COMMISSIONE IX
TRASPORTI, POSTE E TELECOMUNICAZIONI

RESOCONTO STENOGRAFICO

INDAGINE CONOSCITIVA

12.

SEDUTA DI MARTEDÌ 7 MAGGIO 2019

PRESIDENZA DEL VICEPRESIDENTE **DIEGO DE LORENZIS**

INDICE

N. B. Sigle dei gruppi parlamentari: MoVimento 5 Stelle: M5S; Lega - Salvini Premier: Lega; Partito Democratico: PD; Forza Italia - Berlusconi Presidente: FI; Fratelli d'Italia: FdI; Liberi e Uguali: LeU; Misto: Misto; Misto-Civica Popolare-AP-PSI-Area Civica: Misto-CP-A-PS-A; Misto-Minoranze Linguistiche: Misto-Min.Ling.; Misto-Noi con l'Italia-USEI: Misto-NcI-USEI; Misto-+Europa-Centro Democratico: Misto-+E-CD; Misto-MAIE - Movimento Associativo Italiani all'Estero: Misto-MAIE; Misto-Sogno Italia - 10 Volte Meglio: Misto-SI-10VM.

PAGINA BIANCA

PRESIDENZA DEL VICEPRESIDENTE DIEGO DE LORENZIS

La seduta comincia alle 12.30.

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che la pubblicità dei lavori della seduta odierna sarà assicurata anche attraverso la trasmissione televisiva sul canale satellitare della Camera dei deputati e la trasmissione diretta sulla *web-tv* della Camera dei deputati.

Audizione di rappresentanti dell'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (ISCOM) del Ministero dello sviluppo economico.

PRESIDENTE. L'ordine del giorno reca, nell'ambito dell'indagine conoscitiva sulle nuove tecnologie delle telecomunicazioni, con particolare riguardo alla transizione verso il 5G ed alla gestione dei *big data*, l'audizione di rappresentanti dell'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (ISCOM) del Ministero dello sviluppo economico.

Ringrazio i rappresentanti di ISCOM per aver accettato l'invito della Commissione e do la parola alla dottoressa Rita Forsi, direttrice generale, per lo svolgimento della relazione.

RITA FORSI, *direttrice generale dell'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (ISCOM) del Ministero dello sviluppo economico*. Buongiorno a tutti, grazie per questa opportunità di poter fornire un contributo da parte dell'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione, che è una Direzione generale del Ministero dello sviluppo economico.

La nostra esperienza in questi ultimi periodi specialmente, ma che data ormai da lungo tempo, ci ha permesso di approfondire alcuni profili particolari della transizione al 5G, in particolare quelli relativi agli aspetti di *cyber security*. La mia relazione sarà quindi incentrata specialmente su questi tipi di aspetti e aggiornamenti su quanto viene fatto in Italia e anche a livello europeo.

Premetto che le tecnologie dell'informazione e della comunicazione costituiscono l'elemento portante della crescita economica. Finanza, sanità, energia e trasporti, oltre naturalmente alle telecomunicazioni, dipendono dal corretto funzionamento delle reti e dei sistemi informatici.

L'utilizzo di queste tecnologie inoltre si va estendendo anche al settore manifatturiero, modificando radicalmente i processi produttivi. In costante sviluppo grazie alle nuove tecnologie sono anche i servizi del *government*, che permettono di aumentare l'efficienza della pubblica amministrazione nel rapporto con i cittadini.

Parallelamente allo sviluppo di nuove tecnologie e al loro uso estensivo, si registra un incremento degli attacchi *cyber*, che diventano sempre più sofisticati e possono colpire il funzionamento dell'apparato statale o la fornitura di servizi essenziali per i cittadini, con conseguenti danni economici e possibili pregiudizi per la qualità della vita.

In particolare, il prossimo dispiegamento della tecnologia di rete 5G, quindi di quinta generazione, costituirà un fattore abilitante per lo sviluppo di molti servizi digitali, quindi le reti 5G saranno l'infrastruttura portante non solo di nuovi

servizi di comunicazione elettronica, ma anche di una vasta gamma di servizi essenziali, quali l'energia, i trasporti, i servizi bancari e sanitari, i sistemi di controllo industriale.

Se consideriamo il fatto che molti servizi dipenderanno dalle reti 5G, un eventuale attacco o incidente informatico perpetrato a danno di queste reti capiamo che tipo di conseguenze possa avere su cittadini e imprese. Sarà quindi necessario garantire il massimo della sicurezza delle reti 5G, anche in considerazione dell'interconnessione delle infrastrutture e poi della natura transfrontaliera della minaccia informatica. Siamo tutti collegati, quindi un eventuale problema si trasferirebbe velocemente ad altre infrastrutture.

È proprio su tali aspetti che nel corso di questa audizione fornirò il mio contributo, soffermandomi nella parte iniziale sui recenti sviluppi della *cyber security* relativamente al settore specifico delle comunicazioni elettroniche, quindi in particolare alla tecnologia 5G.

L'Unione europea, da almeno una quindicina d'anni, con l'avvio dell'Agenzia europea per la sicurezza delle reti ha cominciato ad affrontare il problema, con l'obiettivo di favorire l'incremento del livello di sicurezza delle reti dell'informazione nell'Unione europea, nonché lo sviluppo di una cultura in materia a vantaggio di cittadini e imprese. ENISA, questa agenzia, agisce come centro di competenza per lo scambio di informazioni e buone pratiche tra settore pubblico e privato, analizzando rischi attuali ed emergenti.

Ricordiamo tutti il noto attacco nella primavera del 2007, che ha colpito l'Estonia e ha fatto crescere in Europa la consapevolezza dei potenziali rischi e la conseguente necessità di rafforzare anche le capacità nazionali e soprattutto anche un coordinamento a livello europeo.

Passo adesso ad analizzare il perimetro specifico delle reti di comunicazione elettronica e la loro necessità relativamente alla sicurezza e all'integrità di queste reti. Partiamo dal decreto legislativo n. 70 del 2012, emanato in attuazione delle direttive 2009/140/CE, in materia di reti e servizi di comunicazione elettronica, e 2009/136/CE in materia di trattamento dei dati personali e tutela della vita privata, che ha modificato il Codice delle comunicazioni elettroniche, cioè il decreto legislativo 259 del 2003.

Il citato decreto legislativo n. 70 prevede per la prima volta nel panorama nazionale disposizioni in materia di sicurezza e integrità delle reti di comunicazione elettronica, cioè i fornitori di reti e servizi di comunicazione elettronica hanno l'obbligo di adottare misure di sicurezza nell'ottica di ridurre al massimo i rischi di interruzione dei servizi forniti agli utenti, e l'obbligo di segnalare al Ministero dello sviluppo economico gli incidenti con significativo impatto sui servizi forniti.

Ai sensi di tali disposizioni, le misure di sicurezza e integrità delle reti e i casi in cui gli incidenti sono da ritenersi significativi sono definiti con decreto del Ministro dello sviluppo economico.

Il 12 dicembre 2018 il Ministro dello sviluppo economico ha emanato il previsto decreto attuativo (pubblicato nella Gazzetta Ufficiale del 21 gennaio 2019), con il quale è stata data attuazione pratica alle citate disposizioni. In virtù di questo provvedimento sono individuate le misure di sicurezza e integrità che gli operatori devono adottare e i casi in cui gli incidenti informatici devono essere comunicati al CSIRT, il *Computer Security Incident Response Team*, di cui parlerò più avanti, e al Ministero dello sviluppo economico, in particolare all'Istituto superiore, che è stato individuato come struttura destinataria di queste segnalazioni.

