Ministero dell'Interno

DIPARTIMENTO DELLA PUBBLICA SICUREZZA
DIREZIONE CENTRALE PER LA POLIZIA STRADALE, FERROVIARIA, DELLE COMUNICAZIONI E PER I REPARTI SPECIALI DELLA POLIZIA DI STATO
Servizio Polizia Postale e delle Comunicazioni

N. 300.D/2017/784-MS.R/1 Roma, *data del protocollo*

OGGETTO: Relazione alla 7^ Commissione "Istruzione pubblica, beni culturali" del Senato, relativa all'audizione del 7 aprile 2021 del Direttore del Servizio Polizia Postale e delle Comunicazioni, dott.ssa Annunziata Ciardi, nell'ambito dell'indagine conoscitiva, sull'impatto del digitale sugli studenti, con particolare riferimento ai processi di apprendimento.

AL SIGNOR PRESIDENTE
DELLA 7^ COMMISSIONE "ISTRUZIONE PUBBLICA, BENI CULTURALI" DEL SENATO DELLA REPUBBLICA ITALIANA
commissioneistruzione@senato.it

ROMA

La Polizia Postale e delle Comunicazioni è un reparto specialistico della Polizia di Stato che opera in prima linea nella prevenzione e nel contrasto della criminalità informatica, a garanzia dei valori costituzionali della segretezza della corrispondenza e della libertà di ogni forma di comunicazione.

Il Servizio Centrale, vertice della struttura, è punto di riferimento nel coordinamento, nella programmazione e nella pianificazione operativa degli uffici periferici della Specialità.

L'attività di prevenzione e contrasto viene supportata da un sistematico coinvolgimento degli organismi di cooperazione internazionale giudiziaria e di polizia, attraverso la condivisione di strategie di monitoraggio e contrasto dei fenomeni concernenti il cybercrime.

La Polizia Postale e delle Comunicazioni ha competenze estremamente ampie, alcune delle quali sono esclusive: in particolar modo forte e puntuale è l'impegno nella prevenzione e nel contrasto degli attacchi cibernetici alle infrastrutture critiche, attraverso l'operatività del **Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche- CNAIPC**, nella lotta alla pedopornografia online e a tutte le forme di aggressione dei minori in rete attraverso l'operatività del **Centro Nazionale per il contrasto alla pedopornografia online-CNCPO**, nella prevenzione del cyberterrorismo, nel contrasto dell'hacking e del financial cybercrime, la repressione dei reati commessi sui socialnetwork, nonché il contrasto ai reati postali. Ai due Centri si

affianca un avamposto virtuale costituito dal **Commissariato di ps online**, portale istituzionale costantemente aggiornato che consente ai cittadini di segnalare, informarsi, chiedere ed ottenere informazioni relative alle emergenze online.

Nel corso del 2020, il diffondersi dell'epidemia da Covid-19 ha senz'altro inciso sulla qualità e quantità dei fenomeni legati al cybercrime, con particolare riferimento al crimine di tipo economico-finanziario (**attacchi alle infrastrutture critiche + 246%; frodi realizzate mediante tecniche di social engineering del tipo BEC e CEO Fraud + 64,1%**) e a quelli in danno dei minori.

Il periodo del lockdown ha costretto l'intera popolazione a rivedere le proprie abitudini di vita e di lavoro ed ha comportato necessariamente uno spostamento di molte attività sulla rete, facendo registrare, in tal modo, anche un **incremento sostanziale della presenza dei minori online.**

Le attività di indagine relative alla protezione dei minori in rete hanno condotto ad un **incremento dei casi trattati pari al 132%** e ad un **numero di persone indagate del 90% in più** rispetto all'anno precedente.

Nel complesso**, le vittimizzazioni online a carico di minori**, siano esse imputabili ad adescamento, cyberbullismo, truffe online, furto di identità digitale, hanno subito un **incremento pari al 77%**.

Fin dall'inizio della diffusione pandemica del virus Sars-Cov-2, la Polizia Postale e delle Comunicazioni, con l'impiego di tutte le sue articolazioni territoriali, coordinate attraverso l'azione strategica assicurata dal Servizio, **ha intensificato il monitoraggio della rete** alla ricerca di materiale pedopornografico e di altri contenuti lesivi per i minori.

