# COMMISSIONE PARLAMENTARE DI INCHIESTA SULLA TUTELA DEI CONSUMATORI E DEGLI UTENTI

# RESOCONTO STENOGRAFICO

## AUDIZIONE

## 23.

# SEDUTA DI MARTEDÌ 31 MAGGIO 2022

PRESIDENZA DEL PRESIDENTE **SIMONE BALDELLI**

## INDICE

PAGINA BIANCA

PRESIDENZA DEL PRESIDENTE SIMONE BALDELLI

**La seduta comincia alle 11.10.**

**Sulla pubblicità dei lavori.**

PRESIDENTE. Avverto che, se non vi sono obiezioni, la pubblicità dei lavori della seduta odierna è assicurata attraverso impianti audiovisivi a circuito chiuso, nonché via *streaming* sulla web tv della Camera dei deputati.

*(Così rimane stabilito).*

**Audizione del direttore del Servizio di Polizia postale e delle comunicazioni, dottor Ivano Gabrielli.**

PRESIDENTE. L'ordine del giorno reca l'audizione del direttore del Servizio di Polizia postale e delle comunicazioni, dottor Ivano Gabrielli.

Ricordo che la seduta odierna si svolge nella forma della libera audizione ed è aperta alla partecipazione da remoto dei componenti della Commissione, che saluto insieme ai componenti che sono in presenza.

Saluto e ringrazio, oltre al Capo della polizia, il direttore Gabrielli, che ha accettato il nostro invito a svolgere un'audizione sui temi di interesse e di competenza della nostra Commissione e lo ringrazio anticipatamente anche per il lavoro che quotidianamente la Polizia postale svolge al servizio dei cittadini. Le modalità dei nostri lavori saranno quelle consuete. Daremo la parola al dottor Gabrielli, il quale svolgerà la sua relazione, anche aiutato da un supporto informatico, e al termine vedremo se alle domande da parte dei commissari si potrà dare risposta immediata o proseguire l'audizione in una successiva seduta.

Do la parola al dottor Gabrielli.

IVANO GABRIELLI, *direttore del Servizio di Polizia postale e delle comunicazioni*. Grazie a lei presidente. Ripropongo i saluti del Capo della polizia che è particolarmente sensibile ai temi della Commissione e ha ritenuto di darmi mandato per poter approfondire il fenomeno delle frodi, con particolare riferimento alle frodi online che sono un settore strategico e impegnativo anche a livello di risorse, per i numeri che produce dal punto di vista delle attività criminali che vengono rilevate da questo specifico comparto della Polizia di Stato, ovvero la Polizia postale e delle comunicazioni. Avvierò il mio discorso con una digressione organizzativa relativa alla nostra attività, funzionale a meglio comprendere il fenomeno e capire quale sia l'attività di prevenzione e contrasto che viene posta in essere con sistemi e organizzazioni con particolare riferimento alla struttura dei nostri uffici, chiamata ogni volta ad adeguarsi alle situazioni. In breve, la Polizia postale e delle comunicazioni ha una struttura in controtendenza rispetto alle moderne organizzazioni di branche specialistiche del *law enforcement* a livello internazionale. È in controtendenza nel senso che si è ereditato un modello di distribuzione territoriale capillare rispetto ad altre soluzioni scelte da Paesi *like-minded* o comunque strutturati come il nostro. Alcuni Paesi hanno visto il sorgere di centri dedicati al contrasto al cybercrime – pochi centri per la verità – diversamente noi ereditiamo una struttura molto capillare che prevede al vertice un servizio centrale a forte vocazione operativa, sia per la tradizione dei servizi centrali di polizia che

abbiamo sia soprattutto per la necessaria componente di coordinamento che si ha quando si contrastano e si prevengono forme di criminalità che vivono nel loro momento più importante in via territoriale cioè si estrinsecano nella rete, facendo emergere poi epifenomeni singoli, soprattutto quando si tratta di reati che aggrediscono il patrimonio, come nei casi che andremo a sviluppare in questa seduta e che prevedono momenti di analisi importanti, soprattutto in virtù di un'attività di ottimizzazione delle risorse e di miglior coordinamento, essendo poi interessate diverse Procure sul territorio.

Abbiamo una struttura che prevede un Servizio centrale molto importante, 20 compartimenti regionali e 80 sezioni provinciali e stiamo vivendo un momento di profonda trasformazione, dettata soprattutto dai numeri incredibili che con la pandemia hanno avuto un incremento notevole. I Compartimenti vedranno una trasformazione peculiare venendo ridenominati Centri operativi per la sicurezza cibernetica (COSC), le Sezioni diventeranno Sezioni operative dedicate alla sicurezza cibernetica. La novità è che avremo l'emersione di alcune Sezioni più importanti, che insistono presso i capoluoghi che hanno una Procura sede di distretto di Corte d'appello. I reati informatici in larghissima parte prevedono infatti la competenza delle procure distrettuali. I 20 compartimenti hanno il coordinamento delle 80 sezioni provinciali, quindi abbiamo una struttura molto diffusa e presente sul territorio. In passato si era dibattuto sul fatto di tornare indietro e di concentrare le risorse presso le sedi compartimentali. In realtà, la prossimità verso i cittadini e il numero altissimo di reati che siamo chiamati a contrastare depone invece per una presenza più importante e più vicina ai cittadini, in modo che essi possano avere da subito un punto di riferimento, soprattutto per quel che riguarda i reati contro il patrimonio e i reati contro la persona, che vengono ormai commessi in via prevalente attraverso la rete.

Il Servizio centrale è strutturato su quattro divisioni. La prima e la quarta divisione sono le strutture organizzative che supportano l'attività operativa della seconda e della terza divisione. La prima divisione è competente in materia di risorse umane – reclutamento del personale che viene individuato all'interno del corpus della Polizia di Stato e soprattutto attività di formazione. Gli operatori delle specialità vivono continui momenti di formazione più o meno verticali in modo da approfondire le attività operative che poi vengono svolte nelle diverse materie di competenza.

La quarta divisione è la struttura di carattere tecnologico, dove risiede la conduzione del complesso sistema informatico che supporta le attività del centro e del territorio. Nella quarta divisione vi è inoltre la struttura di ricerca, che segue l'evoluzione industriale, per quel che riguarda gli strumenti e i software che debbono essere impiegati per contrastare forme di criminalità che si evolvono continuamente. Essa ha soprattutto un rapporto diretto con l'Accademia, laddove si incontra l'*expertise* migliore e dai fabbisogni operativi sorgono esperienze di sviluppo che portano a successi anche dal punto di vista delle operazioni.

La seconda e la terza divisione sono le strutture che operano nell'attività di prevenzione e di contrasto. La seconda divisione è dedicata soprattutto ai reati contro la persona, a partire dalla prevenzione e dal contrasto alla pedopornografia, che viene svolta dal CNCPO, Centro nazionale per il contrasto della pedopornografia online, istituito per legge, che coordina l'attività investigativa, con particolare riferimento – come ho già detto – ai fenomeni di *overlapping*, in modo da evitare che vi siano sovrapposizioni soprattutto nelle attività più importanti e impegnative, ovvero quelle *undercover*, sotto copertura, svolte in rete dai nostri operatori. Una piccola ma particolarissima menzione va fatta per l'UACI, Unità analisi del crimine informatico, un'équipe di psicologi che svolge attività di *profiling* di vittime e autori dei delitti per cercare di comprendere i fenomeni, anticiparli e rendere poi edotta l'intera struttura a livello nazionale sulle nuove forme di aggressione, soprattutto verso le fasce deboli. L'Unità supporta l'intera attività,

che è particolarmente onerosa dal punto di vista psicologico per chi compie attività investigative in determinati contesti.

La terza divisione si occupa di prevenire e contrastare i reati informatici che aggrediscono il patrimonio, a partire dalle infrastrutture critiche. Anche qui al vertice troviamo il CNAIPIC (Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche) che è un'assoluta esperienza di *best practice* nazionale, vista con interesse anche a livello internazionale, una struttura di *law enforcement* – la prima che abbiamo avuto in Italia – che si occupa di tutelare le infrastrutture critiche informatizzate. C'è poi una Sezione che si occupa di cyberterrorismo, che fa soprattutto raccolta informativa e svolge indagini sulle manifestazioni in rete dell'estremismo religioso o politico e che quindi supporta o svolge attività in proprio rispetto all'attività delle DIGOS, della polizia di prevenzione. Anche qui un'attività molto impegnativa che deriva da una legge specifica che demanda alla Polizia postale l'attività di monitoraggio della rete su questa materia.

Quando invece parliamo di frodi dobbiamo collocarci all'interno della seconda sezione, la cosiddetta sezione *Financial cybercrime*, dedicata esclusivamente ai reati contro il patrimonio. Da qui l'attività di prevenzione e contrasto alle frodi che aggrediscono i sistemi di *home banking* e le attività commerciali. Come sapete, una considerevole parte delle attività finanziarie e degli scambi di beni e servizi avvengono sulla rete.

Da un lato della slide, noterete il CERT del Ministero dell'interno. Ho ritenuto di proporvelo perché su questa struttura è in corso un lavoro di riorganizzazione che farà sì che la Polizia postale e delle comunicazioni veda il proprio vertice salire di livello, quindi non sarà più un Servizio ma una Direzione centrale. La Direzione centrale è già stata prevista da una norma di legge e da un regolamento. Stiamo lavorando ai decreti attuativi del Ministero dell'interno che vedranno la creazione di una nuova Direzione centrale dedicata alla tecnologia. La Cyber e la Polizia scientifica verranno dunque accorpate nell'ambito di questo nuovo assetto. Per chi non conosce bene l'organizzazione del Dipartimento, stiamo parlando di un *upgrade* molto importante. La Direzione centrale è il diretto riporto del Capo della polizia e quindi viene data dignità di esclusività rispetto alla materia, vista la crescita nel tempo del numero dei reati e conseguentemente del lavoro di questa struttura. A margine di ciò, verrà svolta anche una profonda riorganizzazione della struttura territoriale che a specchio ricalcherà l'attuale struttura del Servizio centrale. In termini numerici, i COSC – centri operativi sicurezza cibernetica – da poco previsti da un decreto del Capo della polizia, passeranno da 20 a 18, verranno ottimizzate le risorse presenti sul territorio e, come ho già detto, verrà data importanza alle Sezioni operative sicurezza cibernetica che insistono presso le procure sede di distretto di Corte d'appello. Rimangono quindi invariati i numeri, ma vi è un importante *empowerment* che viene dato sia a livello di centri operativi sia a livello di Sezione.