Sul tema della sicurezza invece dobbiamo dire che, nella prospettiva dell'uso pervasivo delle reti del 5G, nel prossimo futuro appare utile anche un'analisi dei possibili rischi in tema di sicurezza nazionale. La nuova tecnologia 5G ha una flessibilità architetturale, per cui la sicurezza diventa un tema veramente complesso da gestire, in quanto queste architetture innovative saranno composte da una pluralità di segmenti, che vanno dalla parte di accesso radio, la parte più esterna, fino alla rete *core*, quella di gestione e con una

vastità di terminali che svolgono funzioni sempre più complesse.

Avremo quindi un insieme molto ampio di elementi, che presenteranno diversi aspetti di vulnerabilità, e tutti questi dovranno essere presi in considerazione se vogliamo considerare la sicurezza di queste reti.

Inoltre, la stessa gestione delle risorse, pensata per essere attuata in maniera virtuale e dinamica con procedure sia centralizzate che distribuite, potrebbe essere oggetto di attacchi mai affrontati finora nelle altre reti che conosciamo. Al riguardo, si coglie l'occasione per citare una recentissima iniziativa europea: il 26 marzo scorso la Commissione europea ha previsto con una propria raccomandazione una serie di azioni e di misure operative, volte a rivedere e rafforzare le vigenti norme di sicurezza in questo settore, per assicurare che riflettano l'importanza strategica delle reti 5G, nonché l'evoluzione delle minacce, in uno scenario in cui l'ampliamento della superficie di attacco porterà verosimilmente a un incremento del numero di attacchi. Non dobbiamo inoltre sottacere che il livello di sofisticazione andrà quasi sicuramente ad aumentare.

In tale contesto, entro la fine di giugno di 2019, quindi molto presto, ogni Stato membro dovrà completare la valutazione nazionale dei rischi ed aggiornare i requisiti di sicurezza vigenti a carico dei fornitori di rete, includendo condizioni per garantire la sicurezza delle reti pubbliche. La raccomandazione inoltre prevede azioni da condurre a livello sia nazionale che dell'Unione e consente di avviare una distinzione, per quanto tecnologicamente possibile, fra azioni prescrittive dirette verso i fornitori di reti e servizi e quelle dirette verso i fornitori degli apparati, che sono due categorie spesso diversificate.

Secondo questa raccomandazione, gli Stati membri dovrebbero elaborare i requisiti di sicurezza specifici, che potrebbero essere applicati nel contesto degli appalti pubblici relativi alle reti 5G, tra cui requisiti obbligatori per la realizzazione di schemi di certificazione in termini di *cyber security*.

Facendo adesso una panoramica sul tema della *cyber security*, mi soffermo su una serie di iniziative in ambito europeo, che hanno consentito a livello nazionale di assistere ad una forte crescita della consapevolezza (molto lavoro è stato fatto e questo lo possiamo riscontrare sia a livello pubblico che a livello privato) e al conseguente avvio di azioni finalizzate al rafforzamento della sicurezza sia nella pubblica amministrazione che nel sistema delle imprese.

In particolare, faccio riferimento alla direttiva nota come Direttiva NIS *(Network and Information Security)*, la n. 1148 del 2016, che è stata recepita in Italia con il decreto legislativo 65 del 2018, quindi a maggio dell'anno scorso. Con questo decreto legislativo sono state introdotte delle « disposizioni volte a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi dell'Unione europea », come recita il titolo della direttiva in inglese.

Il decreto n. 65 quindi ha previsto alcune azioni di rafforzamento della sicurezza informatica nazionale secondo alcune linee di azione, in particolare l'individuazione di autorità competenti nei settori strategici identificati a livello europeo. Questi settori sono energia, infrastrutture e servizi digitali, comparti per i quali è competente il MISE, nonché trasporti, settore bancario e infrastrutture dei mercati finanziari, sanità, fornitura e distribuzione di acqua potabile. Questi sono i settori individuati dalla direttiva, che sono stati quindi coperti da specifiche autorità a livello nazionale.

L'individuazione dei cosiddetti « operatori di servizi essenziali » nei settori individuati era un'altra azione richiesta dalla direttiva, la previsione di misure tecnico-organizzative che questi operatori devono adottare (non è più una scelta opzionale, ma c'è un obbligo: questo è il punto di svolta che va sottolineato) per ridurre il rischio e limitare l'impatto di incidenti informatici, unitamente all'obbligo di notifica di eventi che presentino un rilevante im-

patto sulla continuità dei servizi e quindi si riflettano sulla collettività. Le azioni quindi sono due, adozione di misure e notifica degli incidenti significativi.

La designazione di un punto di contatto unico di interfaccia verso l'Unione europea, che è stato individuato nel Dipartimento per l'informazione e la sicurezza, e la costituzione presso la Presidenza del Consiglio dei ministri di un unico CSIRT italiano, che opera in cooperazione con gli omologhi organismi europei.

Con decreto del Ministro dello sviluppo economico del 26 ottobre 2018, all'Istituto superiore delle comunicazioni e tecnologie dell'informazione di cui ho la responsabilità è stata attribuita la funzione di autorità NIS per i settori energia, infrastrutture e servizi digitali. Il 9 novembre del 2018 era una data importante fissata dalla direttiva, data entro la quale dovevano essere individuati gli operatori dei servizi essenziali da ciascuna autorità, e questo è stato fatto in Italia, il termine è stato rispettato, quindi sono stati individuati con decreto direttoriale gli operatori dei servizi essenziali nei settori di competenza delle varie autorità, specialmente per quanto riguarda il MISE questo è stato fatto.

Contestualmente, sempre presso l'Istituto è stato istituito l'elenco nazionale degli OSE (Operatori Servizi Essenziali), individuati dalle autorità competenti anche in tutti gli altri settori, anche questa previsione del decreto legislativo 65 del maggio dell'anno scorso.

Attualmente è in corso l'*iter* per l'adozione di un DPCM, su proposta del MISE di concerto con il Ministero della pubblica amministrazione, relativa alla costituzione di un Comitato tecnico di raccordo delle autorità NIS nazionali, che sarà istituito presso la Presidenza del Consiglio dei Ministri e avrà la funzione di assicurare la collaborazione fra le medesime autorità competenti, che si chiamano autorità competenti NIS e devono assicurare il dialogo e la collaborazione con il CSIRT italiano e il punto di contatto unico verso l'Europa. Anche questa era una previsione del decreto legislativo 65.

Allo stato, però, le autorità NIS, non essendo ancora stato definito il DPCM, già collaborano per la stesura di linee guida, che dovranno essere emanate a breve, quindi ciascuno per il proprio settore di competenza sta lavorando in questa direzione.

Preme ora dire due parole, siccome l'abbiamo nominato più volte, sullo CSIRT che sarà la nuova struttura operante presso la Presidenza del Consiglio. Questo deriverà dalla fusione del *Computer Emergency Response Team* (CERT) nazionale operante presso il MISE e dal CERT della pubblica amministrazione, operante presso l'Agenzia per l'Italia digitale.

Per quanto riguarda il CERT nazionale, di cui l'Italia si era dotata a partire dal 5 giugno 2014, questo era previsto dall'articolo 16-*bis* del decreto legislativo 259 del 2003, modificato dal decreto legislativo 70 del 2012. La *mission* del CERT nazionale che opera presso il Ministero dello sviluppo economico è quella di supportare cittadini e imprese attraverso azioni di sensibilizzazione, per la crescita della cultura della sicurezza e mettere in campo azioni di prevenzione, assicurando il coordinamento della risposta ad eventi cibernetici su vasta scala. Questo è il compito che ha svolto finora e che continuerà a svolgere finché non ci sarà la fusione.

I principali obiettivi sono fornire informazioni tempestive su potenziali minacce informatiche, che possano recare danno a imprese e cittadini, cooperare con le istituzioni analoghe nazionali e internazionali e con altri attori pubblici e privati, promuovendo anche l'interazione fra di essi, facilitare la risposta a incidenti informatici su larga scala, fornire supporto nel processo di soluzione di crisi cibernetica. Utilizza un sito *web* per dare anche delle informazioni, con *news* e bollettini alla cittadinanza, che altrimenti sarebbe difficilmente raggiungibile.