Il numero delle denunce per reati con vittime minorenni ha conosciuto un progressivo rallentamento, in concomitanza del lockdown nazionale, nei mesi di marzo e aprile; in tale periodo l'emergenza epidemiologica e i timori di contagio hanno probabilmente indotto molte famiglie a procrastinare le eventuali denunce e la stessa presenza dei genitori in casa ha probabilmente aumentato la sorveglianza sui comportamenti online dei ragazzi. Con le progressive riaperture però, avviate nel mese di maggio, e la prosecuzione dell'attività scolastica in modalità online, le denunce hanno ricominciato ad incrementarsi, mostrando un andamento crescente lungo il secondo semestre del 2020.

A livello operativo, è stato **rafforzato il raccordo delle investigazioni** nei canali di cooperazione internazionale giudiziaria e di polizia, quale presupposto strategico fondamentale per disarticolare le comunità virtuali illecite caratterizzate da una struttura organizzata, **ha innalzato,** laddove possibile**, il livello di collaborazione con i social network** più diffusi in Italia, in un'ottica di sinergia nella lotta all'utilizzo improprio del web, definendo canali preferenziali di comunicazione e gestione dei casi penalmente rilevanti, è stato **aumentato l'impegno funzionale** all'individuazione di un numero

sempre maggiore di siti che contengono materiale pedopornografico, da inserire nella black list, stilata dal Centro Nazionale per il Contrasto alla Pedopornografia On-line (C.N.C.P.O.), il cui accesso viene inibito, con modalità diverse a seconda dell'ubicazione dei server utilizzati, agli utenti internet attivi sul territorio italiano.

L'avvento della pandemia ha di fatto bruciato le tappe di una progressione della diffusione dell'uso delle nuove tecnologie in fasce di età sempre più precoci: per riempire i lunghissimi pomeriggi chiusi in casa, per compensare la mancanza di contatti con i coetanei e i familiari, sono numerosissimi i bambini che hanno acquisito, in pochi mesi, una dimestichezza maggiore all'uso di tablet e smartphone.

I bambini più piccoli che approcciano la rete sono attratti dai giochi online, si muovono sui socialnetwork ma rivelano la loro forte fragilità per inesperienza, per immaturità cognitiva ed emotiva, e per una profonda suggestionabilità che li espone, inevitabilmente, al rischio di essere vittime di cyberbullismo e ancor più di adescamento online.

Anche la capacità di prefigurarsi le conseguenze delle azioni online, le conoscenze relative alla distinzione tra gioco e reato sono così labili e in via di sviluppo in queste fasce di età che l'idea di un approccio completamente autonomo, privo di una salda guida adulta è davvero un'evenienza piena di incertezza e, di fatto, pericolosa.

Se ci si pone la domanda se abbia un senso **proibire l'uso di devices tecnologici ai minori di 14 anni**, si arriva ad ipotizzare che oggi si possa procrastinare agilmente alla fase adolescenziale il primo approccio al mondo virtuale.

Un eventuale divieto di uso di supporti tecnologici per minori di 14 anni sarebbe difficilmente praticabile poiché l'acquisto degli stessi non è praticamente mai effettuato da bambini di quell'età ma dai genitori, che potrebbero facilmente essere propensi a dichiarare un interesse personale verso smartphone, tablet, consolle di gioco, etc., considerando che, dopo l'avvento della pandemia, tutte le famiglie hanno incrementato la quantità di devices presenti proprio per garantire la prosecuzione di attività scolastiche e lavorative.

Non solo, essere Millenials oggi significa vivere concretamente i vantaggi del progresso ma è evidente che si tratta di un percorso in cui i primi approcci, le successive esplorazioni necessitano inevitabilmente di una guida e di una riflessione mediata dagli adulti significativi, genitori e insegnanti in primis.

Attraverso un'esposizione progressiva a tali strumenti e ai servizi di networking, sotto la supervisione degli adulti, i bambini prima e i ragazzi dopo possono sviluppare un rapporto sano con tali inevitabili realtà del mondo moderno. Escluderli da tali esperienze può comportare il rischio che, avvicinati da coetanei al web, siano completamente impreparati e fortemente attratti da qualcosa, senza conoscerla.