Se vediamo la slide successiva, ci rendiamo conto di come l'organizzazione territoriale rifletta quella dell'attuale Servizio centrale. Essa prevede un primo settore dedicato al contrasto dei reati che aggrediscono la persona, a partire dalla pedopornografia, e un secondo settore che invece si occupa di tutelare gli *asset* economici strategici del Paese. È importante l'introduzione di un nuovo ufficio, il NOSC, Nucleo operativo sicurezza cibernetica, che riflette le competenze del CNAIPIC. A livello regionale viene ricalcata la dimensione dei nostri Compartimenti. In particolare, ce ne sarà uno, quello napoletano, con una dimensione che andrà oltre i confini della Campania, assorbendo il coordinamento delle sezioni che diventeranno Sezioni operative di Campobasso e Potenza. I NOSC avranno la struttura e le capacità di poter operare h24, contro fenomeni di attacchi informatici. Sono messi in rete con il nostro Centro e, attraverso una piattaforma finanziata con fondi europei, che stiamo ingegnerizzando – ormai è stata ultimata – potranno in tempo reale diramare *alert* di sicurezza alle infrastrut-

ture regionali. Nel secondo settore notiamo la presenza della seconda Sezione che si occupa del contrasto al cybercrime e in generale delle frodi online.

Circa le competenze, la Polizia postale è una branca specialistica della Polizia di Stato e, come tutti i comparti di specialità, vede l'assegnazione delle proprie competenze in virtù di un atto del ministro. Il ministro, con un decreto sui comparti di specialità – l'ultimo è del 2017 – assegna a ciascuna forza di polizia competenze specialistiche, ulteriori rispetto a quelle generali che sono date, da un lato alla Polizia di Stato, dall'altro all'Arma dei Carabinieri. In materia di cybercrime, la Polizia postale è la forza di polizia che interpreta la competenza generale sulla materia che, per dottrina universalmente riconosciuta, include alcuni fenomeni di reato tra i cosiddetti reati informatici. In particolare, per norma di legge, essa è competente in materia di prevenzione di attacchi diretti verso le nostre infrastrutture critiche, attraverso il CNAIPIC e i nuclei operativi sicurezza cibernetica (NOSC). È competente in materia di prevenzione e contrasto alla pedopornografia on line. Stiamo parlando di due competenze esclusive, esclusività dettata dal fatto che lo strumento principale di indagine, come ho già detto, in questi due settori è l'attività sotto copertura e pertanto avere una competenza esclusiva significa evitare possibili diseconomiche sovrapposizioni tra forze di polizia che sotto il segreto istruttorio agiscono *undercover* in rete. Si occupa di cyberterrorismo con un'attività di monitoraggio e di indagine propria che mirano soprattutto a prevenire e contrastare fenomeni di reclutamento, di indottrinamento, di propaganda terroristica in rete – sapete che la rete è ormai lo strumento principale attraverso il quale si compiono attività di questo tipo. Si occupa di *hacking e financial cyber crime* e quindi di contrastare le frodi e i veri e propri attacchi informatici ai sistemi economici del nostro Paese. Infine, si occupa di *social network* e reati postali. Quando parliamo di *social network* ci riferiamo a quella tipologia di reati contro la persona che ormai vengono commessi in maniera preponderante, se non esclusiva, in rete. Parliamo di diffamazione, minacce, *stalking*, *revenge porn*.

PRESIDENTE. Le chiedo una delucidazione sul primo punto. Che cosa intendiamo per infrastrutture critiche ?

IVANO GABRIELLI, *direttore del Servizio di Polizia postale e delle comunicazioni*. Il nostro ordinamento ha previsto l'istituzione del CNAIPIC demandando a esso la missione di tutelare le infrastrutture critiche. Per quanto riguarda la definizione di infrastrutture critiche, queste sono riscontrabili nel primo decreto attuativo della legge n. 144 del 2005, che istituisce il Centro. Stiamo parlando dell'importante decreto-legge Pisanu sull'antiterrorismo che, vi ricorderete, aveva in sé alcuni aspetti cibernetici. Viene considerata a livello internazionale una delle prime leggi cyber. È il decreto che introdusse l'obbligo di identificazione dei fruitori degli *internet point* nonché la necessaria concessione della licenza da parte del questore per la loro apertura. L'introduzione di tale normativa avvenne a seguito degli attacchi terroristici alla stazione di Atosha e alla metropolitana di Londra. Gli ordigni vennero attivati con mezzi tecnologici. Da qui emerse anche tutta una particolare sensibilità verso la *data retention*, ovvero la conservazione dei dati. In sede di conversione, venne poi istituito questo Centro. Nel mondo si stava teorizzando la possibilità di tutelare le infrastrutture critiche dal punto di vista della dimensione cibernetica, nel senso che fino a quel momento non veniva scissa l'infrastruttura informatica rispetto a quella fisica, che ovviamente da sempre è stata oggetto di tutela. Quando parliamo di infrastrutture critiche, parliamo del sistema dei trasporti, del sistema dell'energia elettrica, del sistema sanitario, del sistema delle comunicazioni e del sistema finanziario. Il decreto del Ministro dell'interno del febbraio 2008, che seguì l'istituzione del Centro, diede una definizione amplissima di infrastrutture critiche. All'epoca non si parlò di settori ben definiti, cosa che è stata introdotta successivamente dalla direttiva

NIS o come di seguito avemmo a livello interno con la normativa sul Perimetro nazionale di sicurezza cibernetica. Le infrastrutture critiche vennero individuate come quelle che servono i servizi essenziali del Paese nell'ambito del settore energetico, dei trasporti, delle telecomunicazioni e del settore finanziario, dando un ampio spazio di manovra a chi avrebbe dovuto porre in essere piani di tutela e quindi al CNAIPIC che veniva istituito. Ampio spazio di manovra che tra l'altro vede la realizzazione attraverso un sistema di convenzioni. La norma istitutiva prevede che le infrastrutture critiche possano essere individuate dal Ministro dell'interno. Il Ministro dell'interno nel nostro ordinamento è l'Autorità nazionale di pubblica sicurezza. Il Servizio Polizia postale e delle comunicazioni, oltre a essere il vertice amministrativo della Polizia postale che ne gestisce la struttura, è anche l'organo centrale del Ministero dell'interno per la sicurezza delle telecomunicazioni. Lo è in virtù di una legge del 1998. Questa sua prerogativa fa sì che il Servizio sia anche la proiezione dell'Autorità nazionale di pubblica sicurezza all'interno del mondo virtuale. È in virtù di questa qualifica che il Servizio e la specialità partecipano ai tavoli interistituzionali, come il Nucleo per la cyber sicurezza, che di seguito sono arrivati con le normative Monti, con la normativa Gentiloni e da ultimo con la legge che istituisce l'Agenzia. Per tornare alla risposta, le infrastrutture critiche, per quel che riguarda la nostra missione istituzionale, non vengono predefinite, ma vengono individuate all'interno di diverse categorie. In quelle categorie sono state individuate all'incirca una sessantina di infrastrutture critiche che in questo momento sono convenzionate con il Centro e in virtù di questa convenzione hanno un rapporto diretto di scambio di dati. Noi forniamo loro dati di sicurezza che ricaviamo dall'attività di monitoraggio, ma anche dall'attività di polizia giudiziaria. Le infrastrutture critiche hanno in noi un *hub* privilegiato per avere un confronto sui temi della sicurezza e anche nel momento in cui debbono rappresentare notizie che possono diventare notizie di reato. Questo modello, come ho già detto, verrà calato sul territorio con l'istituzione dei Nuclei operativi sicurezza cibernetica, che a loro volta individueranno a livello regionale le infrastrutture sensibili che però hanno una portata nazionale.

A proposito di cybercrime, si sente parlare spessissimo di attacchi informatici. Il problema è che moltissimi attacchi informatici debbono essere calati in una prequalificazione, nel senso che in costanza di un attacco informatico cioè di un attacco portato verso un'infrastruttura informatizzata ci si chiede se la matrice sia ascrivibile ad atti di altro tipo ovvero sia una matrice criminale. All'esito di percorsi investigativi o di approfondimento, la matrice criminale è assolutamente prevalente nell'ambito dei fenomeni di aggressione alle infrastrutture informatiche. L'ultimo report globale parlava del 76 per cento, nel 2020 addirittura ci si spinge verso l'81 per cento. In questo caso la fonte è il rapporto CLUSIT che ogni anno in Italia fotografa lo scenario generale. Perché è importante comprendere e comunque attribuire anche in sede di analisi una matrice rispetto ad un'altra ? Perché chi deve fare politica criminale si rende conto di quali siano le risorse da destinare al settore del *law enforcement*, quindi alle strutture delle forze di polizia che debbono contrastare questa tipologia di aggressione. Come vedete nell'81 per cento dei casi parliamo di matrice criminale. È pur vero che qualsiasi tipo di attacco informatico, anche qualora possa essere in via di analisi, ma analisi che prevedono tempi importanti e anche momenti di riflessione significativi, qualsiasi tipo di attacco informatico, dicevo, nel nostro ordinamento integra una fattispecie di reato e, nella stragrande maggioranza dei casi, fattispecie di reato procedibili d'ufficio. Da qui questa importante percentuale che conferma anche la dottrina internazionale che vede le strutture di *law enforcement* molto impegnate in questo settore e collaborare con le altre strutture che debbono occuparsi di sicurezza nazionale a partire dalle strutture di *homeland security* fino ad arrivare alle strutture dell'*intelligence* e della Difesa. Come vi ho già detto, come succede per la dinamica cri-

minale, il settore finanziario, e quindi i reati contro il patrimonio sono di gran lunga quelli più importanti in termini numerici. L'anno scorso si è segnato l'importantissimo sorpasso da parte dei reati contro il patrimonio commessi attraverso la rete rispetto ai reati commessi nel mondo reale. Il *financial cyber crime* si trova al vertice per quel che riguarda le forme di aggressività, con momenti anche di interessamento di criminalità organizzata che vengono attratti dagli ampi profitti – poi vedremo di che profitti parliamo – che possono essere acquisiti mediante attacchi informatici, frodi online, *ramsomware*, eccetera. Si parla di *financial cyber crime* quando la componente tecnologica di attacco è, se non esclusiva, preponderante, rispetto a una dinamica, che, come vedremo, coinvolge spesso il fattore umano. Quindi abbiamo tecniche di attacco e di distribuzione di virus informatici sempre più sofisticate. Quello che un tempo era appannaggio di una élite criminale che utilizzava competenze informatiche di assoluto livello all'interno di fenomeni come l'attivismo o all'interno di attacchi che potevano essere *State sponsored*, adesso la criminalità organizzata e la criminalità comune hanno la possibilità di attingere a servizi e a strutture criminali che già predispongono pacchetti di attacco che possono essere acquistati e sfruttati da chi riesce a mettere in piedi organizzazioni che debbono muovere risorse umane e procedere con attività di riciclaggio di altissimo livello.