In tale contesto, il CERT nazionale rappresenta il punto di riferimento nazionale per la prevenzione, il monitoraggio, l'analisi e il coordinamento della risposta verso gli altri CERT europei ed extraeuropei, quindi a livello anche mondiale. Per un

funzionamento efficace del CERT, le interazioni con il settore pubblico e con il sistema delle imprese sono state molto importanti, con il settore pubblico ovviamente il CERT della pubblica amministrazione, adesso il Comando interforze operazioni cibernetiche (CIOC) del Ministero della difesa e con il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (CNAIPIC) che opera nel Ministero dell'interno. C'è un continuo e proficuo scambio di informazioni nell'ambito anche dei tavoli di coordinamento che sono attivi presso la Presidenza del Consiglio, in base all'architettura nazionale di *cyber security*.

Le collaborazioni con il settore privato sono regolate da accordi sottoscritti con il settore privato, che hanno attivato una fattiva collaborazione proprio con le strutture di sicurezza di molte imprese che operano nel settore delle telecomunicazioni, dell'energia, del *government*, nel settore finanziario e assicurativo, manifatturiero e anche con altri attori della sicurezza informatica.

Queste imprese hanno sottoscritto con l'Istituto Superiore delle comunicazioni un impegno a scambiarsi informazioni relative a minacce e vulnerabilità, ad organizzare eventi e a lavorare congiuntamente per l'aumento della consapevolezza dei rischi informatici.

Molte delle imprese che gestiscono e utilizzano reti e sistemi informatici fanno parte di un tavolo tecnico permanente, che è stato creato *ad hoc* presso il CERT nazionale per un confronto diretto. Fra di esse rientrano anche gli operatori dei servizi di comunicazione elettronica di cui parlavo prima, quindi le tematiche del 5G passano anche attraverso questo tavolo.

Come ho già detto, con il decreto legislativo il CSIRT è costituito presso la Presidenza del Consiglio dei Ministri, il CERT nazionale sta già procedendo con le azioni di progressiva integrazione delle procedure con il CERT-PA e adesso continua a guidare comunque le sue azioni l'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione presso il MISE per la parte del CERT nazionale, quella che ha riferimento con le imprese.

Dopo questa rapida carrellata delle misure e delle norme più importanti che stanno nascendo a fronte di una consapevolezza davvero aumentata e dalla situazione che i nuovi rischi e le nuove vulnerabilità stanno portando sotto gli occhi di tutti, è opportuno focalizzare la nostra attenzione anche sulla sicurezza dei prodotti che su tali reti sono installati, e in questa prospettiva va letta la recente istituzione del Centro di valutazione e certificazione nazionale (CVCN) presso il Ministero dello sviluppo economico.

Questo centro si aggiunge ad altri due centri già funzionanti presso il Ministero dello sviluppo economico, in particolare presso l'Istituto superiore, che sono l'OCSI, l'Organo di certificazione di sicurezza informatica attivato nel 2004 per prodotti e sistemi ICT commerciali, che naturalmente opera su base volontaria (sono ovviamente prodotti e sistemi a livello commerciale), e il CEVA, il Centro di valutazione della sicurezza informatica di prodotti e sistemi destinati a gestire dati coperti dal segreto di Stato, quindi dati classificati, o di vietata divulgazione. Questi due centri già operavano presso l'Istituto superiore delle comunicazioni.

Sul piano normativo facciamo riferimento ancora al DPCM del 17 febbraio 2017, che ha definito la nuova architettura nazionale a seguito del DPCM del 24 gennaio 2013, il primo che l'ha disegnata. Il citato decreto del febbraio 2017 l'ha modificata e da questo DPCM sul piano normativo rileviamo una previsione relativa alle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica.

In questo DPCM è infatti previsto quanto segue (lo leggo per sottolineare l'importanza della previsione). È previsto che il Ministero dello sviluppo economico promuova l'istituzione di un Centro di valutazione e certificazione nazionale, per la verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità di prodotti, apparati e sistemi, destinati ad essere utilizzati

per il funzionamento di reti, servizi e infrastrutture critiche, nonché di ogni altro operatore per cui sussista un interesse nazionale.

Successivamente, il Piano nazionale per la sicurezza cibernetica e la sicurezza informatica, che viene redatto a valle del quadro strategico e delle azioni definite a livello architetturale, è stato varato dalla Presidenza del Consiglio dei Ministri nel marzo 2017. Questo piano ha precisato che tale Centro sarebbe stato realizzato presso il Ministero dello sviluppo economico, quindi non solo promosso, ma anche realizzato.

In tale contesto, il Centro di valutazione e certificazione nazionale è stato istituito con decreto del Ministro dello sviluppo economico del 15 febbraio 2019 e costituisce soprattutto in prospettiva un importante tassello ai fini della sicurezza cibernetica del Paese. Il centro è stato istituito presso l'Istituto Superiore delle comunicazioni e tecnologie dell'informazione forse anche per la competenza acquisita negli anni nel settore della certificazione informatica.

La fase di progettazione del centro è stata ultimata ed è in corso di completamento la definizione delle procedure per il suo funzionamento, perseguendo l'obiettivo generale di contemperare gli aspetti di sicurezza e le esigenze di mercato delle imprese coinvolte, che ovviamente non vanno mai dimenticate in questo momento così complesso. Il 19 aprile 2019 è stato firmato il decreto che descrive il modello di funzionamento, l'organizzazione e il piano di sviluppo del CVCN, così come previsto dal decreto del Ministro dello sviluppo economico.

La sua operatività si svilupperà secondo un approccio graduale sulla base delle risorse umane e finanziarie disponibili, quindi al di là degli aspetti tecnici di realizzazione del centro, l'impatto delle sue attività dipenderà da una serie di fattori e anche dalla definizione di un quadro normativo che individui bene le infrastrutture critiche strategiche, problematica già all'attenzione delle componenti governative che hanno in carico questi problemi, e dovrebbero essere stabiliti specifici obblighi per l'acquisizione di prodotti e sistemi destinati a queste infrastrutture.

Tale quadro dovrà tenere anche conto delle disposizioni sulla realizzazione di un *framework* a livello europeo. Aggiungiamo un'altra componente di complessità o forse a breve di maggiore chiarezza, perché questo nuovo *framework* è stato approvato con un regolamento di prossima pubblicazione (lo aspettiamo a giorni) che è stato approvato dall'Unione europea ed è noto come *Cyber Act*. In pratica, è un *framework* unico affinché le imprese non si debbano confrontare con tanti modelli di certificazione diversificati, cosa che può portare a complicazioni anche nello sviluppo del mercato. Ovviamente ogni schema a livello nazionale dovrà poi confrontarsi con le previsioni di questo regolamento europeo.

Questo regolamento prevede fra l'altro anche il rafforzamento del mandato dell'ENISA (Agenzia europea per la cybersicurezza), istituisce un perimetro normativo comune per la certificazione della sicurezza informatica e mira a rafforzare anche il mercato digitale dell'Unione, perché in questo modo si dovrebbe guadagnare anche un'affidabilità maggiore dei prodotti e una consapevolezza maggiore degli utenti.

In questo nuovo contesto che prevede la costituzione dei sistemi europei e nazionali di certificazione di prodotti e servizi il nostro Paese, anche con il grande contributo del Ministero dello sviluppo economico, si trova assolutamente in linea e sta cercando di seguire, monitorare e partecipare attivamente a qualsiasi iniziativa. Grazie.

PRESIDENTE. Ringrazio la dottoressa Forsi per il suo contributo e dichiaro conclusa l'audizione.

