Unione europea, della NATO e del G8, tenendo conto del lavoro già svolto dal COPASIR; e, infine, formulare una proposta organizzativa per mettere a sistema le strutture nazionali esistenti.

Ciò detto, vorrei precisare che il Ministero dello sviluppo economico concorda pienamente sull'esigenza di porre in essere una strategia nazionale di *cyber security*, che dovrebbe essere sviluppata tenendo in considerazione le indicazioni dell'Unione europea alle quali ho già fatto riferimento e, al tempo stesso, anche alla specifica situazione di sviluppo digitale del Paese.

Ad avviso del Ministero dello sviluppo economico, detta strategia dovrebbe, in particolare, prendere in considerazione le seguenti esigenze: educare i cittadini e le imprese attivando meccanismi di sensibilizzazione in ordine ai rischi presenti sul *web*; potenziare strumenti di rilevazione e contrasto delle minacce, intesi come organizzazioni, processi, normative e applicazioni; promuovere la formazione attraverso percorsi formativi in grado di fornire sin dai primi livelli scolastici le competenze necessarie; rafforzare la collaborazione pubblico-privato attraverso

meccanismi di dibattito, condivisione e coordinamento, soprattutto riguardo alla protezione delle infrastrutture critiche; rafforzare meccanismi di cooperazione internazionale attraverso il sempre maggiore coinvolgimento dell'Italia nei tavoli internazionali, dove si discute di standard, *policy* e princìpi internazionali sulla *cyber security*; creare e potenziare meccanismi organizzativi di risposta agli incidenti, soprattutto attraverso l'opera di CERT pubblici e privati e del CERT nazionale; definire uno standard per la gestione delle identità digitali che possa soddisfare le necessità quotidiane dei cittadini nel loro utilizzo dei servizi, con particolare riguardo a una maggiore sicurezza di sistemi di pagamento su Internet; infine, stimolare la crescita di un'industria italiana della *cyber security*, intesa come ambito di sviluppo di tecnologie e di servizi e, al tempo stesso, di arricchimento di esperienze e competenze.

Vorrei, ora, venire ai compiti più specifici del Ministero dello sviluppo economico nella materia in questione, ricordando, anzitutto, la base normativa di riferimento su cui si articolano le sue competenze nel settore delle comunicazioni elettroniche, cioè il decreto legislativo 1° agosto 2003, n. 259, contenente il Codice delle comunicazioni elettroniche, recentemente modificato dal decreto legislativo 28 maggio 2012, n. 70, con il quale è stata recepita la direttiva 2009/140/CE.

Intendo richiamare l'attenzione soprattutto sull'articolo 14 del nuovo decreto che, nel recepire gli articoli 13-*bis* e 13-*ter* della predetta direttiva, affida al Ministero l'individuazione di misure minime di sicurezza, di natura tecnica e organizzativa, che gli operatori di rete e i fornitori dei servizi di comunicazione elettronica sono tenuti ad adottare, per gestire adeguatamente i rischi.

La verifica del rispetto delle suddette misure compete allo stesso Ministero dello sviluppo economico o ad un organismo indipendente da esso incaricato, che può applicare sanzioni in caso di violazioni e inadempimenti delle norme. Ai fini di tale verifica, le imprese sono tenute a fornire al Ministero le informazioni necessarie per valutare la sicurezza e l'integrità dei loro servizi e delle loro reti e, in particolare, i documenti relativi alle politiche di sicurezza.

Al Ministero è affidata, inoltre, la definizione di uno schema, sulla base del quale i suddetti operatori e fornitori di servizi sono tenuti a notificare gli incidenti di sicurezza classificati come significativi sulla base dei valori di soglia stabiliti nello schema stesso. Le segnalazioni di incidenti di sicurezza sono indirizzate dagli operatori al Ministero, che provvede a renderne partecipi, annualmente o quando il caso lo richieda, la Commissione europea e l'ENISA.

Allo scopo di armonizzare l'implementazione delle previsioni della direttiva, l'ENISA ha istituito un gruppo di lavoro al quale partecipa il Ministero dello sviluppo economico per il tramite dell'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione. Si tratta di un gruppo di lavoro che ha prodotto due linee guida tecniche dedicate alla definizione delle misure minime di sicurezza e dei parametri per la classificazione di significatività degli incidenti.

Tali linee guida, ancorché non vincolanti e tuttora soggette a revisione, costituiscono la base per l'emanazione di ulteriori provvedimenti di secondo livello. Tra le attività in materia di sicurezza delle reti svolte dal Ministero, vorrei, in particolare, segnalare quelle relative alle esercitazioni di *cyber security* che di seguito si descrivono.

La prima esercitazione paneuropea « Cyber Europe 2010 » si è svolta nel novembre 2010 con il coordinamento di ENISA e del Joint Research Center della Commissione europea. All'esercitazione, riservata alle pubbliche amministrazioni, hanno preso parte tutti gli Stati membri dell'Unione europea e tre Stati membri dell'EFTA (European Free Trade Association).