Seguono le strategie di *social engineering*. Come ho già detto, il fattore umano è molto importante. Ovviamente la frode di per sé prevede una sorta di cooperazione involontaria della vittima, ma pensiamo agli attacchi informatici prodromici agli attacchi di tipo finanziario, poi vedremo in che modo. Stiamo parlando di veri e propri attacchi informatici che penetrano in sistemi che permettono la gestione economica delle imprese, sistemi di home-banking, sistemi bancari e che sfruttano tecnologia o fattore umano per portarsi all'interno di quelle strutture, studiarne le dinamiche, non soltanto tecnologiche, ma anche relazionali ed economiche, per poter poi sferrare gli attacchi – poi vedremo in quali fenomeni si concretizzano. Il *cyber-profiling* e spionaggio riguardano lo studio che è a monte delle strategie di *social engineering*. Profilazione di amministratori delegati o di plessi organizzativi permettono di addivenire a frodi informatiche complesse come i BEC (*business e-mail compromise*) o le CEO *fraud*, frodi che sfruttano l'organizzazione societaria per poter poi colpire stornando cifre importanti dal budget operativo che è a disposizione delle stesse aziende. Quali sono i reati che vengono intercettati in questo specifico panorama ? Ci stiamo calando all'interno del mondo del *financial cyber crime*, frodi informatiche dirette verso le strutture economiche e finanziarie dei singoli e delle imprese medie, piccole e grandi. Parliamo di reati che vengono di solito contestati dal punto di vista dell'attacco informatico: quelli previsti dall'articolo 615-*ter* del codice penale, accesso abusivo a sistema informatico, cioè il comportamento di chi « buca » i sistemi informatici, violandone il perimetro più o meno protetto; dall'articolo 635-*bis*, danneggiamento del sistema informatico e telematico, cioè la fattispecie che viene integrata qualora un soggetto si porti all'interno di un sistema informatico e, per svolgere le proprie attività criminali, ne comincia ad alterare la struttura, andandone a danneggiare l'infrastruttura logica e fisica sottesa all'interno di un sistema informatico; dall'articolo 635-*ter* e *quater*, danneggiamento di informazioni, dati e programmi utilizzati dallo Stato o da altro ente pubblico, comportamenti che impattano non più soltanto su realtà aziendali e quindi di privati, ma anche a livello pubblico. Seguono i reati che vengono contestati nel momento in cui si concretizza un'attività criminale diretta verso un assetto economico-finanziario, quindi la frode informatica.

Nell'ambito dell'*e-commerce*, non parliamo più di frode informatica ma di un raggiro, di una semplice truffa, che può avvenire ad esempio su una piattaforma in cui un soggetto promette un bene e poi in realtà ne carpisce il corrispettivo senza

corrisponderlo. Sono frodi che non sfruttano quindi l'elemento informatico di per sé, non c'è una strategia informatica, non c'è un artificio o raggiro informatico che permetta il concretizzarsi della frode, bensì un raggiro che a livello di *social engineering* costruisce un *environment* all'interno del quale il soggetto frodato purtroppo cade vittima di un reato di questo tipo. Inoltre, abbiamo l'invio, l'utilizzo e la falsificazione di strumenti di pagamento. In questo momento, il fenomeno non assurge all'importanza criminale che si è avuta in passato, quando avevamo fenomeni di alterazione dei bancomat, della clonazione di carte di credito e di strumenti di pagamento in genere. Ormai le contromisure tecniche hanno molto arginato, anche se residuano fenomeni di questo tipo.

Quando parliamo di attacchi ai sistemi informatici, quindi attacchi finanziari e frodi informatiche ad alta complessità, pensiamo soprattutto a quello che viene considerato ormai in letteratura come il fenomeno più importante e che poi vedremo declinarsi in tante piccole e diverse attività criminali, secondo la tecnica che viene utilizzata per raggirare la vittima. Ci riferiamo soprattutto al fenomeno del *phishing* che non è più come l'abbiamo conosciuto qualche anno fa, cioè esercitato attraverso una sistematica attività di spamming, o, meglio, residua un'attività di questo tipo ma è assolutamente minoritaria. L'attuale attività di *phishing* prevede invece l'ingresso di tecniche di *hacking* evolute che mirano o a distribuire *malware* o a ingegnerizzare sistemi clone che traggono in inganno l'utente che partecipa più o meno volontariamente alla dazione delle proprie chiavi di accesso ai propri conti bancari e alle proprie strutture finanziarie, cioè le USER-ID, le password e gli account con cui si ha accesso al sistema informatico gestionale. Quella che vedete rappresentata è la moderna struttura organizzativa – che tra l'altro abbiamo toccato con mano di recente in un'operazione molto complessa che abbiamo svolto con i colleghi spagnoli – che vedeva una organizzazione criminale italiana insistere presso le Canarie e che ogni anno riusciva a drenare all'incirca 20-30 milioni di euro per poter poi reimpiegarli nelle classiche attività di criminalità organizzata, traffico di droga, traffico d'armi e prostituzione. Questo gruppo è strutturato in un'organizzazione tipica di coloro che hanno compreso il vantaggio economico di poter compiere un'attività che non prevede un rischio diretto a livello personale – così come avviene ad esempio con una rapina – ma contempla la possibilità di operare da remoto e lunghi tempi di indagine per la ricostruzione del fenomeno, tempi di indagine che vengono ulteriormente dilatati dal fatto che spesso tutta l'infrastruttura criminale che serve per poter drenare questi capitali viene collegata strategicamente a Paesi esteri che presentano maggiori difficoltà di cooperazione. Le indagini proseguono nel tempo e sono effettivamente molto importanti dal punto di vista della gestione dell'attività investigativa nella ricostruzione del percorso tecnico e finanziario. La struttura vede un capo, un'organizzazione che sta al vertice, fatta di più soggetti, che si procura il *know-how* tecnologico, ingaggiando spesso delle *crew* di sviluppatori di *malware*. Queste *crew* non è detto siano effettivamente inserite all'interno dell'organizzazione. Come ho già accennato, soprattutto nel *dark-web* vi sono dei portali che forniscono pacchetti tecnologici che vengono acquisiti da soggetti che sono anche in grado di poterli gestire e manovrare. È una struttura composita e non è detto che vi sia un contatto fisico tra la struttura IT e quella al vertice. Molto probabilmente vengono attivate *crew* che da remoto gestiscono e ingegnerizzano la macchina infotelematica sia nel momento in cui va sferrato l'attacco sia nel momento in cui poi va gestito il riciclaggio dei proventi e che poi ricevono parte dei profitti. Proventi che vedono nell'utilizzo di moneta virtuale, quindi di cripto-valute, uno degli aspetti più importanti in questo momento. Sotto, come vedete, c'è una ampia sfera di reclutatori. Questo ha determinato le capacità delinquenziali di articolazioni che hanno strutture organizzative già ben consolidate. Di chi parliamo ? Di soggetti che hanno una presenza importante sul territorio e che riescono a reclutare i *money mules* o rici-

clatori – *money mules* è ormai divenuto un termine internazionale. Parliamo di una amplissima parte della struttura organizzativa che fa da prestanome e agisce nel momento in cui va ingegnerizzata la prima attività di riciclaggio. Un attacco informatico, una frode informatica ad alta complessità come il *phishing*, che, ripeto, fa migliaia e migliaia di vittime, prevede l'ingaggio di una struttura tecnologica che distribuisce ad esempio dei *malware* e lo fa nei confronti di soggetti di cui possiede già informazioni che vengono reperite spesso nel *dark web*. Stiamo parlando del frutto di *leak* di dati che ogni volta sono il prodotto di attacchi informatici. Si attacca un portale, si prendono i dati dei clienti, ovvero le mail, i numeri di telefono, le password che vengono utilizzate per loggarsi a quel portale e che spesso sono simili se non del tutto uguali alle password che poi vengono utilizzate ad esempio per muovere i propri conti bancari. Acquisito questo tipo di *know-how* informativo, si predispone un'attività di attacco che vedrà tecniche diverse. Arrivano i dati delle vittime e i proventi debbono essere monetizzati in maniera rapida con movimenti bancari verso i punti aperti dai *money mules*. I *money mules* incassano quel denaro e poi hanno indicazioni sul ristorno e trattengono una percentuale del denaro, che è il primo profitto illecito. Quelle enormi fonti di danaro poi confluiscono verso i vertici dell'organizzazione, attraverso attività di riciclaggio che coinvolgono spesso o istituti all'estero oppure, come ho già detto, asset di criptovalute.

Si parte da un furto di dati personali che di solito avviene attraverso tecniche di *phishing*, *vishing*, siti clone di altre strutture finanziarie, verso i quali i soggetti vengono indotti a inserire le proprie credenziali, fino alla diffusione di *malware* bancari cioè *malware* che sono strutturati e ingegnerizzati per carpire le credenziali di accesso al conto di *home banking* e quant'altro. Ultimamente, c'è un fenomeno molto importante che è lo *smishing*. Con l'utilizzo del secondo fattore di autenticazione che vede come protagonista lo smartphone, lo *smishing* è diventato uno dei sistemi più importanti con cui reperire informazioni. Viene di solito clonato – *spooffato* in gergo – il numero dell'istituto bancario. Il soggetto riceve un messaggio e il telefono automaticamente lo mette in coda rispetto ai messaggi che riceve dal proprio istituto bancario. Questo lo rende assolutamente credibile e quindi il cliente è indotto a portare all'interno del sistema criminale le chiavi di accesso e le proprie credenziali.

A destra della slide, vedete lo sviluppo di un secondo stage di attività criminali, quindi se a sinistra vi sono le frodi informatiche su larghissima scala, a destra vediamo le frodi molto profittevoli dal punto di vista criminale e che sfruttano invece le risorse economiche e tecnologiche delle piccole, medie e grandi imprese. Sostanzialmente tali frodi vengono suddivise in due grandi categorie. BEC e CEO *fraud*. Con il BEC l'attacco informatico viene portato all'interno dei sistemi aziendali, si cerca di « bucare » il sistema di gestione della posta elettronica aziendale. Quando si ha in mano la posta elettronica si ha in mano tutta l'attività economico-finanziaria dell'azienda stessa, in termini di ordini, forniture e corrispettivi che andranno pagati. Ci si intromette all'interno di una transazione, ci si sostituisce o al fornitore o al prestatore e poi si cerca di stornare il corrispettivo di quella transazione. Tutto questo viene fatto in maniera silente, con un'accurata pulizia del sistema di posta elettronica per non lasciare tracce. Una volta sferrato l'attacco, spesso passano purtroppo giorni e anche mesi prima che un soggetto si accorga che qualcuno si è intromesso all'interno della transazione economica o finanziaria, con milioni e milioni di euro che vengono portati all'estero e poi spacchettati e riciclati attraverso le complesse attività di riciclaggio di cui parlavamo prima.