Audizione di rappresentanti del Servizio di polizia postale e delle comunicazioni del Ministero dell'interno.

PRESIDENTE. L'ordine del giorno reca, nell'ambito dell'indagine conoscitiva sulle nuove tecnologie delle telecomunicazioni, con particolare riguardo alla transizione

verso il 5G ed alla gestione dei *big data*, l'audizione di rappresentanti del Servizio di polizia postale e delle comunicazioni del Ministero dell'interno.

Ringrazio i rappresentanti del Servizio di polizia di polizia postale e delle comunicazioni del Ministero dell'interno per aver accettato l'invito della Commissione.

Do la parola alla dottoressa Nunzia Ciardi, direttrice del Servizio, per lo svolgimento della relazione.

NUNZIA CIARDI, *direttrice del Servizio di polizia postale e delle comunicazioni del Ministero dell'interno del Ministero dell'interno*. Grazie, presidente, buongiorno a tutti. Viene detto da più parti, e io sono assolutamente d'accordo, che in una società moderna coniugare efficacemente le opportunità che tutti i mezzi informatici ci offrono con le esigenze di protezione dalla minaccia *cyber,* che oggi più che mai è una minaccia assolutamente insidiosa, è una delle sfide fondamentali perché lo sviluppo economico e sociale di un Paese e di una convivenza civile sia assicurato.

Fornisco alcuni dati per dare l'idea di quale sia lo scenario in cui ci muoviamo. Il *cyber crime* oggi è la principale causa di attacchi, attacchi dei quali i quattro quinti sono effettuati per ottenere denaro o dati che successivamente verranno monetizzati, perché, come vedremo e come cercherò di rappresentare in questa breve esposizione, la vera miniera d'oro oggi nel *cyber crime* e in generale nella società digitale sono i dati, dati sensibili, dati di ogni tipo che ognuno di noi mette e consegna volontariamente alla rete.

Vediamo l'*escalation* che il *cyber crime* ha avuto negli anni. Ogni anno dagli addetti ai lavori viene definito l'*annus horribilis* del *cyber crime* e il 2018 è stato l'anno peggiore di sempre, come ogni anno è l'anno peggiore di sempre, perché l'aumento è sempre esponenziale, perché come esplode la digitalizzazione della società parallelamente esplode il crimine digitale.

Vediamo che nel raffronto tra il 2014 e il 2018, quindi in un quadriennio, gli attacchi gravi (non gli attacchi generici) sono aumentati di oltre il 77 per cento, quindi un aumento percentuale che rasenta l'80 per cento, quindi parliamo di aumenti estremamente consistenti. Lo studio si basa su un campione che riguarda attacchi di particolare gravità, quindi non parliamo degli attacchi di tutti i giorni, che sono quelle *mail* estorsive che ognuno di noi riceve, « vi abbiamo visto il computer, abbiamo visto la tua navigazione, abbiamo visto che visitavi siti porno, se non vuoi che diffondiamo il tuo video dacci questa determinata somma in bitcoin », oppure l'attacco *ransomware* che avviene in uno studio legale, per cui ti criptano tutti i dati e sei quindi costretto a barcamenarti, o pagare per riottenere la decriptazione dei dati oppure avere tutto il tuo materiale professionale inutilizzabile perché criptato. Qui, invece, parliamo di attacchi gravi. Sono in aumento però anche gli attacchi ordinari.

Come dicevamo, ogni anno è il peggiore di sempre fino ad adesso, perché l'evoluzione è un continuo *trend* di crescita. Gli attacchi gravi sono aumentati di 10 volte nell'ultimo biennio e del 37,7 per cento rispetto all'anno precedente. Vediamo che il peggioramento non riguarda soltanto la quantità degli attacchi, ma la cosa più grave è che riguarda la qualità degli attacchi: gli attacchi sono non solo sempre di più, ma anche sempre più gravi, e questo è un dato particolarmente preoccupante.

Un altro dato che risulta significativo rappresentare è che questi aumenti che stiamo illustrando non sono esaustivi dello scenario criminale, perché un grandissimo numero di aggressioni non diventa mai di dominio pubblico. In altre parole, esiste (non a caso si cita l'immagine dell'iceberg) un sommerso di aggressioni rilevantissimo, che non viene mai reso noto o viene reso noto soltanto a distanza di tempo, quando fa meno male il danno di immagine.

Perché molti non sono denunciati ? Perché gli attacchi alle aziende piccole o grandi, alle pubbliche amministrazioni piccole e grandi costituiscono un danno di immagine enorme. È evidente che una banca o una grande azienda che denunci il furto di dati contenuti al proprio interno, quindi di dati di clienti (di recente

una società americana enorme ha denunciato un attacco di tutti i clienti dell'azienda con tutti i loro dati, compresi quelli economici, le carte di credito) se sono utente di un sito e so che i miei dati in quel sito non sono stati al sicuro, hanno rubato i miei dati finanziari oltre che quelli personali, è chiaro che tendo a non fidarmi più di quell'azienda, di quel marchio, di quella struttura.

Questo è uno dei motivi principali per i quali le aziende, se possono, tengono all'interno del proprio perimetro la notizia dell'attacco o dell'esfiltrazione di dati, tanto che le recentissime normative per determinate aziende che erogano servizi essenziali o di rilievo pubblico impongono la denuncia, perché ovviamente la denuncia tutela i titolari dei dati.

Un motivo più banale è che a ricevere per prima la notizia di un attacco e a vederne per prima le evidenze di un'esfiltrazione di dati è la struttura che deve badare alla sicurezza dell'azienda stessa, quindi le prime teste a cadere, per cui ci sono interessi contrapposti che rendono estremamente complicato far emergere gli attacchi. Nonostante questo, abbiamo visto quale sia la percentuale di aumento e questo ci dà uno scenario veramente fosco del *cybercrime* oggi, in tutti i Paesi del mondo e nel nostro Paese che, essendo una delle società sviluppate, è ai primi posti per gli attacchi subìti.

Sappiamo che il *cybercrime* generico, cioè quello dovuto alla monetizzazione degli attacchi, rappresenta la percentuale più alta. Più bassa, anche se molto insidiosa è l'attivismo, gli attacchi compiuti per ragioni varie, ascrivibili alle formazioni antagoniste, lo spionaggio industriale, fino alla guerra delle informazioni, cioè quegli attacchi dovuti a potenze ostili nei confronti del nostro Paese.

Dirigo la polizia postale e delle comunicazioni, che è il segmento di Polizia di Stato che fa contrasto al *cybercrime* nel suo complesso ed è l'organo centrale del Ministero dell'interno che assicura la sicurezza (scusate il gioco di parole) delle telecomunicazioni. Siamo organizzati in un Servizio centrale, quello che io attualmente dirigo, dal quale dipendono 20 uffici di livello regionale e 80 uffici di livello provinciale, tutti impegnati in questa sfida contro il *cybercrime*.

All'interno del servizio centrale ci sono tre centri operativi *h24*: un centro dedicato alla tutela delle infrastrutture critiche del Paese; un centro dedicato al contrasto di quel triste fenomeno che è la pedopornografia *on line*; un commissariato di Polizia di Stato *on line* che riceve denunce e segnalazioni e dà informazioni sui fenomeni più rilevanti del *cybercrime* ai cittadini.

Dicevo che la polizia postale si occupa di *cybercrime* nel suo complesso, ma ha delle aree di riferimento, delle macroaree sulle quali concentra la sua attività, che sono in particolare quelle dove abbiamo una competenza esclusiva o prevalente. Con esclusiva intendo che siamo l'unica Forza di polizia dedicata a questo tipo di crimine: gli attacchi *cyber* e la protezione delle infrastrutture critiche; la pedopornografia *on line* e tutti i reati di aggressione *on line* ai minori.