L'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione del Dipartimento per le comunicazioni del Ministero dello sviluppo economico ha

svolto, cooperando con la Presidenza del Consiglio dei Ministri e con il Ministero dell'interno, il ruolo di *planner* e successivamente quello di *moderator*, coordinando la partecipazione italiana all'esercizio, che ha visto nel ruolo di *player* il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche del servizio di Polizia postale e delle comunicazioni, il CERT difesa e il CERT SPC, ovvero il Sistema pubblico di connettività e cooperazione istituito presso DigitPA.

L'esercizio ha permesso di stabilire nuovi collegamenti fra i diversi attori e di sottolineare le interdipendenze fra i diversi Stati membri al fine di aumentare il mutuo soccorso.

Nel 2011, l'Italia ha partecipato, invece, all'esercitazione congiunta Unione europea-Stati Uniti « Cyber Atlantic 2011 », coordinata da ENISA e dal Department of Homeland Security degli Stati Uniti. L'esercitazione, a cui hanno partecipato 20 Stati membri, si è realizzata attraverso una simulazione finalizzata alla valutazione del grado di cooperazione fra gli Stati membri dell'Unione europea e gli Stati Uniti nella gestione di una crisi cibernetica e all'identificazione delle relative criticità.

Il Ministero dello sviluppo economico, tramite l'Istituto superiore delle comunicazioni, ha coordinato la partecipazione nazionale, in collaborazione con la Presidenza del Consiglio, e ha partecipato alla fase di pianificazione ed a quella di esecuzione nel ruolo sia di moderatore sia di *player*, con il CERT del Ministero della difesa.

Sulla tematica delle esercitazioni, devo aggiungere che, ai fini di una partecipazione coordinata alle esercitazioni europee, presso l'Istituto superiore delle comunicazioni, è stato formalizzato il tavolo tecnico interministeriale nato in occasione della prima esercitazione paneuropea.

Va ricordata, inoltre, la partecipazione alla seconda esercitazione paneuropea denominata « Cyber Europe 2012 », che si è conclusa il 4 novembre 2012, e che si è distinta dalla prima edizione per aver contemplato la partecipazione di soggetti privati, oltre alle pubbliche amministrazioni. L'Italia, per il tramite dell'Istituto superiore e del tavolo tecnico sopra citato, ha coinvolto Telecom Italia.

Infine, come richiesto dalla Commissione europea agli Stati membri, si è svolta nel giugno scorso un'esercitazione di carattere nazionale. In tale ambito, si è ipotizzato uno scenario di riferimento che prevedeva simulazioni di operazioni aventi l'obiettivo di verificare la reazione delle strutture della pubblica amministrazione, qualora fossero state coinvolte in un incidente informatico piuttosto complesso e verosimile.

Vorrei concludere su questo punto osservando che, attraverso la partecipazione attiva a tutte le esercitazioni organizzate in Europa e attraverso l'organizzazione di una propria esercitazione nazionale, l'Italia ha voluto dare compiuta ed esaustiva risposta all'impegno richiesto dalle politiche europee in materia.

Uno dei punti fondamentali dell'agenda digitale europea per la prevenzione e la gestione degli incidenti informatici è – come ho detto all'inizio – la costituzione di CERT nazionali. La Commissione europea ha posto due obiettivi chiave. Il primo è la costituzione di CERT a livello nazionale in tutti gli Stati membri; il secondo è il rafforzamento della cooperazione fra i vari CERT, che si collegheranno a quello europeo. Si creerà, quindi, una rete che sarà la base di un sistema europeo di condivisione delle informazioni e di allarme per i cittadini e le piccole e medie imprese.

In proposito, ENISA ha stabilito una *road map* per promuovere, entro il 2013, lo sviluppo di questo sistema europeo di condivisione e di allarme, fondato sull'attuazione di servizi di base a livello di CERT nazionali e di servizi di interoperabilità, in vista dell'integrazione dei sistemi nazionali nella condivisione delle informazioni e nelle procedure di allarme.

Attualmente, in ambito nazionale, operano due CERT istituzionali, il CERT SPC, ossia il sistema pubblico di connettività, istituito presso DigitPA, oggi Agenzia per

l'Italia digitale, rivolto agli utenti delle pubbliche amministrazioni, e il CERT difesa, istituito presso lo Stato Maggiore della Difesa, con il compito di servire gli utenti di quell'ambito. Tuttavia, questi CERT, essendo rivolti a una specifica utenza, non corrispondono alle caratteristiche del CERT nazionale, la cui azione, sulla base delle indicazioni comunitarie, dovrebbe essere rivolta a tutti i cittadini e a tutte le imprese, quindi non solo a utenti di specifiche organizzazioni, con un ruolo di coordinamento nazionale degli altri CERT istituzionali e privati verso il CERT europeo.

