Safe Web

Premessa Il compendio Safe Web nasce da un percorso di riflessione e sintesi dei principali rischi che attualmente i giovani affrontano nel loro rapporto quotidiano con le nuove tecnologie. La Polizia di Stato approccia queste criticità attraverso un’opera quotidiana di accoglienza, ascolto e comunicazione sui temi della sicurezza in Rete. Attraverso azioni di sensibilizzazione e informazione, con l’ascolto diretto dei ragazzi e delle loro famiglie quando si trovano in difficoltà, la Polizia di Stato, attraverso una delle sue Specialità, la polizia postale e delle comunicazioni, pattuglia il Web e contribuisce a rendere concreto l’impegno di rendere Internet un posto sicuro e legale per tutti. Negli anni appare sempre più chiaro che per resistere ai pericoli connessi all’uso delle nuove tecnologie è necessario, non solo aumentare le strategie di auto-protezione delle potenziali vittime, ma anche agire nella direzione di un progressivo potenziamento delle sinergie fra adulti. Il compendio Safe Web è stato validato scientificamente dal Centro studi per la Formazione, analisi criminologica e la ricerca sul Web (Far Web), diretto dal prefetto Roberto Sgalla, direttore centrale della polizia stradale, ferroviaria, delle comunicazioni e per i reparti speciali della Polizia di Stato e presieduto dalla professoressa Anna Maria Giannini, con la partecipazione di eminenti accademici di ambito psicosociale e giuridico. Il compendio Safe Web si propone l’obiettivo di porsi come uno strumento duttile e utile ad aiutare il mondo della scuola e i suoi principali attori a orientarsi nella gestione concreta dei casi di rischio on line: la complessità di fenomeni come il cyberbullismo, il sexting e l’adescamento on line viene amplificata da un panorama legislativo in divenire che impone un continuo adeguamento, da uno sviluppo della tecnologia che appare sempre più rapido e dal carattere imprevedibile che le inquietudini adolescenziali possono assumere in una società, quella attuale, non priva di criticità anche a livello sociale. Il compendio Safe Web è stato costruito a partire da importanti riflessioni emerse l’indomani della realizzazione nel 2016 del 1° Corso per formatori sui temi della sicurezza in ferrovia, sulla strada e su Internet realizzato dalla Direzione centrale per le Specialità della Polizia di Stato per insegnanti dell’Ufficio scolastico regionale per il Lazio, allo scopo di condividere informazioni utili per una sempre più efficace protezione dei ragazzi da tutti i tipi di rischi, da quelli tradizionali legati alla strada, sino a quelli attuali rappresentati dal mondo virtuale. Il 49° rapporto Censis sulla situazione del Paese, già nel 2015 aveva menzionato un’esigenza espressa dai dirigenti scolastici di avere maggiori dettagli su come gestire concretamente i casi di rischio on line per gli studenti a scuola (http://www.censis.it/10?shadow_ricerca=121041). L’approvazione della legge n. 71 del 29 maggio del 2017 recante “Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo” apre inoltre la strada a un’organizzazione sistemica delle azioni preventive e repressive di fenomeni complessi, borderline con la devianza minorile, come il cyberbullismo. In accordo con quanto previsto dalla nuova legge contro il cyberbullismo, il compendio Safe Web offre una panoramica dei principali fronti di rischio attuale per i minori, così come appare all’occhio della polizia postale e delle comunicazioni, scegliendo di affrontare, nell’eterogeneo mondo di opportunità d’uso delle nuove tecnologie da parte dei giovani, quei fenomeni che possono, con maggiore probabilità, manifestarsi a scuola, tra gli studenti, sotto lo sguardo degli insegnanti. La polizia postale ha condotto sin dal 2010 percorsi progettuali cofinanziati dalla Commissione europea, frutto di importanti partenariati interistituzionali, condivisi con Ong internazionali e nazionali attive nella protezione dei minori (Save the Children, Cismai , Telefono Azzurro, ecc), con l’obiettivo di aumentare la sua capacità di lettura e di risposta ai nuovi fronti di rischio per i ragazzi on line, mantenendo alta la consapevolezza delle specifiche fragilità di bambini e adolescenti (https://www.savethechildren.it/cosa-facciamo/pubblicazioni/fuori-dalla-rete). L’impegno profuso per la tutela dei minori in Rete rappresenta per la polizia postale e delle comunicazioni un obiettivo prioritario che ha nelle sinergie interistituzionali uno dei presupposti metodologici irrinunciabili: la partecipazione della Specialità sin dagli