La rete ci ha fatto vedere in questi ultimi anni che la pedopornografia non è l'unico gravissimo reato a danno dei minori sulla rete. Basta citare – non mi dilungherò – il *revenge porn*, il cyberbullismo, le estorsioni sessuali, i siti che incrementano le patologie alimentari gravissime, come anoressia, bulimia, uno spettro amplissimo, fino ad arrivare agli ultimi casi di sfide, che *on line* trovano terreno fertile e nelle quali i ragazzi si cimentano fino a esiti fatali, come nel caso del ragazzo che con un sacchetto di nylon in testa, cercando quell'euforia descritta *on line* che è susseguente alla sensazione di soffocamento, è rimasto ucciso con questo tipo di pratica. La competenza inizialmente circoscritta ai reati pedopornografici si è, quindi, allargata a tutti i reati che toccano i minori *on line*.

Per inciso, l'ultimo rapporto Censis ci dice che gli italiani, intervistati su quale fosse il reato che temevano di più *on line*, hanno risposto: i reati di aggressione *on line* come il cyberbullismo. È un reato che preoccupa oltre il 42 per cento degli italiani. È il primo reato che preoccupa oltre il 42 per cento degli italiani.

Poi abbiamo il cyberterrorismo, cioè tutta quell'opera di propaganda e radicalizzazione *on line* che porta poi alla formazione di un'ideologia terroristica, in specie attualmente quella di matrice religiosa; il crimine finanziario, che è un'altra delle nostre competenze e che attualmente ci vede più preoccupati, e diremo perché, fino ad arrivare ai reati postali.

Lo scenario degli attacchi *cyber*, come ho cercato di dire in breve e cercando di essere sintetica nonostante la materia sia vastissima, ha ormai da tempo superato i livelli di guardia nel nostro Paese, rappresentando una delle principali minacce, se non la principale minaccia, alla tenuta economica del Paese.

In questo noi vediamo che fattori determinanti sono innanzitutto la capillare accessibilità di *software*. Oramai, la globalizzazione ha colpito anche su quello. *Software* malevoli che servono per colpire e per realizzare crimini anche di altissimo livello si trovano comunemente nel *dark Web* a cifre economiche decisamente modeste. Questo porta a un disequilibrio di fondo, una regola che tra addetti ai lavori si conosce bene, che è quella simmetria per la quale è difficile difendersi: per attaccare ci possono volere pochissime risorse economiche, mentre per difendersi ce ne vogliono tantissime.

Per realizzare la difesa di un'azienda, di una struttura, di un'amministrazione pubblica, di una struttura sanitaria, e non lo dico a caso – vedremo di quanto sono aumentati gli attacchi ai dati sanitari in questo ultimo anno, dati delicatissimi di ciascuno di noi – ci vuole un investimento consistente. Per attaccare può bastare investire pochissime risorse.

Questo è alla base – lo vedremo – della trasformazione che ha avuto la cybercriminalità oggi. Abbiamo evidenze nelle nostre investigazioni che le organizzazioni criminali a livello internazionale, le più « professionali », così come le mafie nazionali, si sono buttate a capofitto in questo settore.

Qual è l'analisi del dato ? Un *cybercrime* che consente grandissimi introiti, grandissimi compensi all'attività criminale, con un rischio relativamente modesto. In questo scenario è proprio il dato, l'informazione – lo accennavo prima – che immettiamo in rete a essere veramente la miniera d'oro, il filone d'oro di questi tempi, le informazioni che ognuno di noi mette in rete senza rendersene nemmeno conto.

Mi riferisco, ad esempio, alle informazioni economiche. Tutti noi siamo abituati a comprare *on line* e a inserire i dati della nostra carta di credito su PayPal o sul circuito finanziario di riferimento, facendo la spesa ovunque. Mi riferisco ai nostri dati sanitari. Parlavo l'altro giorno con un docente universitario che mi descriveva tutti gli sforzi che stavano facendo per mettere in un'unica banca dati tutti i referti delle varie prestazioni radiologiche (TAC, risonanza magnetica, lastre), in un unico archivio, prima provinciale e poi magari nazionale. Ovviamente, per la medicina sarebbe un passo in avanti grandioso. Vado in un ospedale con una frattura e loro sono in grado di collegarsi al mio archivio digitale e vedere tutte le varie prestazioni che ho avuto senza dover rifare accertamenti sanitari, senza andare a richiederli. Pensate alla delicatezza di un *database* di questo tipo.

Anticipo un dato che avrei illustrato dopo: dall'anno scorso a quest'anno, le aggressioni ai dati sanitari sono aumentate del 99 per cento, *del 99 per cento*, in una progressione spaventosa in cui il criminale che esfiltra dati di questo tipo è in grado di conoscere tutto, con tutte le conseguenze che un tipo di esfiltrazione del genere può creare.

Andiamo al crimine finanziario cui accennavo. Attualmente, è uno dei settori che ci preoccupa maggiormente. Parliamo di attacchi finanziari alle piccole e medie aziende, così come alle grandi imprese, tesi a sottrarre somme di denaro rilevantissime. La polizia postale quest'anno ha ricevuto, rispetto all'anno precedente, un aumento del 320 per cento di segnalazioni di attacchi alle aziende per prendere denaro. A più 170 per cento ammontano gli importi sottratti a grandi e piccole aziende. Sostanzialmente, succede questo.

I criminali si introducono grazie a un attacco informatico nel DNA di un'azienda, ne rubano tutti i segreti e ne mappano tutti i recessi più reconditi. Sono in grado di conoscere l'intera struttura di un'azienda, compresa tutta la corrispondenza che l'azienda ha con i propri fornitori, con i propri clienti e così via. Grazie a questo patrimonio e a tecniche di *social engineering*, inducono l'azienda a versare somme indebite su conti correnti criminali.

L'ultima denuncia che abbiamo ricevuto riguarda una grande azienda italiana che ha pagato 18 milioni di dollari. Mediamente, le somme si aggirano tra i 500.000 euro e gli 8-10 milioni di euro sottratti alle aziende grazie ad attacchi informatici che consentono al criminale di conoscere tutta la struttura e tutte le persone che in quell'azienda lavorano.

È evidente che, quando parliamo di somme di questo tipo, quando parlo di 18 milioni di dollari in mano al criminale che li ha sottratti, non parliamo di quattro *hacker* venuti in possesso di una somma. Per rubare 18 milioni di dollari, hai bisogno innanzitutto di una struttura professionale sofisticatissima, ma non solo. Hai bisogno di una rete di riciclatori, di gente che investe questo denaro, che riesce a prelevarlo. Non è il singolo. È ovvio che c'è una struttura criminale dietro, che peraltro reinveste queste somme sotto il profilo criminale, realizzando profitti sempre maggiori. Ed è un'escalation alla quale assistiamo e stiamo assistendo in questi anni.

Abbiamo virus informatici sempre più sofisticati, strategie di *social engineering* che consentono al criminale informatico di ricostruire la personalità. C'è un grande giornalista che dice che oggi chiunque di noi attraverso *Google* può ricostruire l'identità di una persona con tutti i gusti, le persone frequentate, sostanzialmente mappare la vita di una persona, in cinque minuti, molto meglio di quanto la CIA potesse fare trent'anni fa nelle sue attività investigative, e questo soltanto attraverso le fonti aperte, consultando *Google*. Se voglio sapere chi è una determinata persona, la cerco su *Google*, e ho una miniera di informazioni enorme. Pensate a un criminale che, oltre a questo, si può introdurre in banche dati che gli consentono di profilare nel dettaglio una persona, fino ai suoi dati sanitari per esempio.