In particolare, il CERT nazionale è chiamato a effettuare: il monitoraggio delle vulnerabilità e l'osservazione dei comportamenti ostili registrati in rete; predisporre un sistema articolato di comunicazione, mediante avvisi e segnalazioni delle emergenze; predisporre ed impiegare procedure di coordinamento, in occasione del verificarsi di incidenti informatici; interagire con una pluralità di interlocutori omologhi per funzioni, tali da consentire un'idonea attività di verifica e correlazione delle indicazioni e dei dati ottenuti; migliorare i meccanismi e le misure di protezione, sulla base delle analisi degli incidenti avvenuti.

L'istituzione del CERT nazionale è stata prevista dall'articolo 14 del decreto legislativo n. 70 del 2012 che ha, a questo proposito, modificato il codice delle comunicazioni elettroniche, inserendo gli articoli 16-*bis* e 16-*ter* che traspongono, a loro volta, gli articoli 13-*bis* e 13-*ter* della citata direttiva 2009/140/CE.

Vorrei segnalare, inoltre, che l'Unione europea, come risulta dalla già menzionata Comunicazione del 2011 e, in particolare, dalle conclusioni del Consiglio dei Ministri dell'Unione europea del 27 maggio 2011, ha richiesto anche la definizione di una *policy* nazionale, nel campo della *cyber security*, e la predisposizione di un piano di contingenza nazionale, per una gestione coordinata degli incidenti informatici su larga scala. Si tratta, infatti, di misure che risultano indispensabili ai fini di un'azione efficace del CERT.

Si può comprendere che la realizzazione del CERT nazionale non basterà a risolvere, di per sé, le problematiche di sicurezza. La sua azione, infatti, non può che essere incardinata in una strategia chiara e definita e necessita dell'individuazione di precisi ruoli e responsabilità delle diverse istituzioni coinvolte in materia.

Avviandomi alla conclusione, vorrei accennare, sia pur brevemente, ad altre tematiche connesse alla sicurezza informatica. Mi riferisco, innanzitutto, al tema dell'identità digitale. Come sappiamo, infatti, le politiche dell'Unione europea, negli ultimi anni, sono state rivolte anche alla tutela dei cittadini nell'utilizzo dei servizi in rete.

In linea generale, le identità digitali si dividono in identità forti e deboli; le prime sono tipicamente regolate dalla legge per uso pubblico, come i sistemi di firma digitale; quelle deboli, invece, sono utilizzate dagli operatori *on line* per l'accesso a servizi digitali, quali *e-mail*, *social network* e *e-commerce*, e sono, di norma, costituite da un nome utente e da una *password*, oltre ad alcuni attributi funzionali alla fruizione del servizio.

Mentre le identità forti sono oggetto delle disposizioni del Codice dell'amministrazione digitale, quelle deboli non sono soggette a definite indicazioni e raccomandazioni volte a garantire la sicurezza dell'identità. La mancanza di criteri minimi di protezione espone le identità digitali a diversi rischi, come il furto di identità e l'impersonificazione, che comporta l'utilizzo di un'identità digitale da parte di un soggetto o di un'entità terza rispetto al corretto titolare. Si tratta, in sostanza, di un'identità rubata che può essere utilizzata per impersonificare un soggetto terzo e per compiere azioni, transazioni e comunicazioni in nome del reale titolare dell'identità.

Un altro rischio riguarda la violazione della *privacy*. Infatti, alcuni attributi di un'identità contengono informazioni personali protette dalla legge sulla *privacy*, sicché una non adeguata protezione dell'identità può comportare una violazione della *privacy*, rendendo noti a terzi attri-

buti che, invece, hanno carattere confidenziale. In alcuni casi, questi abusi avvengono non solo attraverso la violazione del sistema di gestione dell'identità, ma anche a causa di configurazioni non corrette da parte della piattaforma o del sistema.

Altro caso sono le truffe *on line*, che si verificano nel caso di identità digitali di tipo finanziario, come i dati di una carta di credito, per la quale può verificarsi un uso non autorizzato, preordinato a frodi e truffe *on line*.

L'ultimo caso è la forgiatura di identità, che consiste nella creazione di un'identità collegata a una diversa da quella a cui l'identità stessa si riferisce, per esempio la creazione di un *account email* a nome di un terzo.

A tali rischi sono soggetti soprattutto gli utenti finali di Internet, considerati, all'interno del sistema, l'anello debole della catena.

Come evidenziato dal Direttore del Servizio di polizia postale e delle comunicazioni nella seduta del 19 settembre scorso, tali situazioni possono realizzarsi in vari modi: il *phishing*, gli attacchi logici, il furto di credenziali mediante infezione dei *computer* o gli attacchi fisici, che consistono nel manomettere gli ATM per il prelievo bancomat, interponendo una telecamera o un minischermo per rubare i dati, nonché la clonazione di carte di credito e il *social engineering*, azione consistente nell'ingannare artatamente e con astuzia una persona per ottenere i suoi dati sensibili.