L'altra tecnica di attacco è quella del CEO *fraud*, attualmente un po' in calo ma effettivamente molto significativa fino all'anno scorso. Parliamo di una tecnica che prevede lo studio delle dinamiche comportamentali all'interno dell'azienda, cioè si studiano i ruoli nell'ambito della attività finanziaria – quindi il CEO, ovvero l'amministratore delegato, e il dirigente che si

occupa delle transazioni finanziarie, il CFO – si capisce la dinamica, se ne studiano i movimenti e le strategie, e quando è il momento più propizio si sferra un attacco che prevede la sostituzione dell'attaccante in capo al CEO che intrattiene quindi una comunicazione con il proprio CFO, cercando poi di stornare e far bonificare all'estero spesso ingenti somme di denaro.

Residua, ma era secondo me importante parlarne anche in questo contesto, il fenomeno, questo invece crescente, dei *ransomware* o cyber estorsioni. Si tratta di un attacco che ha portata spesso devastante dal punto di vista della paralisi dei sistemi informatici. Anche qui la porta di ingresso è un attacco informatico vero e proprio. Si studia la struttura interna, vi è un'attività di *privilege escalation* fino al livello di amministrazione, dopodiché viene lanciato un *ransomware*, un *malware* che è in grado di criptare e cifrare l'infrastruttura informatica, rendendola inutilizzabile. Ultimamente viene richiesto un contatto nel dark web, nel quale, su portali dedicati, viene instaurata una vera e propria trattativa che prevede la richiesta di un riscatto per la decifratura dell'asset cifrato. Quello che appare sempre più frequente è che l'attività di attacco e di danneggiamento del sistema informatico è accompagnata da un'attività di esfiltrazione di dati sensibili dei quali poi viene minacciata la pubblicazione. Quando parliamo di dati sensibili, parliamo di dati aziendali, di trattative, di contratti che, se resi pubblici, creano un danno, se non il danno più importante alla stessa società. Le ragioni di quest'ultima evoluzione sono anzitutto di avere un secondo strumento di pressione, poi perché quel *know-how* che viene pubblicato può essere estremamente sensibile e infine perché ormai alcune strutture aziendali hanno la capacità di difendersi dall'attacco cifrante, attraverso sistemi di backup o un'ingegnerizzazione corretta dell'infrastruttura di rete e quindi se l'azienda non può più essere colpita dal punto di vista infrastrutturale lo può essere minacciandola di pubblicare dati riservati e sensibili.

Vi fornisco alcuni dati. Il rapporto tra il 2020 e il 2021 vede un leggero incremento. L'incremento più importante che abbiamo riscontrato dal punto di vista delle attività si è avuto forse tra il 2018 e il 2020, molto probabilmente dovuto anche alla pandemia. I numeri sono importanti, sono cresciuti tantissimo nell'ultimo periodo sia come attività di casi trattati sia come persone indagate dal 2020 al 2021. Per quel che riguarda la trattazione di quello che abbiamo detto essere l'ambito del *financial cyber crime*, da un lato il mondo delle truffe, dall'altro il mondo della monetica, con un forte ingresso anche delle forme di frodi che riguardano il trading on line e quindi anche l'utilizzo di moneta virtuale. Il *financial cyber crime* puro, cioè ascrivibile al BEC, al CEO *fraud* fino al *phishing*, rimane comunque la componente più importante di quello che può essere considerato *financial cyber crime* in senso lato. Per quel che riguarda il BEC e il CEO *fraud*, l'aumento è estremamente significativo. Stiamo parlando di attacchi che in termini di numeri non sono elevatissimi ma in termini di profitto sì perché vanno a colpire l'asset economico-finanziario più importante di cui abbiamo disponibilità nella nostra società, quindi stiamo parlando degli asset aziendali delle infrastrutture economiche che vengono colpite da questo tipo di attacco. Dal 2019 vedete che c'è un enorme espansione perché i perimetri aziendali informatici con il sopraggiungere della pandemia si sono enormemente ampliati. Soprattutto il telelavoro ha aperto la porta a possibilità di attacchi informatici portati da fuori in domini che non hanno più avuto una gestione ferrea e stretta all'interno della gestione aziendale. Siamo partiti da postazioni di lavoro che molto probabilmente venivano utilizzate dagli operatori *in situ* e gestite dagli amministratori di rete, a postazioni spesso utilizzate in maniera promiscua quindi sia per attività personale sia per attività aziendale che hanno fornito, anche attraverso sistemi di virtualizzazione delle connessioni, che presentavano e presentano diversi momenti di vulnerabilità, la porta d'ingresso all'attaccante e, come ho già detto, prima l'attacco è di tipo informatico e poi mira a sviluppare l'attacco economico vero e proprio.

PRESIDENTE. Nel grafico precedente ci sono anche delle cifre assolute laddove si parla del *financial cyber crime*. A cosa si riferiscono quei numeri ?

IVANO GABRIELLI, *direttore del Servizio di Polizia postale e delle comunicazioni*. Nell'istogramma vede che sono cifre assolute rispetto ai casi trattati dalla specialità, con riferimento alle singole fenomenologie criminali. In verde abbiamo tutte le frodi che, come vedremo, riguardano soprattutto l'e-commerce, però è significativa l'attività di *phishing*, con 2622 casi.

PRESIDENTE. Allora si tratta del numero dei casi trattati.

IVANO GABRIELLI, *direttore del Servizio di Polizia postale e delle comunicazioni*. Sì.

PRESIDENTE. Questo è il grafico relativo al 2021.

IVANO GABRIELLI, *direttore del Servizio di Polizia postale e delle comunicazioni*. Sì.

Veniamo ora ai fenomeni principali di frodi online, che riguardano più i singoli cittadini. Come ho detto, BEC e CEO *fraud* sono frodi importantissime, ma riguardano i plessi aziendali e sono veri e propri attacchi al sistema economico-finanziario. Essi prevedono pochi numeri ma significativi dal punto di vista della esfiltrazione delle risorse. Qui invece ci portiamo su un altro settore, ovvero a quello dove gli attacchi vengono fatti al singolo. Vengono declinate diverse fenomenologie, perché, come ho già detto, il *phishing* di credenziali (che sta per pesca su larga scala) che un tempo veniva fatta semplicemente con attività di spamming massivo di mail mentre adesso lo spamming massivo viene contrastato grazie a filtri antispam più efficaci mentre una corretta educazione da parte dell'utenza nonché l'introduzione del secondo sistema di autenticazione per il controllo degli accessi ai sistemi bancari hanno arginato il fenomeno. Tuttavia l'attività di *phishing* tramite mail continua a essere rilevante quando è prodromica all'installazione di un *malware* – ci sono campagne enormi di questo tipo, una delle più importanti si chiama Emotet, un'altra Trickbot. Stiamo parlando di *malware* che vengono ingegnerizzati e continuamente aggiornati per sottrarsi ai sistemi antivirus e prevedono importanti e significativi momenti di spamming con l'installazione di *malware* su un computer. Il computer comincia a dialogare con un centro di comando e controllo, quindi viene creata una vera e propria *botnet*, cioè una rete di computer che vengono governati da remoto. Quei *malware* sono fatti apposta per poter sottrarre codici e password e vanno a cercare sia a livello di browser quando navighiamo sia a livello di client di posta elettronica sia a livello di cartella interne USER-ID e password di accesso a qualsiasi servizio on line, e ovviamente vengono privilegiati i servizi di accesso all'home banking. Abbiamo poi l'emergere di una tecnica nuova che viene ormai chiamata *vishing*, in cui addirittura abbiamo un contatto diretto da parte di un soggetto che simula di essere ad esempio un operatore bancario, che contatta spooffando, quindi nascondendo il proprio numero – ed è possibile farlo attraverso servizi internazionali che permettono di impostare delle chiamate e quindi di scegliersi il numero da far comparire sul telefono. Lo si fa perché la telefonata non è una telefonata che ingaggia la nostra rete telefonica, ma è una telefonata che avviene tramite traffico dati, da qui il nome *vishing* (Voice Over IP phishing) quindi stiamo parlando della telefonata che avviene attraverso la piattaforma informatica, un po' quello che ormai facciamo tutti utilizzando telefonate Whatsapp o Signal. La voce quindi non è traffico telefonico ma è traffico dati, viene quindi spooffato il numero di partenza, si usa un numero con il quale alcuni istituti bancari contattano i propri clienti e attraverso un colloquio telefonico vengono carpiti i dati che servono ad accedere ai conti bancari. In alcune operazioni di contrasto ci siamo trovati di fronte a situazioni peculiari in cui c'erano dei veri e propri call center criminali in batteria con tanto di formulari, di questionari o di frasi ricor-

renti da potere o dovere usare per poter poi carpire la fiducia e portare il truffato all'interno di un *loop* che poi è quello che succede quando c'è una frode di questo tipo, cioè il soggetto crede di parlare con un operatore bancario. È un fenomeno che abbiamo contrastato anche a livello internazionale per esempio quando il *vishing* non avveniva attraverso Voice Over IP, ma attraverso *carrier* internazionali, quindi su telefonia. Abbiamo chiesto agli operatori nazionali di bannare l'ingresso di numeri verdi italiani che provenivano dall'estero, quindi telefonia spooffata con numeri verdi italiani che contattavano i nostri. Abbiamo anche avuto fenomeni in cui il *vishing* veniva effettuato attraverso la simulazione di essere appartenenti alle forze dell'ordine, quindi c'era un soggetto che chiamava fingendosi di essere un maresciallo dei Carabinieri o un operatore di polizia che stava lavorando a un'indagine e quindi chiedeva informazioni.

Lo *smishing* è un altro tipo di attacco di *phishing* che avviene attraverso sms che riportano all'interno un *link* sul quale cliccare per poi recarsi all'interno di un ambiente che dissimula in tutto e per tutto il *brand* di istituti bancari o di altri servizi. In quel caso la vittima è indotta a inserire le proprie credenziali.