Quest'anno, per esempio, è stato rilasciato l'aggiornamento per questo tipo di dispositivo che consente di fare l'elettrocardiogramma che posso inviare al mio medico. Ovviamente, tutto questo è in *cloud* e sono dati che io volontariamente sto consegnando alla rete e che, se non sono ben protetti, possono andare in pasto a chiunque, così come la mia opinione religiosa, la mia tendenza sessuale. Quando andiamo in un negozio e ci fanno una tessera e ci chiedono i nostri dati, sono in grado di profilarci commercialmente. Viviamo in una società in cui il dato è assolutamente moneta sonante.

Tutti gli attacchi che vediamo, gli attacchi spiccioli di cui parlavo prima, quelle singole *e-mail* mandate a tutti e che ci dicono che hanno violato il nostro computer, che sono stati in grado di filmarci mentre vedevamo video pornografici, che in oggetto portano la nostra *password*, la *password* che noi riconosciamo, e per questo ci allarmiamo, e noi riceviamo migliaia di telefonate allarmate – le persone sono convinte effettivamente di essere di fronte a qualcuno che è entrato nel loro computer, che li ha filmati nelle loro case, nei loro uffici, perché sono in possesso anche della loro *password* – queste campagne massicce di *e-mail* inviate provengono proprio da precedenti esfiltrazioni da banche dati violate e grazie alle quali sono venuti in possesso della mia *e-mail*, della mia *password*, della mia data di nascita.

In grande, sono dati utilizzati per attacchi informatici di questo tipo; in piccolo, per campagne capillari di questo genere di estorsione, motivo per il quale tra le raccomandazioni dico sempre di non usare assolutamente la stessa *password* per più siti. È una pratica logicamente molto comoda per tanti. Si usa una *password* considerata sicura, magari difficile, per più siti. Questo significa che il criminale che buca una banca dati, e quindi conosce la

mia *e-mail* e quella *password*, la prova in tutti gli *account* collegati alla mia *e-mail*: se la *password* è la stessa, entra in tutti i miei *account*. Una buona norma è quantomeno quella di utilizzare *password* diverse per ogni sito frequentato.

Dicevo del sistema sanitario. Gli ultimi attacchi di cui tutti probabilmente avete avuto notizia e ricordate dalle prime pagine di tutti i giornali sono *WannaCry* e PITA, i due virus che a livello mondiale sono stati forse tra i primi esempi di attacco su scala planetaria. *WannaCry*, nelle prime tre o quattro ore in cui ha colpito, ha criptato i dati delle strutture sanitarie, soprattutto in Gran Bretagna. Sono stati quasi una decina gli ospedali che hanno dovuto chiudere le strutture di pronto soccorso, e quindi rimandare interventi chirurgici, accertamenti di tipo radiologico, perché tutte le banche dati erano criptate, e non accedevano quindi più a nulla, comprese le cartelle cliniche.

Tutto questo ci ha fatto rendere conto che i dati sanitari devono essere inseriti anche loro in un perimetro di tutela. Noi stiamo per lanciare un progetto in cui, oltre a quel centro che vi dicevo prima di tutela delle infrastrutture critiche, inaugureremo a livello regionale dei centri che tuteleranno anche la sanità sul territorio, in un rapporto pubblico/privato che cercherà di mettere a frutto e a fattor comune tutte le informazioni delle quali come Polizia di contrasto al *cybercrime* veniamo in possesso.

Andiamo direttamente al tema del 5G, altrimenti temo che non ci sarà tempo per le domande.

Tutti noi sappiamo più o meno come funzionerà la rete 5G. Come per le altre reti radiomobili, si baserà su un sistema di antenne, antenne terrestri distribuite sul territorio in diversi settori, detti celle, lungo una dorsale detta *backbone*. Qual è il problema del 5G ?

È una rete attraverso la quale riuscirà a passare una mole enorme di dati, incomparabile con quella attuale. Avrà, innanzitutto, una velocità di connessione decisamente maggiore. Diminuirà la latenza della connessione. Significa che, rispetto al dato che io chiederò, i tempi di attesa saranno ridottissimi. Questo velocizzerà tutte le connessioni, velocizzerà lo scambio di dati, e soprattutto supporterà la connessione contemporanea di tantissimi dispositivi.

Con il famoso IOT, l'*internet* delle cose, avremo decine di dispositivi connessi che potranno accumulare dati e saranno i dispositivi delle nostre case, la famosa domotica, il sistema di riscaldamento collegato alla rete, il sistema di illuminazione delle nostre case collegato alla rete, fino a dispositivi come elettrodomestici vari, che accumuleranno dati, saranno collegati alla nostra rete, saranno teoricamente violabili, come è violabile ogni sistema di accumulo di dati. E si arriverà – è noto che ci sono gli studi per la guida automatica – a macchine che si guideranno da sole. Anche quello sarà un sistema, quindi potenzialmente violabile.

Che cosa ci dice l'introduzione del 5G ? Da una parte, ci saranno enormi potenzialità, potenzialità di sviluppo economico, potenzialità di utilizzo di una tecnologia sofisticatissima, che contrarrà i tempi di utilizzo, e quindi sarà molto efficace a livello sia individuale sia di aziende.

Quali sono, però, i problemi di una tecnologia così potente, che accelererà tantissimo i processi di scambio ? Avrà anche come contraltare enormi rischi che si acuiranno. Rischi che si sono già acuiti con il 4G diventeranno ancora più insidiosi con il 5G.

Tra i rischi teorici di cui attualmente parliamo, c'è l'ostacolo all'esatta identificazione e localizzazione dei dispositivi mobili.

C'è da dire che il 5G non farà altro che approfondire la connessione in mobilità. Noi siamo abituati a ragionare in termini di decenni, ma qui la progressione della tecnologia è talmente veloce che nel giro di pochi mesi tutto cambia in modo sostanziale. Io cito sempre un dato: nel 2009, gli italiani che avevano uno *smartphone*, quindi che si connettevano in mobilità, erano all'incirca il 15 per cento della popolazione. Tutti gli altri usavano il telefono per telefonare, punto.

Nel 2017, gli italiani che hanno uno *smartphone* sono oltre il 75 per cento. Questo significa che la quasi totalità degli italiani – nel 75 per cento ci sono, ovviamente, neonati, bambini, tutta la popolazione – vive perennemente connessa. Non aspetta di tornare a casa per connettersi, ma vive in continua connessione col proprio dispositivo mobile.

Il 5G accelererà completamente questa tendenza. Vedo un certo fermento. Questo, ovviamente, renderà più complessa la gestione del crimine informatico.

Che cosa sarà necessario fare ? Innanzitutto, sarà necessaria un'attenta valutazione dei gestori di queste infrastrutture di comunicazione, attraverso le quali passeranno e passeranno in maniera massiccia tutti i dati che riguardano ogni persona; intensificare a ogni livello l'attività di protezione delle reti.

Soprattutto, in questo scenario così inquietante che mi rendo conto di aver descritto c'è un dato di complicazione fondamentale: non si può pensare di lavorare soltanto con la legislazione nazionale in un settore fondamentalmente transnazionale. Quando parliamo di crimine, di *cybercrime*, parliamo quasi sempre di reati che avvengono coinvolgendo diverse parti del mondo. Pensiamo soltanto alle nostre continue interazioni con i *social network*: non c'è un *social network* che sia italiano sul quale noi abbiamo diretta giurisdizione. Dobbiamo sempre chiedere a un altro Stato. E questo avviene in tutto il settore del *cybercrime*, perché la rete è fondamentalmente transnazionale.

Occorre, quindi, uno sforzo, in parte già fatto, per esempio sui tavoli europei. Noi siamo in molte sessioni per cercare di uniformare il più possibile. Pensiamo soltanto al problema di conservazione dei dati. Se io voglio accertare un dato, chi si è connesso a quel determinato sito, e lo chiedo ai *provider* telefonici, ogni *provider* telefonico al mondo ha l'obbligo di tempi diversi per conservare quel dato. In Italia, i dati telematici mi possono essere dati entro un anno. In altri Paesi, ci sono tempi più lunghi.