Il Direttore del Servizio di polizia postale e delle comunicazioni, nel sottolineare l'impegno sempre maggiore dei servizi investigativi per migliorare le tecniche di risposta, a fronte di un notevole incremento dei furti di identità verificatisi negli ultimi anni, ha evidenziato la necessità di prevedere una specifica normativa sul furto di identità digitale in quanto, attualmente, si utilizzano – cito – « schemi obsoleti sul piano giuridico per cercare di inquadrare questo fenomeno ».

Nel condividere in pieno la necessità di una normativa che renda il furto di identità un reato perseguibile all'interno dell'ordinamento nazionale, è evidente che occorrerebbe agire anche in via di prevenzione. Dal punto di vista delle imprese che gestiscono servizi, l'amministratore delegato di Poste italiane, ingegner Massimo Sarmi, ha rappresentato, a questo proposito, l'esigenza – sulla quale concordiamo – di definire specifici standard di identità digitale e di interoperabilità.

Al fine di garantire la protezione dell'identità digitale occorre, quindi, cercare di implementare azioni di prevenzione attraverso la definizione di una normativa specifica per l'erogazione, la gestione e l'interoperabilità di identità, ma anche attraverso un'azione di sensibilizzazione dei cittadini verso i rischi presenti sul *web*.

Una significativa iniziativa che affronta, a livello comunitario, la problematica dell'identità digitale è la recente proposta di regolamento del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

In considerazione del fatto che la maggior parte degli Stati membri ha introdotto differenti sistemi di identificazione elettronica e tenuto conto delle problematiche connesse all'interoperabilità transfrontaliera e alle identità digitali nazionali, la proposta prevede il riconoscimento e l'accettazione reciproci dei mezzi di identificazione elettronica e la definizione di una base giuridica comune, che obbliga ogni Stato membro a riconoscere e accettare i mezzi di identificazione elettronica, rilasciati in altri Stati membri, per accedere a servizi *on line*. Ciò dovrebbe consentire ai cittadini e alle imprese di trarre i massimi benefici dal mercato unico digitale.

In questa proposta, c'è un'importante disposizione che intendo sottolineare. Infatti, l'articolo 6 obbliga gli Stati membri a garantire un legame univoco tra i dati di identificazione elettronica e la persona alla quale si riferiscono.

La proposta di regolamento sarà sottoposta all'esame del Consiglio dei Ministri delle telecomunicazioni il prossimo 20 dicembre, al quale parteciperò in rappresentanza del Governo.

Per ragioni di connessione con quanto sin qui detto, vorrei fare un brevissimo cenno alle iniziative riguardanti la tutela della *privacy*, rammentando il recente decreto legislativo 28 maggio 2012, n. 69, di recepimento della direttiva 2009/136/CE che ha modificato il codice in materia di protezione dei dati personali, introducendo ulteriori obblighi in capo ai fornitori dei servizi di comunicazione elettronica.

In particolare, è stato introdotto nel suddetto codice l'articolo 32-*bis,* che obbliga le imprese fornitrici di servizi di comunicazione elettronica accessibili al pubblico a notificare sollecitamente al Garante ogni avvenuta violazione di dati personali. Al comma secondo, del medesimo articolo, viene stabilito che tale comunicazione debba rivolgersi anche al contraente del servizio o ad altra persona, qualora la violazione dei dati personali rischi di arrecare pregiudizio ai loro dati e alla riservatezza.

Nella comunicazione della violazione di dati agli abbonati al servizio o alle persone coinvolte sono incluse – questo mi sembra particolarmente importante – anche raccomandazioni sulle misure da adottare per attenuare i possibili effetti pregiudizievoli della violazione stessa, mentre nella comunicazione al Garante sono incluse informazioni riguardanti le misure adottate dal fornitore del servizio per affrontare la violazione di cui trattasi.

Vorrei aggiungere, a questo proposito, che la Commissione europea, in linea con quanto previsto dalla direttiva, sta predisponendo una proposta di regolamento sulle modalità di notifica. La proposta è ora al vaglio del Comitato comunicazioni presso la Commissione, nell'ambito del quale il Ministero dello sviluppo economico, d'intesa con il Garante per la protezione dei dati personali, sta valutando le diverse problematiche, offrendo il suo specifico contributo.

Vorrei ricordare ancora che l'ENISA, a seguito dell'adozione della direttiva 2009/136/CE, ha istituito un gruppo di lavoro che ha elaborato delle linee guida tecniche per l'individuazione dei criteri atti a stabilire quando un incidente di sicurezza determina la violazione dei dati, come pure per l'individuazione delle misure tecniche finalizzate alla rilevazione e alla valutazione delle suddette violazioni.

Vorrei fare, infine, un breve cenno al *cloud computing*. Siamo tutti consapevoli che il *cloud computing* può portare efficienza, efficacia e risparmi sia alla pubblica amministrazione sia alle piccole e medie imprese che costituiscono la spina dorsale del sistema economico italiano. Tuttavia, tali risultati possono essere conseguiti solo qualora vengano affrontati i temi della sicurezza che, in ambito *cloud*, sono particolarmente rilevanti.