Sarebbe auspicabile immaginare un percorso progressivo, mediato dagli strumenti e dai linguaggi propri dell'attività educativa, la cui finalità sia quella di

garantire l'acquisizione da parte dei minori di consapevolezza e responsabilità nell'uso dei nuovi media e dei devices, attraverso il conseguimento di un **"patentino digitale"**.

I ragazzi potrebbero così acquisire un'abitudine a riflettere sul rischio e sulle opportunità di internet, dei socialnetwork e della tecnologia nei luoghi della loro formazione, con l'obiettivo di conseguire una sorta di titolo, il patentino, che illustri come e quanto siano diventati consapevoli e siano in grado di agire in modo corretto e protetto in rete.

La maggiore presenza in rete di bambini piccoli durante l'ultimo anno, l'allungamento dei tempi di permanenza sul web come conseguenza della mancanza di attività ludiche e sportive in presenza, **hanno attratto anche l'attenzione di adulti interessati ad interazioni sessuali in rete con bambini** oppure, talvolta, facilitato l'incontro tra ragazzi più grandi e bambini, generando situazioni di reale pericolo, sia da un punto di vista concreto che psicologico.

E' evidente come le regole che i diversi **socialnetwork** hanno indicato per garantire l'accesso a piccoli internauti di età **mai inferiore ai 13 anni** non siano sufficienti a garantire che bambini più piccoli accedano ai loro servizi e ne usufruiscano: in questo ambito è stato verificato come la sorveglianza degli adulti e il rispetto puntuale dei limiti di età previsti sia un'evenienza non sempre certa. Molti bambini di età inferiore ai 13-14 anni hanno profili social e li usano in pressochè totale autonomia, in una condizione che non li preserva dall'accesso a contenuti inappropriati per la loro età, nonché la raggiungibilità di potenziali vittime fragili da parte di prepotenti e malintenzionati.

I 14 casi di adescamento online che riguardavano bambini fino ai 9 anni denunciati nel 2018 sono diventati **41 casi del 2020**: hanno riguardato approcci sessuali in rete, avvenuti soprattutto sui socialnetwork, circuiti virtuali ai quali bambini così piccoli non dovrebbero nemmeno accedere.

I casi registrati sono un numero che, seppur ancora contenuto, preoccupa per l'estrema fragilità che caratterizza queste piccole vittime e per il potenziale lesivo che può avere un approccio sessuale precoce tecnomediato. Spesso infatti **l'adescamento online** prevede prima la costruzione di un legame di reciproca fiducia, a cui segue magari l'invio di materiale pornografico quale avvicinamento psicologico al vero interesse dell'adulto-groomer che è quello di avviare il bambino ad attività sessuali autoerotiche, sino alla produzione e all'invio di immagini e video sessualmente espliciti.

La pandemia e quanto ha determinato in riferimento al rapporto tra minori e internet hanno evidenziato come un'anticipazione dell'approccio alle nuove tecnologie da parte dei bambini, così come una loro maggiore presenza in rete, determinino potenziali effetti negativi in termini di rischio, aumentando la possibilità che siano vittime troppo precocemente di varie forme di violenza tecnomediata o che compiano azioni illegali, sempre attraverso la rete.

Alcuni fenomeni di solito propri dell'età adulta, come la **sextortion** (estorsione sessuale conseguente all'invio di immagini sessualmente esplicite), hanno investito, nell'ultimo anno, anche i ragazzi e talvolta anche i bambini, arrivando ad interessare 14 casi di ragazzi di età inferiore ai 13 anni.

Recentemente si è osservato come la tendenza ad esplorare la sessualità via web sia aumentata sia attraverso l'ascesa di circuiti di videosharing come Youporn e Xamster, sia attraverso la frequentazione di chat e servizi di rete in cui le persone si "incontrano" per sessioni di scambi sessuali in rete. I minori, soprattutto in fase adolescenziale, si avvicinano per curiosità e goliardia a questi circuiti e mostrano tutta la loro inesperienza e suggestionabilità, cadendo nelle trappole realizzate da sedicenti avvenenti ragazze, spesso affiliate a vere e proprie organizzazioni criminali.