esordi dei lavori del Safer Internet Center Italy (SIC) coordinato dal Miur, quale punto di riferimento nazionale ed europeo per le politiche di sensibilizzazione e prevenzione dei rischi di Internet per i minori, ha avviato e di fatto consolidato, attraverso un protocollo di collaborazione, una sinergia interistituzionale necessaria e positivamente strategica, con il fine condiviso di innalzare sempre di più i livelli di protezione dei minori sul Web. L’insieme di questi elementi e la crescente esigenza di rafforzare le sinergie di protezione dei minori su Internet hanno condotto a immaginare quali destinatari elettivi di questo compendio gli insegnanti, gli animatori digitali e i nuovi referenti a livello scolastico sul tema del cyberbullismo previsti dalla legge n. 71 del 2017 (art. 4 comma 3). Gli uni e gli altri sono oggi chiamati dalle specifiche della loro determinante funzione educativa, tradizionale quella degli insegnanti e più nuova quella degli animatori digitali e dei referenti per il cyberbullismo, a ricoprire un ruolo strategico nella gestione quotidiana delle complessità del rischio on line dei loro studenti, spesso così capaci da un punto di vista digitale eppure così fragili da un punto di vista emotivo. Questa breve pubblicazione nasce come uno strumento che può rendere più chiaro, anche ai genitori, quale sia il ruolo che la scuola può svolgere quotidianamente, in sinergia con altre istituzioni, in relazione a un rischio così multiforme e difficile da decifrare per un mondo adulto “immigrato digitale”. Si tratta di un compendio “aperto” poiché si compirebbe un errore nel ritenere di avere oggi tutte le risposte utili alla protezione dai rischi per i minori on line: ogni nuovo servizio di Internet, ogni nuova app, ogni supporto informatico che si afferma tra i giovani apre infinite prospettive di progresso e nuovi fronti di rischio concreto per i giovani internauti. Si tratta di un documento aperto a cui sarà possibile proporre aggiornamenti e riflessioni aggiuntive ogni qualvolta apparirà necessario, in ordine a quanto accade nel mondo della tecnologia e dei giovani. Protezione reale dai rischi virtuali L’attrazione tra giovani e nuove tecnologie è oramai inarrestabile: lo sviluppo di smartphone e tablet sempre più facili da usare ha condotto a un recente aumento esponenziale del numero dei ragazzi connessi a Internet, 24 ore su 24, ovunque si trovino. Lo sviluppo così rapido della tecnologia, la sua progressiva portabilità a buon mercato, l’impulso a essere sempre più connected e social ha condotto tutta la società civile a misurarsi con temi e problematiche di incredibile dinamismo e complessità: il cyberbullismo, l’adescamento on line sono solo alcuni esempi dei livelli di criticità che possono assumere le interazioni tra giovani e Internet. Il lavoro quotidiano di pattugliamento del Web, la gestione concreta dei casi penalmente rilevanti, l’impegno capillare nelle campagne di sensibilizzazione svolte dalla polizia postale e delle comunicazioni su tutto il territorio nazionale hanno consentito negli anni la costruzione di knowhow pratico utile, non solo alle attività di repressione, ma importante anche per le attività di prevenzione e protezione delle potenziali vittime. Con questo compendio si sintetizza quanto è stato osservato nella gestione concreta dei casi, ascoltato dalla viva voce dei 500mila giovani studenti incontrati nelle scuole durante gli incontri di sensibilizzazione della campagna informativa Una vita da social, che può essere utile a promuovere una maggior

consapevolezza di cosa si rischia on line a scuola e aiutare gli animatori digitali e gli insegnanti a orientarsi per la gestione concreta dei casi problematici e difficili. 1. Schede giuridiche 1.1 La qualifica di pubblico ufficiale attribuita agli insegnanti Agli insegnanti della scuola statale e di quella paritaria è riconosciuta, secondo quanto specificato in numerose sentenze della Cassazione penale, “la qualità di pubblico ufficiale”, in quanto essi esercitano una funzione disciplinata da norme di diritto pubblico, caratterizzata dalla manifestazione della volontà della pubblica amministrazione e dal suo svolgersi attraverso atti autoritativi e certificativi (art. 357 cp). L’insegnante di scuola è quindi un pubblico ufficiale a tutti gli effetti e l’esercizio delle sue funzioni non è circoscritto alla sola tenuta delle lezioni, ma si estende alle attività preparatorie, contestuali e successive alle lezioni stesse, potendosi estendere anche a tutte le attività che comprendano