Nel corso del 2011, sono stati pubblicati alcuni documenti volti all'approfondimento delle tematiche di sicurezza e consapevolezza relativamente al tema *cloud*. Segnalo, in particolare, il Quaderno CONSIP « *Cloud Security*: una sfida per il futuro » e la scheda di documentazione del Garante della privacy « *Cloud computing,* indicazioni per l'utilizzo consapevole dei servizi ».

Questi documenti si inseriscono nell'ambito di un'apprezzabile tendenza da parte di molti organi governativi a produrre linee guida e regolamentazioni che rendano più immediato, semplice e sicuro l'utilizzo del *cloud computing*. Tra queste indicazioni spiccano le linee guida di ENISA, sulla valutazione del rischio e la recentissima « Procure secure », sulle modalità di approccio all'approvvigionamento dei servizi *cloud*.

Come tema di approfondimento, segnalo anche, per la loro fondamentale importanza, le normative statunitensi che fissano obblighi e modalità di approccio per le agenzie federali americane, « Federal Cloud Strategy », e il programma di certificazione FedRAMP (« Federal Risk and Authorization Management Program »).

Dagli accennati documenti e, più in generale, dal dibattito in materia, emerge – ripeto – la necessità di un'attenta regolamentazione dei servizi *cloud* nel contesto governativo, tale da fornire suggerimenti e indicazioni a tutti gli altri com-

parti nazionali. È, quindi, da ritenere di fondamentale importanza che l'Italia si doti rapidamente di linee guida e di strumenti di approccio standardizzati ai servizi *cloud*, sia in ambito governativo sia in quello delle infrastrutture critiche, incoraggiando lo sviluppo e la diffusione di queste tipologie di servizi.

Concludo segnalando un'iniziativa di DigitPA, oggi Agenzia per l'Italia digitale, che ha recentemente pubblicato un documento, risultato delle attività di un gruppo di lavoro al quale hanno partecipato rappresentanti sia del settore pubblico sia di quello privato, nel quale si ritrovano interessanti raccomandazioni e proposte sull'utilizzo del *cloud computing* nella Pubblica Amministrazione.

PRESIDENTE. Do la parola ai deputati che intendono intervenire.

JONNY CROSIO. Grazie, presidente. Ringrazio il sottosegretario della relazione molto interessante, che ha toccato punti che ritengo fondamentali da affrontare in questo dibattito fra la Commissione e il Governo.

Non le rivolgerò delle domande perché non credo che dobbiamo fare questo. Vorrei fare, piuttosto, delle considerazioni su quanto ha esposto perché credo siano importanti per la nostra indagine conoscitiva che sta arrivando alla conclusione, per cui è bene iniziare a fare delle riflessioni.

Parto dal presupposto che è compito sia del Parlamento che del Governo tutelare, a diversi livelli, la rete in quanto patrimonio fondamentale del nostro sistema sociale e del nostro sistema Paese. Credo che sia fondamentale fare una distinzione fra quelle che lei ha definito identità deboli e forti. Sono, infatti, cose molto diverse, anche come approccio. Penso che debba essere sempre più implementato un piano nazionale di sensibilizzazione e di educazione delle identità deboli, cioè dei cittadini, in quanto elementi più vulnerabili nel sistema rete Paese, visto che le identità forti hanno strumenti e mezzi a disposizione per tutelarsi.

Sotto questo aspetto, i CERT hanno dei pregi, ma anche un difetto. Abbiamo due piattaforme CERT, una relativa alla pubblica amministrazione e un'altra alla difesa. È giusto che sia così, ma il sistema deve essere ulteriormente sviluppato perché questo non è sufficiente. È una filosofia che definisco, in maniera impropria, molto americana, ma questo è lo stato dell'arte.

Anche nel nostro Paese, come in tutto il sistema globale della rete, viviamo in un'epoca di passaggio generazionale. Tra gli utenti più deboli, ci sono i « debolissimi », vale a dire i minorenni che, però, fruiscono di più della rete rispetto agli altri utenti deboli che sono responsabili per loro, cioè i genitori. Questo passaggio generazionale crea una grossa conflittualità anche per quanto riguarda l'approccio che si deve avere nel tutelare l'utente debole. Non è facile.

Ecco, su questo, credo che bisognerebbe fare un lungo discorso. Il piano nazionale di sensibilizzazione deve mirare anche a questo. Nel decreto-legge che abbiamo approvato la settimana scorsa in Assemblea, mi aspettavo qualcosa di più concreto per quanto riguarda l'agenda digitale proprio su questo tema. È, infatti, un po' debole rinviare le decisioni alla decretazione d'urgenza. Forse, dovrebbe esserci un piano più performante, anche perché l'agenda digitale europea che lei ha citato ci dà dei fondamenti, ma le va costruito attorno molto altro da parte dei sistemi di vari Paesi, specialmente sul furto di identità dell'utente più debole, che diventa una vittima.