Ultima tecnica particolarissima, sulla quale siamo in contatto anche con l'AGCOM, è l'attività di SIM-*swap*. Essendo stato introdotto il secondo fattore di autenticazione, l'attaccante cerca di sostituirsi all'attaccato, quindi alla vittima, interloquisce con il provider di comunicazione, si fa abilitare una nuova SIM sulla quale viene poi attivata la portabilità del vecchio numero di telefono, fingendo di avere perso o di essergli stata sottratta la SIM precedente. Quando riesce a compiere questa attività diventa il proprietario di quella SIM telefonica e quindi riesce a ottenere il secondo fattore di autenticazione direttamente sul proprio telefono. La vittima non se ne accorge subito e scambia quel « buco » nelle comunicazioni del proprio telefono come un malfunzionamento o un disservizio e in quel frangente purtroppo rimane vittima di un'attività che poi vede lo svuotamento del proprio conto corrente. Queste attività, come vi ho già detto, conoscono un'attività prodromica che va riportata al furto di identità digitale. Tutte le tecniche di cui abbiamo parlato – *phishing*, *vishing*, *smishing* – servono a carpire le credenziali di accesso o i dati sensibili che permettono l'accesso a un servizio bancario. Come vedete, in questo momento, è enormemente preponderante l'attività di *smishing* rispetto a quella dei siti clone, che rimangono ancora importanti, rispetto al *vishing* e al SIM-*swap*. Quando parliamo di furti di identità digitale parliamo dell'acquisizione di dati della vittima che sono prodromici alla successiva attività criminale.

Un focus particolare l'abbiamo dedicato al *ransomware*, perché, ripeto, costituisce uno dei fenomeni emergenti. Non parliamo di frodi, non parliamo di attività predatoria di tipo ordinario, però è una fattispecie che viene integrata a livello di contestazione del reato di estorsione che, come vedete, è in crescita con casi gravi – sono stati 256 nel 2021. Nel primo trimestre purtroppo abbiamo un ulteriore momento di crescita. Da un lato, abbiamo quindi forme di aggressione di massa per quel che riguarda tutta la famiglia del *phishing* declinato nelle varie sottospecie. Qui abbiamo invece attacchi che, come ho già detto, sono molto settoriali, molto verticali e ad alta complessità tecnologica che colpiscono le nostre aziende in maniera molto significativa.

Dal punto di vista della risposta, come ho già detto, da tempo abbiamo strutturato una sezione a livello centrale e oggi la caleremo anche a livello territoriale – i nostri compartimenti hanno già strutture dedicate esclusivamente all'antifrode. Il modello organizzativo che abbiamo scelto è specializzante e iper-verticale proprio perché finalizzato a intercettare quanto prima fenomeni in crescita, comunque a livello di nuove tecniche di aggressione e nuove tecniche di attacco informatico prodromiche alle tecniche di attacco ai sistemi finanziari. Un'attività dunque svolta dal centro. Si sta pensando anche a un modello organizzativo diverso che ricalchi quella che è stato secondo noi una buona pratica che abbiamo sviluppato sia per il contrasto alla

pedopornografia sia per il contrasto agli attacchi informatici portati verso le infrastrutture critiche. Vorremmo portare anche questa materia a livello di centro nazionale, perché spesso le informazioni, trattandosi di fattispecie su larga scala, conosciute con un fenomeno, possono essere messe a fattor comune di tutto il sistema bancario per innalzare i livelli di sicurezza. In questo settore è importantissima l'attività di cooperazione internazionale. La sezione *financial cyber crime* fa attività di indagine di propria iniziativa su fenomeni che sono più ampi, hanno proprio una caratteristica di extraterritorialità o comunque hanno una proiezione all'estero e deve fare dunque attività di coordinamento nazionale perché, come ho già detto, parliamo di micro-fenomeni che, letti da chi sta al vertice di una struttura, possano essere riportati all'interno di un fenomeno criminale e quindi risparmiare energie e risorse per l'attività di contrasto. Attività importantissima è dunque quella della cooperazione internazionale: non esiste un'indagine di questo tipo che non preveda comunque l'ingaggio delle strutture di cooperazione, a partire da Europol che ha una struttura dedicata al cyber crime (EC3) all'interno della quale c'è una articolazione preposta al *financial cyber crime*, fino ad arrivare a Interpol e all'ingaggio diretto dei nostri ufficiali di collegamento, quindi gli esperti per la sicurezza, soprattutto quando ci muoviamo in velocità per recuperare delle somme, su cui vedremo anche qualche dato. Stiamo parlando di svariati milioni di euro che cerchiamo di rincorrere nel momento in cui c'è un'attività delittuosa in atto per far sì che quelle risorse non vengano disperse e non siano definitivamente riciclate all'interno di circuiti criminali.

Le truffe on line ricorrenti che invece riguardano dinamiche diverse e insistono più sull'attività commerciale svolta attraverso la rete, come vedete, sono importanti come numeri e riguardano soprattutto quattro settori. Abbiamo le truffe immobiliari che sono molto importanti soprattutto quando ci si avvicina ai periodi di vacanza e rimangono una costante significativa per quel che riguarda anche il prodotto criminale che sviluppano. Abbiamo poi le truffe su piattaforme di e-commerce che continuano a essere significative e importanti. Come vi ho già detto, in questi casi non abbiamo una struttura in cui sia preponderante la parte tecnico-informatica, ma mi riferisco all'ingegnerizzazione di portali e siti che riescono a inserirsi all'interno della corretta gestione dell'e-commerce. Vi è poi il falso trading on line che in quest'ultimo periodo sta diventando un'importante modalità di aggressione ai patrimoni – stiamo parlando di quelle offerte di trading on line, di finanziamenti, di investimenti addirittura attraverso sistemi di multilevel marketing che vengono ingegnerizzati in rete. Parliamo di interi patrimoni consegnati a soggetti che all'inizio corrispondono un guadagno, secondo il classico schema, tipico della cosiddetta truffa Ponzi, per cui un soggetto viene agganciato promettendo ricavi e tassi di interesse rilevantissimi, riceve le prime tranche di pagamento, dopodiché la struttura viene chiusa e sparisce, portandosi con sé svariati milioni di euro. Anche qui abbiamo svolto indagini molto interessanti soprattutto con il compartimento di Cagliari che recentemente hanno portato a diverse misure cautelari nei confronti di appartenenti a una struttura che operava non soltanto in Italia, ma in Spagna e in Ungheria, costruendo delle vere e proprie cellule di proposte finanziarie – le persone sono molto allettate dalle voci che circolano intorno alle cripto valute per cui si propongono guadagni da capogiro, dopodiché si scompare con il maltolto.

Importante è anche il fenomeno delle truffe romantiche (*romance scam*). Se ne è parlato moltissimo. Sono truffe che riguardano la sfera sentimentale, hanno una dimensione particolare in cui viene sfruttata la debolezza psicologica di un soggetto che soltanto alla fine di un percorso, spesso perché aiutato dai propri familiari e dai propri conoscenti, riesce a tirarsene fuori. Anche qui parliamo di ingenti patrimoni che vengono corrisposti a persone con cui non si ha nessun tipo di contatto fisico o visivo ma con le quali vengono intrattenute

relazioni costruite ad hoc. Una delle più importanti operazioni, iniziata l'anno scorso e tuttora in corso, riguarda una batteria di soggetti stranieri. Senza entrare troppo nei particolari perché ancora ci stiamo lavorando, è stato curioso vedere come vi fosse una batteria di ragazze e ragazzi che gestivano contatti tramite piattaforme di messaggistica Whatsapp e altre, con una specie di prontuario o manuale dedicati alla impersonificazione del soggetto adescante. Quindi avevamo prontuari dedicati alla impersonificazione di ufficiali dell'esercito e della marina, di professionisti, con risposte e anche con tratti di vita privata che debbono essere calate all'interno di quel percorso di costruzione di una falsa identità che poi adesca la vittima portandola all'interno di una relazione, che si rivela ovviamente come una relazione immaginaria. Ne stiamo studiando alcuni aspetti con l'UACI, l'Unità analisi del crimine informatico, i nostri psicologi, perché si vede quanto siano ricorrenti alcune forme di adescamento, alcune tecniche che vanno dal rappresentare tragedie familiari a difficoltà economiche. Il percorso più o meno è sempre lo stesso, ma non è lasciato alla fantasia dei soggetti, viene costruito addirittura attraverso tecniche di ingegneria sociale e quindi codificate.

La slide vi dà il senso del prodotto di questa attività delittuosa, sia in termini di casi trattati, divisi per macro-categorie, tra trading on line, e-commerce, *romance scam*, truffe immobiliari per centinaia di migliaia o milioni di euro che risultano dalle denunce sporte. Crediamo che ci sia una cifra oscura molto più elevata. In particolare crediamo che soprattutto nel caso del trading on line e delle *romance scam* ci sia una scarsissima propensione a denunciare i fenomeni. Ciò vale per il trading on line perché ne sono vittime anche imprenditori e professionisti che cadono in un sistema che evidentemente porta con sé anche un discredito sociale e familiare in relazione alla cooperazione involontaria con il soggetto che svolge l'attività fraudolenta. Lo stesso dicasi per le *romance scam* che attengono alla sfera più intima.

Un breve focus riguarda la pandemia del COVID-19. L'ampliamento del perimetro dell'utilizzo delle piattaforme di comunicazione più evoluta, della messaggistica e soprattutto l'attività di *smart working* ha enormemente fatto lievitare i casi di campagne di *phishing* e *vishing* così come delle frodi BEC e delle CEO *fraud*. Maggiormente significativa durante la pandemia del COVID-19 è stata l'incidenza di casi di *financial cyber crime* nel loro complesso. Ciò è dovuto all'utilizzo dello strumento dell'home banking e delle tecniche di transazione finanziaria per le attività commerciali, che hanno remotizzato funzioni che prima venivano svolte direttamente. Purtroppo, abbiamo avuto anche un incremento delle attività di contrasto alla pedopornografia on line. I ragazzi erano molto più presenti in rete con una sorta di socialità surrogata e vi sono state moltissime vittime in più, soprattutto per reati di adescamento. Ciò è dovuto al fatto che essendo più presenti in rete e avendo una socialità virtuale erano più esposti ad attività criminali di questo tipo.

Grazie per l'attenzione. Sono naturalmente a disposizione per rispondere a domande o a richieste di chiarimento.

PRESIDENTE. Grazie dottor Gabrielli, anche per la completezza della relazione. Do la parola all'onorevole Zanella.

FEDERICA ZANELLA. Lei è stato molto esaustivo e quindi non avrò molte domande da porre. Sulle frodi online come sul cyber crime a livello internazionale penso sia molto più facile attaccare che difendersi, tanto più che abbiamo visto che ci sono addirittura dei pacchetti a disposizione sul dark web.