contatto e interazione con i ragazzi e le loro famiglie (es. colloqui, riunioni, assemblee, ecc). Lo svolgimento delle lezioni può quindi essere inteso come espressione della volontà educativa della pubblica amministrazione, così come l’attribuzione di voti, quale esito dell’attività valutativa dell’insegnante, diviene espressione del potere certificativo dell’insegnante che manifesta così una delle attribuzioni proprie dell’essere un pubblico ufficiale. Per quanto riguarda i collaboratori scolastici, la Corte di cassazione, ha riconosciuto loro la qualifica di incaricato di un pubblico servizio (art. 358 cp) “ in ragione dello svolgimento della funzione di vigilanza sugli alunni, oltre che di custodia e di pulizia dei locali, può dirsi collaboratore alla pubblica funzione spettante alla scuola”. Secondo quanto previsto dall’art. 347 cpp, i pubblici ufficiali e gli incaricati di un pubblico servizio che hanno notizia di un reato perseguibile di ufficio, durante lo svolgimento del loro servizio, devono farne denuncia per iscritto, anche quando non sia chiaro chi sia la persona che ha commesso il reato. Se però il pubblico ufficiale o incaricato di pubblico servizio ha notizia di un reato in situazioni differenti da quelle di servizio, l’obbligo cessa e al suo posto sorge la facoltà di denunciare propria di qualsiasi altro cittadino. La notizia di reato potrebbe essere acquisita anche in modo indiretto, cioè derivata da dichiarazioni di altri soggetti o da documenti, immagini, video o altri tipi di testimonianze indirette. Ciò che conta è la conoscenza di un fatto accaduto che, secondo una valutazione approssimativa, abbia o possa aver determinato la commissione di un reato. L’insegnante, pur in qualità di pubblico ufficiale, non è tenuto a valutare l’effettiva illegalità di una condotta né è necessario che verifichi la veridicità di quanto gli è stato riferito. La definizione di questi elementi importanti verrà demandata in via esclusiva all’autorità giudiziaria che assumerà il controllo delle attività investigative necessarie, qualora lo ritenesse utile. I reati che vengono definiti perseguibili d’ufficio sono quei reati che, per il loro carattere di estrema gravità e offensività, vengono considerati perseguibili a prescindere dalla volontà di denunciarli da parte delle persone offese. L’obbligo di denuncia di reato è previsto nel caso in cui un minore sia vittima, ma anche qualora sia autore di reato. L’omissione o il ritardo della denuncia potrebbe configurare il reato di cui all’art. 361 del codice penale “omessa denuncia di reato da parte del pubblico ufficiale”. Il dirigente dell’Istituto scolastico statale o paritario, è tenuto senza indugio a denunciare all’autorità giudiziaria competente i reati procedibili d’ufficio commessi dagli studenti o a danno di questi di cui egli sia venuto a conoscenza in ragione del ruolo ricoperto all’interno della comunità scolastica. Il dirigente scolastico potrà essere informato in forma scritta dall’insegnante che è venuto a conoscenza di fatti rilevanti e provvederà a effettuare una denuncia in forma scritta, anche nell’ipotesi in cui sia diretta contro ignoti. Nella denuncia potranno essere esposti i fatti in maniera chiara e completa, senza necessità di effettuare valutazioni sull’attendibilità del fatto. Pur non essendo previsto un termine per l’inoltro della denuncia, la stessa dovrebbe essere effettuata il prima possibile, per non pregiudicare l’accertamento del fatto da parte della competente autorità giudiziaria. La tempestività con cui vengono riferiti fatti penalmente rilevanti o presunti tali che riguardano l’uso delle nuove tecnologie è elemento determinante in ordine alla specifica volatilità della prova informatica. I tempi di conservazione dei dati possono essere molto diversi a seconda del servizio di Internet che si considera. Le norme di riferimento circa l’obbligo e le modalità di formalizzazione della denuncia sono contenute nel codice di procedura penale agli artt. 331 e 332. La denuncia potrà essere indirizzata alla procura della Repubblica competente, e quindi nel dettaglio: alla procura della Repubblica presso il tribunale del luogo dove è avvenuto il reato, se indiziato del reato è un maggiorenne; alla procura della Repubblica per i minorenni se indiziato è un minore; a un ufficiale di polizia giudiziaria (carabinieri, polizia, guardia di finanza, vigili urbani, ecc.) La denuncia può essere inoltrata anche nell’ipotesi in cui il presunto autore del reato sia minore di anni 14, anche se non è