Uno dei passaggi – lo dico al Governo, ma anche il Parlamento deve fare una riflessione – è quello di mettere in campo tutte le azioni possibili al fine di sanare la mancanza giuridica che lei citava e che la Polizia postale ha sottolineato nella sua audizione, cioè il fatto che non esistano i fondamenti giuridici per poter mettere le manette a colui che compie certi reati. Questo è paradossale, per cui è un passaggio che deve essere fatto.

L'agenda digitale europea ci dà questo *input*, ma non ha creato le condizioni

affinché le polizie dei vari Paesi possano avere un'interoperabilità dinamica, come la rete. Questo limite va registrato. Deve esserci un'azione da parte dei governi o comunque dell'Europa. Insomma, se l'Europa ha ragione di esserci e vuole farsi sentire, su questo campo non si può pensare di frazionare. L'Europa ha senso soprattutto su questa partita, per cui credo che l'azione debba essere mirata.

Mi sono chiesto perché abbiamo fatto questa audizione, che credo fondamentale. Cosa percepisce il cittadino? Personalmente, mi preoccupo meno della parte industriale del Paese o della pubblica amministrazione, che – come dicevo – ha una sorta di tutela che viene dal sistema che, per forza, deve tutelare questo aspetto. In questo momento, si stanno aprendo degli scenari nuovi a livello globale. Ho letto recentemente un libro di un americano che ha ipotizzato che – come ormai sappiamo tutti – abbiamo sovvertito il fatto che, come qualcuno diceva, avremmo combattuto la Terza guerra mondiale con le clave. Invece, non è così. È finita questa previsione degli anni Ottanta. Forse, la combatteremo davanti a una tastiera, che farà più danni dei B52 e quant'altro perché, se si riesce a penetrare nella rete di un Paese, lo si fa morire. Insomma, è meglio avere dieci *hacker* che 10.000 soldati. Questa è la realtà attuale.

Allora, il cittadino percepisce che c'è un'azione forte da parte dei governi e degli operatori a creare strade informatiche sempre più performanti, ma c'è un grosso problema perché chi viaggia su queste strade non si trova, come quando viaggia in automobile, la Polizia stradale, il 112, il 133 o il 118, a seconda del tipo di emergenza. Il cittadino viaggia su queste strade in cui circola un sacco di merce avariata. Infatti, continuiamo a implementare la rete, nella consapevolezza che una percentuale sempre maggiore di ciò che vi gira è sporcizia, cioè merce che non produce PIL per i governi, bensì per il malaffare. Questo è abbastanza contorto, ma è un dato di fatto sul quale molti analisti internazionali si stanno interrogando.

Allora, in conclusione, ribadisco che va fatta una legge che deve cercare di tutelare il più possibile la rete. Bisognerà, quindi, fare delle scelte. Di conseguenza, due filosofie, che spesso anche nel nostro Paese vengono prese in considerazione, devono essere ammorbidite. Mi riferisco, in particolare, alla filosofia che chiamo « da figli dei fiori », secondo cui la rete deve essere libera e per tutti. Certamente deve essere così, ma questo non vuol dire che si può fare tutto quello che si vuole. Bisogna pensare che la rete non ha frontiere, ma probabilmente dovremmo anche bloccare coloro che gestiscono la questione della *privacy* perché lo spartiacque passa anche da lì. Bisognerà essere forse più rigidi o più laschi, a seconda dei punti di vista. Comunque, bisogna fare delle scelte.

Non solo questo Governo, ma anche quello che l'ha preceduto, in maniera ancora più irresponsabile, è stato latitante su questo. Resto fermamente convinto che occorrerebbe un dicastero dedicato alle reti e alle telecomunicazioni, come succede in altri Paesi del mondo, senza continuare a essere il cugino povero del Ministero dello sviluppo economico e che questo tema non debba essere minoritario in questa Commissione, dove vengono prima i trasporti, poi le poste e infine le telecomunicazioni, quando non si sa di cosa parlare.

Chiudo questa riflessione con l'auspicio che questa indagine conoscitiva possa produrre un documento di riflessione fondamentale per il prossimo governo e la prossima Commissione che si insedierà. Non dico che stiamo correndo il rischio dell'anarchia dalla rete perché non è così, ma lo sviluppo, anche nel nostro Paese, passa sempre di più attraverso la rete. Peraltro, siamo già carenti dal punto di vista dell'infrastruttura.

In definitiva, credo che dobbiamo darci una filosofia diversa, con la consapevolezza e la determinazione di tutelare e di valorizzare la rete. Ecco, ritengo che questo sia fondamentale e che occorra tenere fuori da questo discorso chi continua a mantenere un approccio a *spot* verso la rete. Spesso, quando si dice che la rete

deve essere libera e così via, non si sa neppure di cosa si sta parlando. Mi scusi, signor presidente, se sono violento, ma è la verità.