Mi aggancio alla parte finale del suo intervento perché sono molto impegnata sul tema della tutela dei minori sul web. Lei ha parlato di aumento delle azioni di contrasto alla pedopornografia on line. Essendo stati collegati ai vari *device* molto più a lungo del normale, i minori sono stati anche vittime di reati on line legati al cyber bullismo e alla lesione della dignità personale, come nel caso del *revenge porn*, oltre

che vittime di frodi. Lei ha dati aggiornati su questi fenomeni ?

Per quanto concerne il discorso più attinente ai consumatori – sebbene la tutela dei minori on line sia comunque una tutela di consumatori e utenti di social network di minore età – le chiedo che cosa facciate per allertare i consumatori sui fenomeni che ci ha descritto, *phishing*, *vishing*, truffe sulle SIM card. L'altro giorno ho ricevuto una telefonata in cui mi è stato raccontato di una persona che si è trovata ad affrontare quel fenomeno di cui lei parlava, ovvero il SIM *swap*, e di essersi recato alla Polizia dove gli avrebbero detto che non potevano farci niente. Non gli hanno detto di recarsi alla Polizia postale. Infatti io gli ho risposto che ci sono sezioni dedicate a questi fenomeni. Si tratta di una vera e propria truffa e questa persona si è trovata cifre non indifferenti da pagare. Cosa si può fare ? Le stesse strutture preposte della Camera dei deputati che gestiscono le nostre mail personali mandano spesso alert per sventare i rischi di cadere nell'adescamento. Mi chiedo dunque cosa possiamo fare, anche noi, per incrementare le tutele dei consumatori, perché in effetti i dati sono inquietanti e in continua crescita.

Una ultima curiosità. Visto che ieri si parlava della possibilità di un attacco da parte di hacker filorussi che avrebbe paralizzato l'Italia, che attività avete posto in essere per monitorare il fenomeno ?

PRESIDENTE. Raccogliamo tutte le domande dei colleghi e poi decidiamo se procedere alle risposte, a tutte o a parte di esse, ovvero ad aggiornarci a una seduta successiva.

Do la parola all'onorevole Manca.

GAVINO MANCA. Nel ringraziare il direttore per la interessante ed esaustiva relazione che ci ha messo a disposizione, ho preso alcuni brevi appunti per porre delle domande spot, conformemente a come è stata la stessa esposizione.

Per quanto riguarda la tipologia dei reati si è fatta la distinzione tra i reati contro il patrimonio e reati contro le persone e abbiamo visto una cifra complessiva di 74 milioni e 400 mila euro. Sarebbe interessante sapere se si possa stabilire quanto di tale cifra si riferisca ai reati contro il patrimonio e quanto ai reati contro le persone.

Le chiedo altresì se si possa stabilire, da un punto di vista territoriale, da dove partano principalmente queste frodi. Sebbene, quando si parla di sistemi informatici, si possa operare da ogni parte del mondo, volevo sapere se si è fatta una sorta di cartina dell'azione malavitosa nel nostro Paese.

Per quanto riguarda la riorganizzazione delle vostre strutture, ho notato che tendenzialmente nella prima versione esse erano distribuite su base regionale, mentre ora sono diminuite. Per esempio, a proposito dei COSC, essi scendono da 20 a 18. Le chiedo se c'è una minore redistribuzione dal punto di vista territoriale e se sono state accorpate delle regioni, perché penso invece che l'organizzazione precedente, che gestiva il Paese in senso territoriale, fosse molto razionale.

Inoltre – ma non credo che potrà darci questa informazione nell'immediato – dato che questi fenomeni sono in continua evoluzione, le chiedo, proprio nella mia veste di parlamentare, se la loro disciplina dal punto di vista normativo sia adeguata ovvero se non siano necessari interventi ulteriori diretti ad agevolare la vostra azione di prevenzione e repressione.

Sempre dal punto di vista organizzativo, dato che si tratta di materia molto complessa e delicata e anche molto specializzata, le chiedo se ritenete quantitativamente corrette le vostre dotazioni finanziarie che vengono stanziate ogni anno dal ministero nonché le dotazioni di personale. Comprendo che sia un tema delicato e non intendo fare ragionamenti particolari, chiedo solo le dotazioni finanziarie e di personale siano strutturate in maniera adeguata rispetto a fenomeni che, come abbiamo visto, sono in crescita esponenziale.

PRESIDENTE. Do la parola alla vicepresidente Alemanno.

MARIA SOAVE ALEMANNO. Anch'io ringrazio il dottor Gabrielli per averci il-

lustrato una relazione che per quanto mi riguarda va al di sopra di qualunque aspettativa. Mi ha veramente dato la possibilità di conoscere in maniera dettagliata tutti i temi di interesse della Polizia postale e non solo, e che diventano fondamentali in questo periodo storico. Immagino che ciascuno di noi, a margine di questa audizione, avrebbe il desiderio di porre infinite domande perché i temi che ci ha rappresentato abbracciano veramente tantissime sfere d'interesse. Oggi però mi limiterò a porre una domanda specifica che mi interessa molto, fermo restando che anche tutte le altre che vorrei porre avrebbero lo stesso interesse, ma in questo momento, poiché sono membro della Giunta delle elezioni della Camera, abbiamo appena concluso un'indagine conoscitiva sui problemi emersi dal voto degli italiani all'estero. Dopo aver audito diversi soggetti istituzionali emerge con sempre maggiore prepotenza la possibilità di attuare un voto elettronico. Mi domando se sia una strada perseguibile e sicura, se abbiamo già degli elementi che possano essere messi al vaglio in questo momento, prima di intraprendere una qualunque strada dal punto di vista istituzionale, e se effettivamente ci sono delle modalità per poter rendere il voto sicuro senza ombra di dubbio.

Mi riallaccio alla domanda che poco fa poneva la collega Zanella. Accade purtroppo quotidianamente in questo periodo, anche a causa di una crisi internazionale che ha risvegliato l'attenzione di tutti riguardo alla cyber-sicurezza. Mi chiedo se effettivamente potremmo essere sotto attacco dal punto di vista delle nostre telecomunicazioni e se possiamo ritenerci al sicuro.

Espongo un ultimo tema senza necessità di una domanda, ma mettendolo solo all'attenzione di tutti. Mi dispiace soltanto che in questo caso ci siano veramente troppi termini tecnici, anche in lingua inglese. Mi rendo conto che quando parliamo di attività on line i confini cadono però mi pongo il problema che non tutti i nostri concittadini possano conoscere cosa si nasconde dietro a ogni termine e in questo momento invece, perlomeno a livello nazionale, dovremmo rendere edotti tutti i nostri cittadini al fine di poter consentire loro di avere un minimo di conoscenza su tanti reati, alcuni dei quali personalmente ne ho scoperto oggi l'esistenza. Vi ringrazio ancora per l'ottimo lavoro che ogni giorno svolgete.

PRESIDENTE. Do la parola all'onorevole Giuliano.

CARLA GIULIANO. Saluto e ringrazio il dottor Gabrielli che ha fatto una disamina dell'attività della Polizia postale e dei maggiori crimini informatici. Volevo innanzitutto chiedere al dottor Gabrielli se la Polizia postale prevede od organizza delle campagne di informazione per i comuni cittadini che, per una parte piuttosto rilevante, sono spesso poco avvezzi alle nuove tecnologie. Mi chiedo quindi se distribuiscano opuscoli informativi o mettano in atto campagne di informazione e di sensibilizzazione per allertare la popolazione da determinati attacchi. Vorrei inoltre sapere come in Italia i nostri sistemi informatici possano eventualmente essere rafforzati e in che modo, e se a livello normativo possiamo agire per prevenire e rendere più sicura la nostra infrastruttura informatica.

Per quanto riguarda i crimini che riguardano in particolare i minori e anche gli episodi di cyber-bullismo che sono in continuo aumento, volevo capire, oltre all'eventuale oscuramento di determinati siti o di determinati video, quali attività ulteriori possano essere messe in campo. Immagino che ci sia una prima esigenza di tempestività perché in questi casi è proprio la diffusione via web che crea e amplifica ancora di più il danno.

PRESIDENTE. Non essendovi altre richieste di intervento, aggiungo un paio di considerazioni e di richieste aggiuntive, al netto del fatto che sulla questione del voto elettronico non vorrei che ci sovrapponessimo all'attività che legittimamente svolge la Commissione affari costituzionali che su questo argomento credo abbia fatto o stia facendo gli approfondimenti del caso.

Sarei curioso di sapere come lavoriate insieme all'Agenzia sulla cybersicurezza per-

ché mi pare di capire che ci siano delle sovrapposizioni in termini di obiettivi e di temi, anche se immagino che ci sia una collaborazione tra il vostro, che è un servizio di polizia, e l'Agenzia, che invece svolge attività di direzione di carattere più generale.

Volevo sapere se era possibile avere dei dati in relazione a eventuali somme recuperate, rispetto alle indagini che avete svolto nei vari settori che sono stati evidenziati e per i quali anche io mi auguro che possano esistere dei nomi in italiano, in modo da far comprendere anche a una parte della popolazione più debole di che cosa si tratti. Parlo per esempio di una popolazione che ha più di 60-70 anni che sì usa gli smartphone ma che ha difficoltà a barcamenarsi in tutto questo curioso « acquario » di tipologie di truffe e di raggiri che a volte prendono le forme più disparate e che sono difficili da spiegare se non facendo degli esempi perché è poco indicativo semplicemente mettere in guardia una persona contro il *vishing*. Va spiegato che cosa è e quali conseguenze determina. In questo senso, credo sia molto opportuna la domanda della collega Giuliano in relazione alla possibilità di fornire strumenti di informazione e di prevenzione alla popolazione. Non so quanto possano essere efficaci e con che formula, però probabilmente avrete anche dati statistici sulle vittime, cioè quanti minori, quanti anziani. Il dato non è secondario.

Mi chiedo anche quale sia l'iter processuale dei reati contro la persona commessi, come il dottor Gabrielli ha già sottolineato, tramite piattaforme che hanno una loro collocazione in Paesi stranieri, fattispecie per alcuni versi magari meno importanti in termini economici rispetto ai gravi reati finanziari oppure alle alterazioni che si possono fare sui meccanismi bancari di grandi aziende, ma certamente non per questo debbono essere trascurate, penso alla diffamazione attraverso i social. A un certo punto si arriva a chiedere alla piattaforma l'identità della persona che, nascondendosi dietro un account qualunque o un nickname di fantasia, perpetra un reato che può essere quello di divulgazione di informazioni false, di diffamazione o altro. A quel punto, l'indagine si interrompe e anche qui probabilmente manca un elemento legislativo di cooperazione internazionale che possa fare da trait d'union per portare a una soluzione. Immagino che lo stesso problema accada per i reati finanziari per cui, al di là della collaborazione tra gli organi inquirenti e le polizie postali dei vari Paesi dove in uno c'è la sede legale della piattaforma in cui si prepara il reato e in un altro si trova il gruppo criminale che agisce, ci si chiede quale sia il motivo per cui non si riesca a pervenire alla celebrazione di un processo. Forse perché ci sono legislazioni diverse nei vari Paesi e quindi si rischia di portare avanti processi che poi decadono o addirittura non si riescono a instaurare ? La vostra attività rischia così di essere da un lato molto impegnativa, ma dall'altro non produttiva di risultati definitivi.