formalmente imputabile poiché spetta al tribunale dei minori la competenza di valutare gli interventi eventuali e necessari. Esiste una possibilità, come testimoniato da diverse pronunce della Corte di cassazione, che sussista il rischio per la scuola di incorrere nella responsabilità della culpa in vigilando per un fatto illecito commesso dagli studenti, qualora la scuola stessa non sia in grado di dimostrare di aver adottato tutte le misure atte a scongiurare e prevenire episodi di violenza sulle persone e sulle cose. Di seguito a titolo esemplificativo si espongono alcuni esempi di reati virtuali procedibili d’ufficio la cui gravità, anche solo potenziale, richiede maggiore attenzione. Si tratta di reati gravi o che assumono carattere di particolare gravità soprattutto quando commessi in danno di minori di 14 anni: adescamento di minori anche in Rete (art. 609 undecies cp), prostituzione minorile anche in Rete (art. 600 bis cp), pornografia minorile (art. 600 ter cp), detenzione di materiale pedopornografico (art. 600 quater cp), violenza sessuale in danno di minori di 14 anni (art. 609 bis cp), violenza privata (art. 610 cp), sostituzione di persona (art. 494 cp). Vi sono poi alcuni reati invece che necessitano di una formale querela da parte della parte offesa perché si avvii un procedimento penale teso a individuare i responsabili di azioni illegali dannose. In tutti i casi assimilabili a quelli di seguito descritti, il supporto dell’insegnante potrà essere determinante perché le vittime chiedano il necessario aiuto e trovino il coraggio di sporgere denuncia, quando necessario. Fra i reati on line ricordiamo quelli che più frequentemente possono essere commessi dai ragazzi in danno di coetanei, utilizzando le nuove tecnologie: le diffamazioni (art. 595 cp), le molestie, lo stalking (fatte salve alcune eccezioni) anche quando messi in atto attraverso Internet con profili falsi e/o travisati, l’accesso abusivo a sistema informatico (art. 615 ter cp), le violazioni della privacy e dei diritti di immagine dei minori. 1.2 TRACCIABILITà E REATI ON LINE La navigazione in Internet avviene attraverso l’utilizzo di servizi, primo fra tutti la connessione alla Rete, generalmente forniti dai provider attraverso un’utenza telefonica analogica, digitale, o su fibra, satellite, radio, ecc. La connessione alla Rete presuppone in genere un processo di autenticazione che permette al fornitore del servizio (provider) di “riconoscere” l’utente che ne fruisce, assegnandogli un indirizzo telematico (ip address) che identificherà la macchina connessa alla Rete in un determinato intervallo temporale e garantirà il corretto scambio di dati tra il computer/smartphone e i vari server che saranno interessati durante la navigazione in Rete. La possibilità di individuare l’autore di un reato informatico è legata alla lettura delle tracce informatiche che i singoli collegamenti hanno “seminato“ sulla Rete, generalmente su server attraverso i quali sono effettuati i collegamenti stessi. Per l’intera durata della navigazione il personal computer/smartphone collegato alla Rete lascerà tracce telematiche (cosiddetti file di log) del proprio “passaggio” su ogni server interessato; queste tracce verranno registrate sotto forma di file di testo. I file di log si traducono quindi in informazioni a disposizione degli investigatori per l’eventuale individuazione delle condotte tenute in Rete e per l’identificazione dei soggetti autori delle stesse. L’analisi del log può consentire di stabilire se un determinato utente si sia collegato alla Rete nel giorno e ora di interesse, da quale nodo vi sia

entrato, quale provider abbia fornito l’accesso in Rete, e in taluni casi quale attività sia stata svolta. Le tracce telematiche sono soggette a elevato tasso di volatilità, la loro conservazione inoltre è disciplinata da specifiche leggi che definiscono gli intervalli di tempo in cui vige l’obbligo per i provider di conservare i dati telematici e telefonici. Al di fuori di tali intervalli di tempo sarà difficile e talora impossibile ricostruire eventuali responsabilità penali. Gli intervalli di tempo entro i quali i provider devono rendere accessibili alle forze dell’ordine dati telematici relativi ai loro servizi sono diversi a seconda del tipo di dato informatico: per esempio i gestori di telefonia hanno obbligo di conservare i dati relativi alle chiamate effettuate per circa 30 giorni, questo comporterà che, qualora sia necessario ricostruire da chi provengono chiamate mute e anonime che disturbano un utente, potrebbe