La rete è libera, ma non lo deve essere al punto di essere violentata. Questo è il rischio che stiamo correndo. Credo, dunque, che dobbiamo arrivare a produrre un testo di buonsenso. Esprimo il punto di vista delle opposizioni di questo Parlamento, ma credo che non sia un fatto di opposizione o meno, ma, appunto, una questione di buonsenso, che deve prevalere in questa partita. Grazie.

PRESIDENTE. Prima di dare la parola al professor Vari e ai rappresentanti del Ministero per la replica, vorrei porre una domanda. Nella proposta di regolamento europeo sull'identità digitale, è previsto il tema del furto di identità ? Se sì, con quali sanzioni ? Qualora ciò non sia previsto, è possibile inserirlo nel dibattito, visto che lei domani sarà presente in Europa in sede di Consiglio ?

RITA FORSI, *Direttore generale dell'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione*. Vorrei fare una precisazione sulla distinzione tra identità digitale debole e identità digitale forte. La differenza fra queste modalità di riconoscimento in rete è ciò che dovrà essere valutato nel regolamento perché il problema sta proprio in questo. L'identificazione in termini deboli vuol dire un normale utilizzo di nome utente e *password*. Si tratta, insomma, di sistemi semplici per questo si parla di un'identificazione poco sicura. Su questo dovrà essere previsto, quindi, un maggiore approfondimento. Viceversa, l'identità forte sarà proprio quella che garantirà l'accesso sicuro e quindi lo sviluppo – come diceva il sottosegretario – dei servizi più importanti.

Su questo tema, vi è una forte discussione ancora in corso. Sono state emanate due direttive, ma la discussione non ha prodotto ancora alcun regolamento. Ci sarà, dunque, un ulteriore dibattito lo stesso 20 dicembre.

PRESIDENTE. Comunque, il tema sarà affrontato.

JONNY CROSIO. Avendo analizzato la questione con degli operatori, vorrei evidenziare che c'è il passaggio generazionale sugli *ID number* e su tutti i protocolli IP che passano dal 3 al 4, detto in maniera un po' impropria. Comunque, questo passaggio implica il fatto che per il sistema di storicizzazione, di mantenimento, di implementazione dei dati di identificazione – alla fine, questo è il dibattito – bisognerà mettere a disposizione risorse e spazi per conservare questi dati. Insomma, chi paga e dove si mettono ? Bisogna, quindi, creare un sistema internazionale riconosciuto. A parte il fatto giuridico, occorre stabilire dal punto di vista tecnico chi deve svolgere questo compito. Lo facciamo fare da Telecom ? E come viene gestito ?

Questo è un grosso problema perché se si vuole tutelare la rete e il cittadino, che è la parte debole, occorre mantenere una banca dati in cui l'utente viene registrato con opportuni sistemi. Questo – ripeto – è il grosso problema che deve essere risolto.

MASSIMO VARI, *Sottosegretario di Stato per lo sviluppo economico*. L'impostazione di questo regolamento mi pare più orientata a un criterio di mutuo riconoscimento e di mutuo impegno per evitare che ci siano queste forme di falsificazione.

Quanto, invece, all'altro tema, quello della libertà o meno della rete, chiedo di poter dare la parola all'ingegner Palombini, che è appena tornata da Dubai, dove nei giorni scorsi c'è stata la Conferenza internazionale delle telecomunicazioni, che si è conclusa, però, con un nulla di fatto.

PRESIDENTE. È un dibattito molto interessante. Recentemente, vi sono state anche azioni di indagine conoscitiva e ispettiva da parte dei colleghi proprio sull'approccio del Governo, ma quel giorno non c'era il sottosegretario. Mi sembra abbia risposto il sottosegretario dell'agri-

coltura. Comunque, ingegnere Palombini, le chiedo di dirci qualcosa su queste famose giornate di Dubai, in cui si doveva profilare un nuovo protocollo di intesa su Internet.

ISABELLA PALOMBINI, *Funzionario del Gabinetto del Ministro del Ministero dello sviluppo economico*. Fin dall'inizio, il Governo italiano, anche attraverso la lettera aperta di risposta dei Ministri Passera e Terzi, pubblicata su *La Stampa* del 19 ottobre scorso, ha espresso la sua posizione sui temi della Conferenza, affermando subito che essa era conforme a quella dell'Unione europea.

A Dubai, l'Unione europea poteva intervenire solo come osservatore, perché la Conferenza internazionale della UIT (Unione internazionale delle telecomunicazioni) è riservata ai governi: tuttavia, di fatto, vi ha partecipato nell'ambito della delegazione cipriota, che attualmente ha la Presidenza del semestre europeo, coordinando così la posizione dei Paesi membri.