Come metodo di lavoro, ritiene di poter rispondere alle questioni che sono state poste, in tutto o in parte, oppure di rinviare a una seduta successiva ?

IVANO GABRIELLI, *direttore del Servizio di Polizia postale e delle comunicazioni*. Posso rispondere a tutte le domande senza nessun problema, se lei me ne dà facoltà. Mi riservo invece sin da subito di produrvi i dati più strutturati sia per quanto riguarda la pedopornografia sia per quanto riguarda tutta la parte *financial*, in modo da fornire dati conformi alle richieste avanzate e più analitici rispetto all'attività svolta. Vi farò avere sia i dati che riguardano i minori sia quelli che riguardano l'intero corpus della parte *financial*.

PRESIDENTE. Do la parola al dottor Gabrielli per le risposte ai quesiti posti.

IVANO GABRIELLI, *direttore del Servizio di Polizia postale e delle comunicazioni*. Parto dalle domande che sono state poste da più componenti. Circa le campagne informative, ne vengono svolte diverse. C'è un'attività di *alerting* puntuale che viene svolta dal nostro sito di riferimento, il sito del commissariato virtuale, che non è sol-

tanto un sito di tipo divulgativo ma viene utilizzato proprio per fare *alert* di questo tipo. È molto conosciuto anche tra gli utenti, abbiamo una community di qualche centinaia di migliaia di persone, nostri utenti abituali che ricevono le nostre notifiche e tra l'altro riceviamo diverse decine di migliaia di segnalazioni. È ovvio che può essere fatto qualcosa di più, soprattutto con riferimento, come diceva lei, presidente, alle fasce più deboli, soprattutto agli anziani che, a differenza dei più giovani, più abituati a informarsi in rete, non hanno confidenza con questo modo di informarsi. Bisognerebbe pensare a campagne di massa che intercettino metodi di comunicazione più diffusi e pervasivi. Mi riferisco anche alla televisione. Qualcosa è stato fatto con l'Associazione bancaria italiana (ABI). Di recente è stata lanciata una campagna secondo me molto intelligente in cui si mostravano comportamenti ricorrenti ed era molto efficace. Bisognerebbe però cercare di gestire una comunicazione più efficace raggiungendo il più ampio numero di persone. Periodicamente vi sono campagne che riguardano determinati fenomeni importanti e vengono lanciati *alert* continui, poi replicati sulle nostre piattaforme social, però è ovvio che è un rivolgersi a tutto un mondo di soggetti che riescono a informarsi attraverso la rete. Diversamente, dovremmo accedere a forme di comunicazione più di massa e forse più semplici per chi è meno confidente con lo strumento informatico. Soprattutto i giovani hanno una forte attenzione, ma vengono lanciate periodicamente anche campagne sulle truffe immobiliari o sulle *romance scam*. Sono molto verticali e molto settorializzate.

PRESIDENTE. Chiedo scusa, le truffe immobiliari come si concretizzano tecnicamente ? Sono transazioni che poi non vanno a buon fine ?

IVANO GABRIELLI, *direttore del Servizio di Polizia postale e delle comunicazioni*. Sono vendite e transazioni oppure locazioni che non si concretizzano. Soprattutto durante il periodo delle vacanze, quando i portali vengono utilizzati per cercare un'abitazione, abbiamo dei picchi considerevoli di denunce in tal senso.

PRESIDENTE. Sono quindi finti intermediari.

IVANO GABRIELLI, *direttore del Servizio di Polizia postale e delle comunicazioni*. Finti intermediari.

Per quel che riguarda gli attacchi di quest'ultimo periodo, la soglia di attenzione è altissima e qui mi collego anche ai rapporti che abbiamo con l'Agenzia per la cybersicurezza nazionale così come con le altre strutture che concorrono alla sicurezza nazionale cibernetica. La soglia alta significa che soprattutto da quando è cominciato il conflitto russo-ucraino abbiamo implementato protocolli di attività che hanno moltiplicato soprattutto la presenza in turni h24 del personale, al centro così come sui NOSC, che opera per monitorare ed essere attivo nel momento in cui c'è un attacco informatico di questo tipo. Ve ne sono stati diversi, ci stiamo muovendo con attività investigative complesse e lo stiamo facendo all'interno di un'architettura che ormai è definita nel nostro Paese, che ha vissuto un momento evolutivo particolare, ora cristallizzato con la presenza di un'Agenzia che raccoglie soprattutto quelle competenze in termini di resilienza e policy che erano distribuite su tanti ministeri. Oggi noi abbiamo un interlocutore tecnico, che è appunto l'Agenzia, che deve occuparsi della cyber resilienza. Essa emana fondamentalmente delle regole di sicurezza che poi debbono essere rispettate e vengono verificate attraverso un'attività ispettiva. Ha uno CSIRT (*Computer security incident response team*) che raccoglie le informazioni di sicurezza informatica. Le informazioni tecniche debbono essere calate all'interno delle infrastrutture che fanno presidio di sicurezza. La sicurezza informatica non è qualcosa di statico, è qualcosa di dinamico che oramai deve essere svolta attraverso strumenti intelligenti, che prevedano quindi il costante aggiornamento dei dati tecnici che servono a innalzare questi sistemi di sicurezza. Noi collaboriamo a stretto giro con loro perché

siamo portatori di informazioni di sicurezza importanti che sono il frutto del prodotto investigativo e preventivo, che viene ovviamente spogliato degli aspetti sensibili, e che vengono poi condivise anche con l'Agenzia. A margine degli attacchi informatici, è previsto che l'Agenzia informi la nostra struttura, l'organo del Ministero dell'interno per la sicurezza delle telecomunicazioni, anche ai fini dell'attivazione del procedimento penale che, come ho già detto, sempre segue un attacco informatico perché comunque si tratta sempre di fattispecie di reato. La norma istitutiva prevede che l'Agenzia, nel momento in cui intercetta o comunque acquisisce un'informazione – qualora non l'avessimo già acquisita anche noi, perché spesso le informazioni vengano acquisite in contemporanea dato che una struttura attaccata informa noi e informa loro – deve comunque riferire a noi proprio ai sensi di quanto previsto dall'articolo 331 del codice di procedura penale, essendo quindi pubblici ufficiali che fanno un'informativa di polizia giudiziaria ed è previsto che lo facciano a noi, in modo da poter da subito lavorare in simbiosi. C'è una collaborazione ovviamente assoluta e piena con quella struttura e devo dire che fino adesso è stata, anche se siamo partiti da poco, molto efficace.

Per quanto riguarda la domanda che chiedeva se vi sia una provenienza geografica peculiare, confermo che esiste perché alcune modalità truffaldine sono proprie anche di alcuni Paesi stranieri. Ci sono soprattutto alcuni Paesi dell'Africa occidentale, Nigeria e Costa d'Avorio, che operano in determinati settori. Ad esempio tutte le *romance scam* o le *sextortion* provengono da quel mondo e lo abbiamo visto sia perché gli attacchi partono da là sia perché alcuni gruppi criminali che sono etnicamente connotati in tal senso operano anche sul nostro sul nostro territorio. Paesi dell'Europa dell'est, come la Romania e la Bulgaria, fino a qualche tempo fa erano patria soprattutto di alcuni attacchi di *phishing* più evoluti. Anche qui trovavamo gruppi sodali sul territorio nazionale che dialogavano con le strutture di vertice che spesso risiedevano nei Paesi di provenienza, sia per quanto riguarda la parte dell'Africa occidentale sia per quanto riguarda l'Est Europa. Abbiamo anche una criminalità « autoctona » molto significativa che vede, per quanto riguarda le truffe, l'interessamento di tutto il territorio, però l'area della Campania è interessata in maniera importante. Con l'occasione, rispondo all'onorevole Manca anche sulla riorganizzazione territoriale. Come si è visto e come lei ha giustamente notato, abbiamo avuto una riduzione dei COSC da 20 centri operativi a 18. In realtà, la nostra struttura non cambierà. Abbiamo scelto di dare al Compartimento di Napoli la responsabilità di un coordinamento più ampio e quindi avrà sotto di sé le due sezioni, che non saranno più compartimenti, di Potenza e Campobasso. Dal punto di vista dei presidi e anche delle dotazioni attuali, perché è previsto comunque lo stesso livello di dirigenza, non si avranno mutamenti. Sarà dato un coordinamento all'autorità napoletana perché in quell'area insistono gruppi criminali che spesso hanno visto nella pratica operativa l'interessamento di questi altri due compartimenti e quindi abbiamo scelto un concentramento di coordinamento su Napoli, tra l'altro elevando Napoli a una dirigenza superiore. I nostri Compartimenti sono adesso diretti per lo più da primi dirigenti. Sei compartimenti, tra cui quello campano, verranno elevati a livello di dirigenza superiore: Milano, Torino, Bologna, Roma, Napoli e Palermo. Quindi la Campania verrà ulteriormente potenziata da questo punto di vista e rimane la scelta strategica di avere un presidio territoriale perché, l'ho già detto, per noi è stato assolutamente efficace.