essere possibile avere questo dato solo entro i 30 giorni successivi alle chiamate stesse. Per l’identificazione dei reali utilizzatori di profili social, profili utenti, utilizzatori di servizi di messaggistica dai quali provengono insulti, denigrazioni, minacce ai danni di altri utenti è necessario richiedere i dati entro e non oltre i 12/24 mesi successivi agli eventi presunti illegali. Per questi motivi è indispensabile che le segnalazioni/denunce siano sporte con la massima tempestività in modo da garantire che l’autorità giudiziaria, che dispone l’acquisizione delle tracce telematiche e la polizia, che effettua gli accertamenti tecnici, possano agire prima che i dati non siano più disponibili. 1.3 L’IMPUTABILITà DEI MINORI SU INTERNET L’art. 85 del cp detta il principio generale per il quale nessuno può essere punito per un fatto previsto dalla legge come reato se al momento in cui lo ha commesso non era imputabile. È imputabile la persona che sia capace di intendere e di volere al momento dei fatti oggetto di valutazione. L’ art. 97 del codice penale stabilisce che non è imputabile chi al momento in cui ha commesso un fatto reato non ha compiuto i quattordici anni. Il legislatore ha dunque stabilito che i minori di 14 anni non siano da considerarsi penalmente responsabili delle loro azioni, quando queste comportino un reato. Sino a quell’età si presume che i ragazzi non abbiano raggiunto una maturità psicofisica che gli consenta di distinguere in modo sufficientemente adeguato cosa sia giusto e cosa sia sbagliato. Non è escluso tuttavia che i genitori di un minorenne autore di reato rispondano penalmente per il reato punibile commesso dal figlio. Questo significa che in tutti quei casi in cui sia chiaro o si presume che ragazzi di età inferiore ai 14 anni abbiano commesso azioni illegali, è comunque necessario effettuare una denuncia/segnalazione poiché la determinazione dei fatti, l’applicazione di misure di sicurezza, l’attribuzione di responsabilità penali ai genitori sono in capo alle necessarie valutazioni dell’autorità giudiziaria. La denuncia di fatti che possano costituire reato può essere fatta sempre in forma scritta e non è previsto l’obbligo di convocazione o avviso alla famiglia perché la denuncia è sottoposta all’obbligo di segreto istruttorio afferente alla fase delle indagini preliminari. Fatta salva tale indicazione, sarà auspicabile coinvolgere la famiglia informandola in breve di quanto accaduto, quale presupposto della migliore sinergia tra adulti, strategica per la valutazione della situazione. L’avvio di un procedimento penale in relazione ad azioni illegali compiute da un minore degli anni 14 ha un valore importante, non necessariamente in ottica punitiva, ma perchè può favorire una necessaria valutazione delle criticità insite al percorso di crescita di quel minore. Esiste inoltre una possibilità per la quale, qualora il minorenne commetta azioni particolarmente gravi e per queste sia giudicato pericoloso, possa essere sottoposto, nonostante abbia un’età inferiore ai 14 anni, a misure di sicurezza quali il collocamento in una comunità per minori o la libertà controllata. Nel caso dei minori di età compresa tra i 14 e i 18 anni, l’imputabilità va giudicata caso per caso, secondo quanto previsto dall’art. 98 del codice penale. Il giudice dovrà dunque appurare la concreta capacità di intendere e di volere del minore degli anni 18 al momento in cui ha commesso il fatto. In caso di mancanza di tale capacità il minore non è punibile. Nel diverso caso in cui il minore degli anni 18 sia capace di intendere e di volere al momento della commissione del fatto viene considerato punibile, ma la sua pena sarà diminuita rispetto a quella prevista dalla legge per gli adulti. Anche per azioni commesse da minorenni nella fascia di età 14-17 anni, il coinvolgimento dei genitori non deve essere necessariamente antecedente alla formalizzazione di una denuncia/segnalazione ma sarà comunque auspicabile in un’ottica di collaborazione tra care-givers. È importante ricordare che esistono vari tipi di reati che possono essere commessi in Rete: alcuni di essi si compiono attraverso semplici azioni compiute direttamente on line (es. aprire un profilo Facebook a nome di altri, rubare e diffondere senza autorizzazione sui social immagini altrui, ecc.), altri invece prevedono l’uso del mezzo informatico quale semplice veicolo o oggetto dell’azione illegale (pubblicare su Facebook insulti, falsità, indiscrezioni sul conto di qualcuno). Molto ... ...

08/01/2018