Per gli adolescenti la distinzione fra i diversi fenomeni di sexting, revengeporn, cyberbullismo, grooming, pedopornografia sembra perdere sempre più di consistenza. Nella loro esperienza l'esplorazione della sessualità può comprendere lo scambio di immagini sensuali quando sono innamorati, lo scambio di questo materiale per goliardia fra coetanei, la diffusione incontrollata di insulti contro un compagno per prepotenza o per vendetta, la partecipazione a gruppi chiusi di messaggistica dove fare a gara a chi ha lo stomaco più forte nel guardare immagini anche di violenza sessuale su bambini: tale dinamismo, non sempre positivo ha determinato l'avvio di numerose indagini la cui finalità era fermare la circolazione di materiale illegale e individuare i partecipanti, maggiorenni e minorenni, responsabili della gestione dei canali per lo scambio delle immagini e dei link.

Le attività investigative che hanno consentito di individuare decine di minorenni che, con livelli assai labili di consapevolezza, partecipavano al turpiloquio tra coetanei, scambiandosi su circuiti di messaggistica immagini illegali di pedopornografia e di violenza, fra cui ve ne erano diverse rubate a compagne di classe e diffuse senza controllo.

Già nel corso del 2019 era stato posto sotto osservazione il fenomeno degli stickers. Nati come adesivi virtuali scaricabili su Whatsapp, erano ben presto diventati attraverso sapienti opere di ritaglio delle immagini veicolo di foto violente, antisemite, discriminatorie ed infine persino pedopornografiche, senza che nessuno dei ragazzi segnalasse la cosa o la considerasse grave in se per se.

Nel 2020, l'Operazione *"Pay to see"* è scaturita dalla denuncia di un genitore che aveva rinvenuto sul cellulare della figlia una chat contenente un vero e proprio *listino prezzi* per prestazioni di natura sessuale online, con tariffe differenziate a seconda delle richieste (es.: *"sexchat 45 minuti in cui faccio da schiava = 30 euro"*). La Polizia Postale di Bari e Foggia, coordinata dal C.N.C.P.O., ha eseguito 21 perquisizioni su tutto il territorio nazionale, anche nei confronti di diversi minori che avevano acquistato i "servizi" offerti dall'adolescente.

L'Operazione *"Dangerous Images"* invece ha condotto alla denuncia di 20 minorenni che, in concorso tra loro, detenevano e diffondevano materiale di pornografia

minorile. La Polizia Postale di Firenze ha individuato un 15enne, organizzatore e promotore, insieme ad altri coetanei, dello scambio di innumerevoli filmati e immagini pedopornografiche, anche in forma di *stickers*, attraverso diversi social network. Il giovane era in possesso anche di numerosi files c.dd. *gore*, ovvero filmati e immagini provenienti dal Dark Web, raffiguranti suicidi, torture, mutilazioni, squartamenti e decapitazione di persone e animali.

La pandemia ha imposto inoltre nuove modalità per lo svolgimento **dell'attività scolastica** che, sospesa in presenza, si è avvalsa dell'uso di piattaforme di videochiamata per tutti gli studenti, da quelli della scuola primaria a quelli della secondaria di secondo grado.

Sono stati circa **30 i casi di intrusione nella didattica a distanza** segnalati nel corso del 2020: emerge che in molti casi sono stati identificati, quali autori delle condotte principali o concorrenti nel reato, **soggetti minorenni, talvolta non imputabili** poiché infraquattordicenni. Il fenomeno ha interessato trasversalmente tutto il territorio nazionale, con il coinvolgimento di studenti soprattutto delle scuole secondarie.

Le condotte sono consistite, sostanzialmente, nell'accesso abusivo alle piattaforme (Zoom in massima parte, ma anche Google Meet, Jitsi, ecc..) e nel compimento di azioni di disturbo, nella maggior parte dei casi concretizzatesi in offese ai docenti o nella pubblicazione di contenuti pornografici. **I Dirigenti degli istituti scolastici**, così come i docenti destinatari delle offese, pur riservandosi in molte delle segnalazioni la facoltà di proporre querela, **hanno poi di fatto rinunciato, optando per l'apertura di procedimenti disciplinari all'interno degli istituti stessi.**

Le attività organizzate ruotavano intorno a gruppi Telegram, denominati "Invadiamo Lezioni", "Invadiamo le Lezioni 2", ove erano pubblicati anche dei veri e propri regolamenti di funzionamento del servizio, e talvolta anche su canali Youtube, questi ultimi prontamente chiusi dalla piattaforma. In un caso, a Lecce, all'incursione in DAD è seguita una condotta di adescamento ai danni di due minori di sesso femminile.