Molti sforzi, quindi, sono già stati fatti per uniformare la legislazione, ma altrettanti ne vanno ancora fatti, così come anche la legislazione nazionale dovrà tener conto delle maggiori esigenze di tutela dei dati e di contrasto al *cybercrime* nelle proprie legislazioni nazionali.

PRESIDENTE. Grazie, dottoressa Ciardi.

Do ora la parola agli onorevoli colleghi che intendano intervenire per porre quesiti o formulare osservazioni.

FEDERICA ZANELLA. Intervengo, innanzitutto, per ringraziare la dottoressa Ciardi e il dottor Cervellini. La relazione della dottoressa Ciardi è stata molto completa, direi molto interessante sotto molti profili, anche nella parte non specificamente riguardante il 5G.

Noi abbiamo sempre parlato molto di cyberbullismo e ci è capitato tante volte di essere a un tavolo insieme, ma capire la portata del *cybercrime* è sinceramente molto importante, soprattutto perché devo dire che il profilo della sicurezza e della possibilità che i dati siano hackerati è uno dei temi sui quali chiediamo sempre di esprimersi a tutti coloro che vengono a parlarci di 5G, anche alle società che sviluppano il 5G.

Sulle infrastrutture abbiamo appreso qualche giorno fa che per esempio Huawei, che forniva Vodafone, aveva delle *backdoor* che non ha mai chiuso, per cui probabilmente una serie di dati è stata illecitamente sottratta anche da realtà straniere, Nazioni straniere. Questo sarà ovviamente da approfondire ed esperire.

Sicuramente, però, voi ci date conferma dei nostri timori. Tutte le volte chiediamo: sotto il profilo della sicurezza dei dati, ci sono dei maggiori *vulnera* ? Tutti ci dicono che sì, sicuramente, ma che cercano di anonimizzare i dati e altro, ma è evidente che la problematica relativa al furto dei dati personali e a possibili tracciature molto sofisticate è qualcosa a cui il 5G ci espone. La ringrazio perché purtroppo ha confermato quello che noi temiamo da molto tempo.

Se ci sono altre considerazioni in più da aggiungere sotto questo profilo, sarebbe

interessante capirlo, in ogni caso grazie per il suo intervento davvero molto intervento.

PAOLO NICOLÒ ROMANO. Ringrazio i relatori, per la loro relazione direi molto esaustiva.

Vorrei capire se avete delle proposte, dei suggerimenti, per poter migliorare la sicurezza in generale. Va bene mettere una *password* diversa, e io suggerisco sempre anche di mettere una doppia protezione con un *token*, che sicuramente garantisce una protezione maggiore, ma penso che sia un suggerimento più per il singolo utente, non per un'amministrazione. A livello di legislatore, sarebbe interessante capire quali iniziative si potrebbe intraprendere per migliorare quest'aspetto.

Una su tutte, sicuramente ci sarebbe da investire maggiormente in questo settore, lo posso anticipare, ma vorrei capire se avete anche altre idee che si possono portare avanti.

NUNZIA CIARDI, *direttrice del Servizio di polizia postale e delle comunicazioni del Ministero dell'interno del Ministero dell'interno*. Sicuramente, gli investimenti maggiori sono decisivi. Pensiamo, per esempio, a *WannaCry*, che colpiva i sistemi non aggiornati. Ha colpito gli ospedali inglesi che avevano XP, che non era aggiornabile. Non è che le strutture informatiche degli ospedali non volessero aggiornare. È ovvio che, se hai XP, non aggiorni. Per avere dei sistemi aggiornabili, e quindi nuovi, devi investire. La pubblica amministrazione, le strutture sanitarie dovrebbero avere sistemi aggiornabili, e quindi più sicuri. Quello dipende dagli investimenti. Dipende anche dalla consapevolezza, ma anche dall'investimento economico.

Bisogna poi lavorare molto a livello internazionale per uniformare le norme. Per cercare di combattere il crimine, non è sufficiente che io faccia una legge nel mio Paese se poi mi rivolgo a uno Stato diverso dal mio per ottenere dei dati e lui non me li dà, perché non li conserva o perché non ritiene per la legislazione... È un'informazione che conoscono tutti, completamente sdoganata, che quando c'è una diffamazione su *Facebook*, chiedere i dati a *Facebook* è inutile perché per gli americani la diffamazione non è reato, per cui loro non consegnano dati in quanto il loro ordinamento giuridico tutela completamente la libertà di espressione. Questo è soltanto un esempio, ma per dire che l'armonizzarsi di diverse legislazioni è fondamentale.

Inoltre, abbiamo il problema in Italia che i dati vengono conservati, ora per più tempo, ma possono essere consegnati solo per motivi di terrorismo dopo un tempo maggiore. Se voglio investigare su altro, dopo un anno non posso più avere dati informatici, perché per ragioni di *privacy*, di tutela della sfera individuale e così via, un anno viene considerato un termine oltre il quale non si può andare per ottenere certi dati, neanche per fini investigativi. Forse, anche su questo una riflessione potrebbe essere fatta.

Ci sono molti aspetti sui quali secondo me bisogna imparare a riflettere tenendo un occhio su questo tipo di criminalità, peraltro una delle poche criminalità veramente in crescita, e in crescita così rilevante.

BERNARDO MARINO. Anch'io ringrazio la dottoressa Ciardi per l'esposizione.

Come probabilmente saprete, questo Parlamento sta ponendo l'accento sul reato del *revenge porn*, con una condivisione politica da parte di tutte le forze presenti, per cercare di punire questo reato prettamente informatico.

Siccome tra le varie ipotesi c'è anche quella di punire, oltre che chi mette *on line* certe immagini, anche chi le condivide, questo dà l'idea della complessità della situazione. Come polizia postale sarete sicuramente in prima linea, perché siete quelli che dovranno appurare questo tipo di reato: come immaginate, come vedete questo scenario in cui si prefigura una nuova fattispecie di reato sul *revenge porn* che vada a colpire non soltanto chi mette in rete le immagini, ma anche la immagino sterminata platea di potenziali condivisori ? Come immaginate questo scenario che si sta affacciando ?

NUNZIA CIARDI, *direttrice del Servizio di polizia postale e delle comunicazioni del Ministero dell'interno del Ministero dell'interno*. Purtroppo, il *revenge porn* è uno dei reati che veramente ci ha visto maggiormente impegnati negli ultimi anni.

È una forma di reato che deriva dal *sexting*. Ormai, la pratica di scambiarsi immagini sessualmente esplicite, immagini intime, è estremamente diffusa. E questo ha portato successivamente a queste forme terribili di immissione in rete di immagini intime senza il consenso della persona interessata.

Tutto questo è possibile grazie al potere di replicazione tremendo della rete di un'immagine infilata in rete, mandata su un gruppo *WhatsApp*. Noi vediamo spesso i ragazzi. Una coppia di sedicenni si scambia immagini intime e poi il ragazzo, magari perché lasciato, per vendetta, immette la foto nuda della ragazza sul gruppo *WhatsApp* di classe o la manda all'amico del cuore.

È poi la replicazione successiva che rende virale l'immagine. Quella foto nel giro di un'ora è in possesso di mezza città, nell'ora successiva dell'intero Paese. È un meccanismo di replicazione infernale che diventa stritolate per la vittima.