La preoccupazione era che con la revisione del Trattato internazionale sulle telecomunicazioni si uscisse dall'ambito definito a suo tempo. Infatti, il Trattato è stato siglato l'ultima volta nel 1998, quando si parlava a malapena di Internet, ed era riferito alle telecomunicazioni tradizionali e alla telefonia vocale. La preoccupazione, quindi, era che questo trattato potesse estendere il suo ambito di riferimento proprio ai servizi di Internet, con tutte le conseguenze del caso.

Per tale motivo, c'è stato un intenso dibattito, nei mesi precedenti la conferenza, scatenato, innanzitutto, dalla proposta delle TELCO europee, attraverso l'Associazione ETNO (European Telecommunications Network Operators' Association). In particolare le TELCO hanno cercato di veicolare una loro proposta perché potesse essere riconosciuto un tipo di modello di *business* atto a remunerare diversamente i servizi di trasporto forniti oggi dagli operatori delle telecomunicazioni. Ciò in considerazione dei notevoli guadagni che, da tali servizi, possono invece trarre i *social network,* o i motori di ricerca, cioè i vari Google, Amazon, Facebook e così via.

Queste ultime sono per lo più società americane, che guadagnano moltissimo soprattutto sui ricavi pubblicitari o sulla veicolazione delle informazioni attraverso gli algoritmi dei motori di ricerca. In particolare i loro ricavi sono molto più alti rispetto a quelli delle telecomunicazioni, che, invece, stanno diminuendo. Di conseguenza, si è cercato di utilizzare il veicolo della revisione del trattato UIT per poter cominciare a regolamentare il mondo di Internet, trovando però la ferma opposizione dei soggetti che operano sulla rete, i cosiddetti *over the top*, fortemente sostenuti dal Governo americano, al quale si sono associati il Regno Unito e l'Australia, per citare i Paesi più importanti.

In ambito europeo, la Germania, la Francia e anche l'Italia hanno mantenuto più un ruolo di osservatori, pur nella linea per l'Italia stabilita dal Ministro, che era quella di ritenere che Internet, essendosi sviluppato attraverso soggetti diversi – non soltanto governi e operatori di telecomunicazione, ma anche la società civile, il mondo accademico e i singoli individui – dovesse continuare ad evolvere secondo questo modello *multi-stakeholder*. Al tempo stesso, nel ribadire tale ferma posizione, Paesi come Germania, Francia e Italia sono stati attenti anche a cercare di capire come tutelare le realtà domestiche, quindi gli operatori di telecomunicazioni nazionali, che sono quelli che subiscono l'effetto dirompente di Internet.

A ogni modo, si è detto che queste problematiche reali – come la tassazione dei profitti sulla rete, il riconoscimento del diritto d'autore e della *privacy* – vanno discusse al di fuori dell'ambito strettamente intergovernativo quale quello dell'UIT. Ciò è stato confermato anche durante la conferenza, in una maniera forse non proprio ideale, per come sono andate le cose. Infatti, vi sono state due settimane di discussione fino a notte inoltrata, per cercare di arrivare a delle soluzioni di compromesso che non si riuscivano a trovare. Alla fine, si è giunti ad un testo che sembrava accettabile, ma poi, all'ul-

timo momento, è stata inserita una modifica che – in maniera forse un po' pretestuosa – è stata considerata come un tentativo di ribaltare i presupposti iniziali. In sostanza, con questa modifica il trattato estendeva il suo mandato, quindi non riguardava più soltanto le telecomunicazioni, ma anche il mondo di Internet.

Questa modifica non è stata accettata dagli Stati Uniti, dal Regno Unito e neppure dall'Unione europea. Di conseguenza, gli Stati membri dell'UE si sono conformati al parere comunitario, prendendo del tempo per verificare se effettivamente le modifiche proposte estendono questo mandato e fino a che punto, quindi per valutare la loro reale portata.

MASSIMO VARI, *Sottosegretario di Stato per lo sviluppo economico*. Questo è il problema che poneva l'onorevole Crosio. Il punto interrogativo è fino a che punto si spinge la regolamentazione di Internet.

JONNY CROSIO. Fino a che punto bisognerà pagare la campagna elettorale del signor Obama ?

PRESIDENTE. Credo che questo sia un tema complicato. Comunque, ringrazio il sottosegretario per lo sviluppo economico, professor Massimo Vari, per il suo intervento e per la documentazione depositata, di cui autorizzo la pubblicazione in allegato alla seduta odierna *(vedi allegato)*, e i rappresentanti del Ministero intervenuti. Dichiaro conclusa l'audizione.

La seduta termina alle 15,50.

IL CONSIGLIERE CAPO DEL SERVIZIO RESOCONTI ESTENSORE DEL PROCESSO VERBALE

DOTT. VALENTINO FRANCONI

Licenziato per la stampa il 20 febbraio 2013.

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

Ministero dello Sviluppo Economico

Indagine Conoscitiva sulla Sicurezza Informatica delle Reti presso la Commissione IX Trasporti, Poste e Telecomunicazioni della Camera dei Deputati

Audizione del Sottosegretario di Stato Massimo Vari

18 dicembre 2012