Significativa l'attività di indagine svolta dal Compartimento di Genova che ha condotto all'identificazione e alla denuncia di tre giovani *hacker in erba*, che pubblicando i link delle lezioni online invitavano compagni di scuola e altri minori ad interrompere lezioni ed interrogazioni online.

La prevenzione e la sensibilizzazione rappresentano per la Polizia Postale e delle Comunicazioni la modalità elettiva per promuovere una tutela che sia sempre più efficace e partecipativa: da anni ingenti risorse umane, specializzate e formate sui temi dell'approccio ai giovani e sui correlati psicologici dell'uso delle nuove tecnologie, vengono impegnate quotidianamente in incontri scolastici con i ragazzi, nella conduzione di seminari e meeting anche online, in cui gli studenti possano ascoltare da operatori di polizia come proteggersi e divertirsi in sicurezza, usando il web e i socialnetwork.

Le iniziative e i progetti di sensibilizzazione sono stati numerosissimi negli anni e la cooperazione con altre istituzioni e associazioni di settore ha caratterizzato il metodo di realizzazione delle varie iniziative: tra le tante meritano menzione "*Una vita da social*", la più grande campagna educativa itinerante a bordo di un truck brandizzato, con un'aula didattica multimediale con postazioni internet dove gli Operatori della Polizia Postale incontrano studenti, insegnanti e genitori sui temi della sicurezza online. L'obiettivo è quello di sensibilizzare gli utenti dei social network ad un uso consapevole e responsabile per proteggersi dai pericoli dell'adescamento in chat e del cyberbullismo; #cuoriconnessi è una Campagna educativa itinerante teatrale sul cyberbullismo realizzata in collaborazione con Unieuro che porta nei teatri centinaia di ragazzi lasciando che si confrontino e ascoltino storie di vittime di cyberbullismo per comprendere come evitare di fare del male o di subirne.

Questo complesso e mutevole quadro di rischio per i bambini e i ragazzi ha confermato l'importanza di articolare un'azione di tutela dei più piccoli dal rischio online sempre più capillare e puntuale.

L'art. 240 del D.L. n. 34/2020, convertito in legge n.77/2020, indica l'istituzione di una nuova Direzione Centrale, per la sicurezza cibernetica. Si tratta di una proiezione fondamentale per realizzare un'attività di coordinamento e attuare politiche di protezione dal rischio cibernetico sempre più incisive e chirurgiche, anche in ambiti come quello della protezione dei minori in rete, caratterizzati da estrema delicatezza e necessaria sinergia.

In continuità con l'istituzione della nuova Direzione Centrale per la Sicurezza Cibernetica sarà realizzato un **Centro Anticrimine per i Minori Online (CAMON)** che estende la sua opera di coordinamento, tutela e protezione dei bambini e dai ragazzi da ogni forma di minaccia proveniente dal web e dalle nuove tecnologie.

Il Centro sarà operativo nelle 24 ore nel dialogo con i principali *stakeholders* interessati, quali ONG e **tutte le scuole** presenti sull'intero territorio nazionale, in modo da catalizzare in un unico *hub* segnalazioni, trend ed esigenze di tutela dei ragazzi nelle quotidiane dinamiche del web.

Tale nuovo Centro costituirà un punto di riferimento per il mondo della scuola e delle associazioni attive per la protezione dei minori, con la finalità ultima di promuovere un approccio integrato al rischio online e una sinergia sempre più efficace nella gestione delle fragilità adolescenziali che si riversano in rete: al centro affluiranno segnalazioni e casi che, attraverso un'opera di coordinamento nazionale, daranno origine ad investigazioni ed approfondimenti per monitorare il rischio online e contribuiranno a diramare alert e informazioni utili per la protezione dei minori in rete.

IL DIRETTORE DEL SERVIZIO
Ciardi