È estremamente corretto che sia stata individuata una fattispecie specifica per il *revenge porn*. Prima, le normative applicate o applicabili c'erano, ma erano non attagliate su quel tipo di danno fatto alla vittima. C'era la violazione della *privacy*, poteva essere configurato uno *stalking*, una diffamazione, fattispecie di reato che potevano essere applicate al fatto in esame, però una fattispecie specifica, che è questa diffusione gravissima di immagini lesive intime senza il consenso dell'interessato, che quindi provoca un danno enorme alla persona che si vede in questo modo alla mercé di tutti coloro che hanno condiviso quest'immagine, è quanto mai opportuna.

Punire chi inoltra determinate immagini è sicuramente un mezzo efficace, che però deve andare di pari passo con una cultura dell'educazione e della consapevolezza. Molto spesso, chi riceve un'immagine, la inoltra a un gruppo di amici senza rendersi conto che sta commettendo un reato gravissimo. Ci potremmo trovare di fronte a intere scolaresche che hanno inviato quest'immagine, e quindi imputabili di un reato di questo tipo.

È giusto che la normativa preveda certe fattispecie, ma è altrettanto giusto che si lavori in termini di consapevolezza, nel rendere noto a tutti quanto possa essere potenzialmente lesivo per la parte che si vede messa in rete in questo modo, ma anche relativamente al rischio che si corre penalmente a livello individuale nell'inoltrare un'immagine di questo genere.

Noi, per esempio, a proposito dell'intervento dell'onorevole che citava le nostre collaborazioni, siamo molto impegnati nelle scuole. Andiamo quotidianamente a compiere un'attività di educazione alla navigazione nelle scuole, e diciamo anche questo: inoltrare un'immagine non è qualcosa che non ha conseguenze, non solo di tipo etico o di tipo aggressivo nei confronti della vittima, ma anche penali per noi stessi. Vediamo che molto spesso le persone non hanno chiara questa conseguenza, non sono consapevoli. Parliamo di ragazzi che non si rendono conto di aver commesso la violazione di una regola.

FEDERICA ZANELLA. Scusi, intervengo velocemente.

Di fatto, la fattispecie di reato di cui stiamo discutendo nasce da un emendamento che ho presentato io. Poi abbiamo elaborato un emendamento condiviso anche da altri gruppi parlamentari. Noi avevamo due proposte di legge, e in effetti la proposta di legge del Movimento 5 Stelle non prevedeva il *sexting* di secondo grado, l'inoltro. Quello è stato un tema su cui abbiamo dibattuto. Abbiamo pensato, però, che la fattispecie lesiva fosse rappresentata dal *rebound*, che quindi dovesse essere punito. Poi starà al giudice, ma ricordo che alla fine tutti in Parlamento abbiamo giudicato assolutamente importante – tante volte abbiamo parlato insieme ai ragazzi – inserire un reato che non si rifà a quello di diffamazione, al *sexting* o allo *stalking*, in un codice rosso che prevedesse appunto tutte violazioni di genere, in realtà. Sappiamo che non è solo una questione di genere, ma una tutela della persona sul

Web in generale, anche se molto spesso sono le ragazze le vittime.

Volevo spiegare la genesi, perché in effetti sul *sexting* secondario, sul reinoltro, c'è stata un po' di discussione prima della stesura finale dell'emendamento comune. Ritengo che abbiamo fatto una cosa giusta. È giusto dare consapevolezza del fatto che inoltrare la prima volta è un reato, ma lo è pure rendersi complici anche solo con un « like », che trasmettiamo sempre che è quello che fortifica e che induce spesso il ragazzo a postare la scena di bullismo, che gli fa ottenere tanti « *like* » e gli fa avere il suo accreditamento sociale. Sarebbe troppo punire il « *like* », ma sicuramente ci sembrava corretto porre la fattispecie lesiva per il *rebound*.

PRESIDENTE. Grazie, collega Zanella. Mi scuso con il collega Marino, che prima ho impropriamente citato. Avrei anch'io, dottoressa Ciardi, una domanda.

Nella sua relazione, tra l'altro molto esaustiva e approfondita, ha fatto riferimento alla criminalità organizzata. Vorrei conoscere, nei limiti di quello che è possibile esporre in questa sede, le evidenze che avete come polizia postale dell'entità delle attività che la mafia e altre organizzazioni criminali organizzate fanno nell'ambito del *cybercrime*.

Do la parola al nostro ospite per la replica.

NUNZIA CIARDI, *direttrice del Servizio di polizia postale e delle comunicazioni del Ministero dell'interno del Ministero dell'interno*. In diverse attività investigative abbiamo notato questo coinvolgimento. Una delle ultime, per esempio, che abbiamo svolto in collaborazione con la Polizia rumena, proprio relativa al crimine finanziario, ci ha reso evidente che tra gli arrestati c'erano personaggi di spicco legati alle 'ndrine calabresi, arrestati in Romania.

Vediamo sempre più spesso che la criminalità organizzata investe in questo campo anche comprando pacchetti professionali. Nel *dark web*, oltre al singolo *software*, ai singoli strumenti che occorrono per attaccare per esempio un'azienda, è possibile trovare disponibili prestazioni professionali che si comprano. Laddove un'organizzazione criminale ha una schiera di reclutatori, una schiera di organizzatori dell'attività, ci sono anche gli informatici le cui prestazioni si comprano sul *dark Web*, che servono poi a realizzare l'intera fattispecie. Da diverse indagini abbiamo tratto quest'evidenza, che logicamente rende tutto molto più preoccupante.

PRESIDENTE. A proposito di quest'ultima informazione e citando anche quello che ha ricordato all'inizio di questa relazione, ha detto che c'è un'evidente asimmetria tra il costo della difesa e il costo dell'attacco.

Vorrei comprendere se il personale in dotazione, in forze al centro che lei presiede e guida, è sufficiente, visto anche la crescita esponenziale degli attacchi. È immaginabile il coinvolgimento di altri attori, entità, enti pubblici, che possano supportarvi ? Come Stato, siamo sufficientemente preparati e attrezzati per far fronte a una crescita esponenziale di questi fenomeni ?

NUNZIA CIARDI, *direttrice del Servizio di polizia postale e delle comunicazioni del Ministero dell'interno del Ministero dell'interno*. Io ritengo che come Paese abbiamo lavorato per un'architettura in questo campo estremamente utile. La polizia postale è un settore della Polizia di Stato, del *law enforcement*, che ha cominciato a occuparsi di *cybercrime* quando non era un fenomeno così preoccupante, tantissimi anni fa, quindi ha avuto modo di sviluppare una competenza e un *know-how* attualmente estremamente utile.

Non in tutti i Paesi del mondo c'è una polizia specializzata nel *cybercrime*. Noi abbiamo avuto quest'opportunità grazie a una serie di intuizioni che nel tempo ci hanno portato ad avere una Forza di polizia con questa competenza specifica.

Siamo pochi ? Sì, siamo pochi. Abbiamo una necessità di aggiornamento continua, di formazione continua, perché l'evoluzione di questo tipo di crimine è estremamente veloce, estremamente complessa, come lo è tutta la tecnologia.

Ci sono anche dei progetti che vanno proprio nel senso di rafforzare le nostre strutture, di darci più uomini. Abbiamo in programma di aprire a breve, per esempio, un centro dedicato a tutte le aggressioni ai minori *on line*, non soltanto alla pedopornografia. Stiamo lavorando per rendere sempre più incisiva la nostra azione. Questa, secondo me – lo dico *pro domo mea* – è un'azione estremamente utile, perché è un fronte che va assolutamente rafforzato.

PRESIDENTE. Ringrazio gli auditi per il loro contributo.

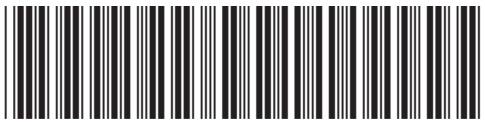
Dichiaro conclusa l'audizione.

La seduta termina alle 13.50.

Licenziato per la stampa
il 13 novembre 2019

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

PAGINA BIANCA



18STC0066290