Per quanto riguarda invece la parte normativa, abbiamo una struttura normativa importante in Italia. A livello di previsione di fattispecie di contrasto siamo forse tra i più evoluti al mondo. Sulle frodi potremmo fare qualcosa di più, soprattutto dovremmo lavorare a una migliore definizione di alcuni aspetti aggravanti e alcune fattispecie. Sebbene il reato associativo ci permetta di contestare e di attivare anche strumenti investigativi diversi elevandosi la soglia edittale, alcune fattispecie potrebbero però pre-

vedere forme di punibilità un po' più elevate che permettano l'attivazione di strumenti investigativi come le intercettazioni. Dal punto di vista organizzativo, ritengo che, trattandosi di fenomeni che hanno proprio una dimensione aterritoriale per eccellenza, il momento del coordinamento potrebbe essere meglio valorizzato, questo a livello centrale. Occorrerebbe prevedere quindi, come si è previsto anche per le infrastrutture critiche o per la pedopornografia, una forte componente centrale che fornisca immediatamente, in tempo reale, gli indicatori criminali che permettano da subito, soprattutto agli istituti bancari, di arginare le attività che, come ho già detto, esplodono in fenomeni concentrati in brevissimo tempo e che mirano a fare grandi numeri. Se si avessero per tempo informazioni banali come la ricorrenza di IBAN sui quali vengono modificate le cifre o degli IP che vengono utilizzati per mandare determinate comunicazioni truffaldine, noi riusciremmo ad avere una attività di prevenzione molto efficace, attività di prevenzione che deve essere assolutamente preponderante rispetto all'attività di contrasto, perché, come giustamente ha rilevato il presidente, qui ci si trova in situazioni in cui le attività investigative hanno momenti non compatibili con la tutela dei soggetti, cioè sono attività di lunghissimo respiro, soprattutto perché riguardano l'estero. L'Italia è inserita in un contesto internazionale di cooperazione che vede tutto il mondo occidentale all'interno della Convenzione di Budapest sul *cybercrime* che costituisce il *framework* giuridico internazionale più importante in questa materia. L'Italia è uno dei Paesi che hanno aderito per primi, ha strutturato il proprio *framework* legale rispecchiando appieno la Convenzione, vi è un punto di contatto che è istituito presso il CNAIPIC che serve ad attivare in tempo reale l'attività di cooperazione, perché, come è stato detto giustamente, stiamo parlando di prove informatiche che purtroppo o non vengono raccolte in maniera uniforme per via di leggi difformi in materia di *data retention* o comunque intercettano momenti di non reciprocità. Ci troviamo quindi a dover scontare in sede rogatoriale lunghissimi percorsi che non vanno a buon fine. In Italia abbiamo uno strumento molto efficace. L'articolo 234-*bis* del codice di procedura penale ha previsto l'ingresso all'interno dei nostri procedimenti dei dati che vengono forniti da chi è legittimo detentore, anche se internazionale, di quel dato. Mi spiego meglio. Chiediamo a Facebook di fornirci un dato esibendo un decreto italiano. Facebook ritiene di dover ottemperare e corrisponde all'informazione, che ci viene fornita. Quell'informazione viene acquisita all'interno del nostro procedimento, accorciando enormemente i tempi e dandoci la possibilità poi di sviluppare ulteriormente l'attività investigativa. L'attività investigativa in questo particolare settore cerca di ripercorrere punto per punto le attività tecniche svolte fino ad arrivare a un soggetto che poi viene – passatemi il termine – aggredito in termini di indagine ordinaria. La nostra attività non è soltanto un'attività tecnica. È tecnico-informatica fino a un certo punto, dopodiché diventa un'attività investigativa vera e propria. Noi dobbiamo arrivare a quel punto, il momento in cui facciamo atterrare indagini svolte nel virtuale nel reale. Questo tipo di attività prevede dei passaggi spesso molto onerosi in termini di ricostruzione dell'iter con cui è stata fatta una truffa o una diffamazione. Sarebbe importante se riuscissimo ad accorciarlo ed è lo scoglio sul quale ci infrangiamo perché non tutti i Paesi hanno la stessa legislazione, non tutti i Paesi, per esempio per i reati contro la persona, prevedono la diffamazione e quindi questo comporta difficoltà nel poter procedere a livello investigativo. Si procede comunque e lo si fa grazie al fatto che gli investigatori capaci riescono a ricostruire quelle miriadi di informazioni che possano poi portare all'individuazione di un responsabile a prescindere dal dato di registrazione, a prescindere dal puntuale dato con cui è stato postato un commento diffamatorio, però ovviamente sarebbe auspicabile, come ripeto, un *framework* internazionale che tenga conto anche delle esigenze di neutralità che la rete ormai si è data da tempo. Sappiamo che è anche il territorio della libertà di espressione, quindi

portare all'interno momenti di identificazione importante dei soggetti che si affacciano in rete non sempre viene visto come un momento valorizzante rispetto a ciò che la rete fornisce.

Circa la dotazione finanziaria del personale, in questo momento stiamo cercando di efficientare al massimo la nostra struttura. Questo passa attraverso modalità importanti di formazione. Stiamo lavorando molto dal punto di vista della formazione. Sono stati recentemente istituiti tre corsi specialistici diretti sulle capacità trasversali investigative. Ne stiamo costruendo uno sull'*incident response* che mira all'attività di indagine a margine di attacchi cibernetici. Ne abbiamo già istituito uno che riguarda l'OSINT, quindi l'attività di investigazione fatta su fonti aperte ed è molto importante. Ne avremo uno dedicato alle fasce deboli, quindi all'investigazione con un occhio particolare alla formazione di attività sotto copertura per il contrasto alla pedopornografia. Il tema del personale è importante e trasversale, non soltanto per la nostra istituzione. È ovvio che in questo momento c'è un enorme bisogno di esperti in cyber sicurezza. Stiamo lavorando per costruire dei profili all'interno della Polizia di Stato che siano dedicati a questa esigenza, però scontiamo un ritardo, anche nel processo formativo perché anche portandoci oggi sul mercato non credo che tutti avremmo la possibilità di intercettare le esigenze, questo a prescindere dall'istituzione che si affaccia sul mercato. Noi, l'Agenzia, la Difesa scontiamo tutti lo stesso problema. Bisogna creare una forza lavoro importante e farlo da subito, soprattutto cercando di orientare la formazione secondaria, quindi non aspettare prodotti che possono venire o verranno dall'università, ma intercettare momenti di formazione intermedia, come la scuola secondaria, rivalorizzando gli istituti tecnici, in modo da poter avere da subito forza operante e forza produttiva che può essere immediatamente assorbita dallo Stato, ma anche dai privati con i quali ci confrontiamo spessissimo e hanno lo stesso bisogno, noi e a livello internazionale. La cybersicurezza è oggi un percorso e un'opportunità enorme, soprattutto per i ragazzi, perché fa curriculum, è un'attività assolutamente interessante e c'è una domanda fortissima in questo particolare settore. Costruirsi percorsi professionali credo che sia semplice, vi sono tante opportunità, anche considerando il fatto che poi chiunque assume soggetti che hanno una base poi a loro volta formano e ultra specializzano. Quindi è veramente un percorso professionale interessante.

PRESIDENTE. Che formazione hanno ?

IVANO GABRIELLI, *direttore del Servizio di Polizia postale e delle comunicazioni*. Noi avremmo bisogno di formazione di informatici di base quindi persone che capiscono sia di reti sia di sistemi informatici in generale e che comunque abbia già un minimo di infarinatura sulla gestione della sicurezza informatica, quindi come viene organizzata un'infrastruttura, quali sono i rudimenti per mettere in piedi un sistema di sicurezza. Su quella formazione base poi possono essere verticalizzate anche forme di formazione che attengono più al livello investigativo proprio del nostro settore. Su quella competenza l'azienda privata così come le altre Istituzioni possono costruire qualcosa di importante anche perché, come ho già detto, ce n'è bisogno e quindi la domanda è fortissima.

PRESIDENTE. Chiedo ai colleghi se vi siano altre domande o richieste di chiarimento. Do la parola alla vicepresidente Alemanno.

MARIA SOAVE ALEMANNO. Chiedo se sia possibile avere qualche informazione sul voto online, nello specifico per gli italiani all'estero.

IVANO GABRIELLI, *direttore del Servizio di Polizia postale e delle comunicazioni*. Come Polizia postale ho fatto parte del tavolo di lavoro che si è occupato di proporre soluzioni per portare all'adozione di un sistema normativo che disciplini il voto online. Distinguiamo il voto line in due macro-categorie. Una è un surrogato del

voto cartaceo fatto per diretta persona, attraverso una postazione fissa che prevede l'identificazione di un soggetto che si presenta in un sito elettorale e, attraverso un account che viene generato al momento, esprime la propria preferenza. Siamo di fronte quindi a un surrogato di quello che avviene con una scheda elettorale, né più né meno, cambia soltanto la raccolta e anche il conteggio immediato, ma è estremamente verificabile e in questo caso non si pongono particolari problemi. Il voto da remoto invece qualche problema lo pone, perché c'è la possibilità di certificare assolutamente il percorso del voto, attraverso anche i sistemi di *blockchain* che vengono utilizzati per esempio per la moneta elettronica. Adesso si stanno studiando sistemi che certifichino a livello distribuito anche atti notarili, quindi avremmo pubblicamente il percorso di un voto anonimo che va da A a B e quindi potremmo sicuramente quantificarlo. Il problema sta a monte, cioè nell'identificazione del soggetto. Il soggetto ha comunque in mano un device: deve presentarsi, deve esserci corrispondenza tra chi esercita quel voto, attraverso lo strumento informatico, e il soggetto che effettivamente è titolato. Bisognerebbe cercare di trovare momenti di identificazione sicura di quel soggetto e quindi dovremmo passare attraverso sistemi di rilevamento biometrici, sistemi di certificazione forte, come avviene con lo SPID. Siamo sicuri che siano sufficienti ? È possibile che un soggetto possa essere non libero nel momento in cui esprime il voto ? Certo per gli italiani all'estero, pensando al voto per corrispondenza, ci troveremmo sostanzialmente nella stessa situazione. Può essere che chi ha espresso quel voto per corrispondenza, lo abbia fatto come autore mediato di qualcun altro o abbia subito pressioni. La tecnologia in questo caso è pronta, bisogna accettarne il rischio perché comunque un rischio c'è sempre. Il rischio viene abbattuto al massimo nel momento in cui c'è un soggetto che si reca in un seggio elettorale, si fa identificare e comunque propone la propria preferenza. Il rischio diventa leggermente più ampio nel momento in cui questo soggetto esercita questo diritto da casa propria con uno strumento elettronico. Lasciando ovviamente impregiudicata o comunque a voi la valutazione sui rischi di pressione e di interferenze sul voto, però a livello tecnico lo si può fare accettando il rischio che dall'altra parte vi sia un soggetto che deve essere identificato e identificabile.

PRESIDENTE. C'è anche l'elemento della segretezza da tenere in considerazione. Ringraziamo il dottor Gabrielli per la disponibilità e anche per la prontezza e velocità che ci ha permesso di esaurire in una sola audizione di oggi anche la fase dell'approfondimento delle domande. Se ci sono ulteriori dati saremo felici di riceverli, anche mantenendo un rapporto costante di collaborazione con la Commissione, per le sue attività istituzionali ed eventuali attività di indagine con il vostro servizio. Ancora una volta grazie per la disponibilità e grazie per il lavoro che svolgete quotidianamente. Ci riaggiorniamo secondo il calendario dei lavori già fissato dall'Ufficio di Presidenza per la prossima settimana.

Dichiaro conclusa l'audizione.

**La seduta termina alle 13.**

*Licenziato per la stampa*
*il 25 luglio 2022*

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

*18STC0188460*