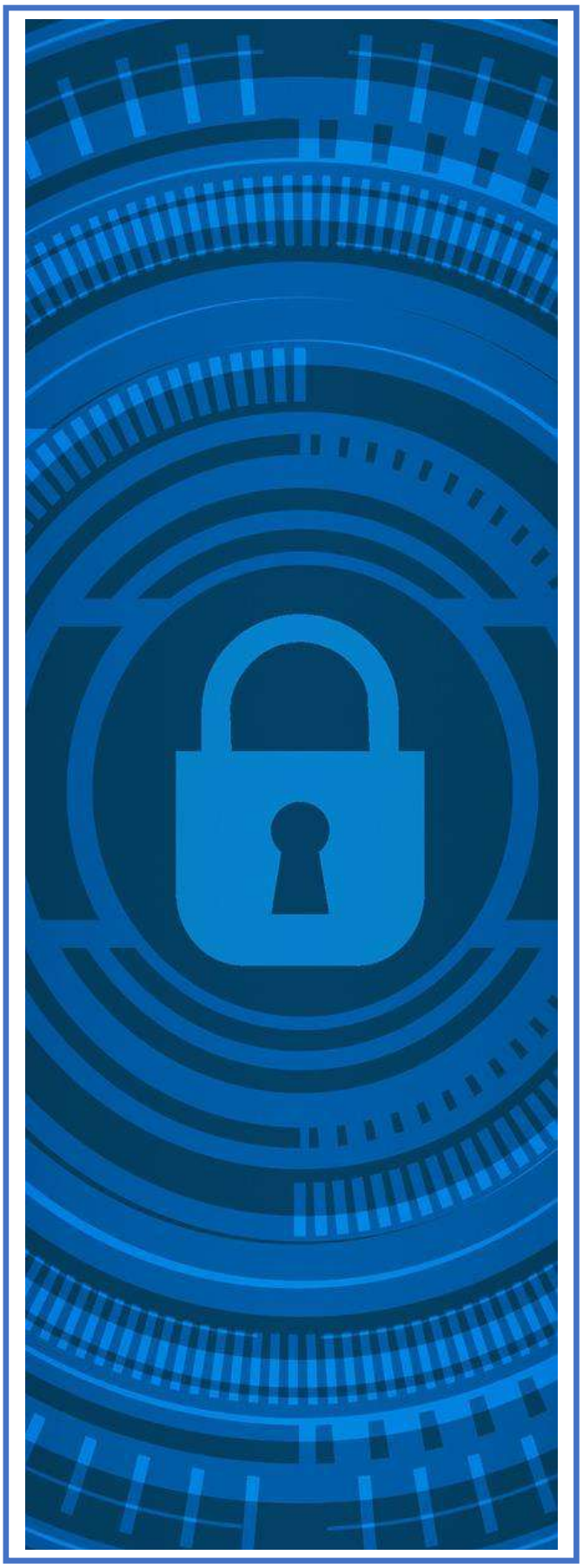
IL RUOLO DI INTERNET NELL'ERA DIGITALE: BENEFICI, RISCHI E SICUREZZA DEL MONDO ONLINE

EUROPE DIRECT LIVORNO

COMUNE DI LIVORNO

europe direct Livorno

Co-funded by the European Union



Il ruolo di Internet nell'era digitale: benefici, rischi e sicurezza del mondo online

europe direct Livorno

Testi a cura di:
Greta Pachetti

La pubblicazione è frutto del lavoro di ricerca realizzato dal team dei Tirocinanti del Centro di Informazione Europe Direct del Comune di Livorno: Greta Pachetti, Jessica Greco e Nadir Attou.

Il volume è stato realizzato grazie al contributo della Commissione Europea, rappresentando un obiettivo raggiunto del piano di comunicazione Europe Direct Livorno 2020.

L'immagine di copertina e tutte le altre immagini sono state ottenute da www.pixabay.com.

Si ringraziano Sabina Borgogni, Katia Le Rose, Alberto Alessandro Maria Savio e Alessandro Gronchi.

Con il co-finanziamento della Commissione Europea.

europe direct Livorno

Co-funded by the European Union

INDICE

PREFAZIONE

Anche quest'anno ho il piacere di introdurre la lettura di questa nuova pubblicazione realizzata dal Centro Europe Direct, coordinato dall'Ufficio Finanziamenti Comunitari, Sviluppo economico ed EDIC del Comune di Livorno, nell'ambito delle attività approvate dalla Commissione Europea per il periodo 1° gennaio 2020 – 30 aprile 2021.

Sulla base della Convenzione triennale vigente, sottoscritta tra l'Amministrazione Comunale e la Commissione Europea, il Centro Europe Direct di Livorno è impegnato nella diffusione di informazioni, attraverso il suo sportello informativo, la gestione dei social, l'organizzazione di eventi e la realizzazione di pubblicazioni, rispetto alle principali tematiche europee, oggi più che mai attuali, con lo scopo di rendere la cittadinanza consapevole delle politiche e delle opportunità europee, e di attivare percorsi di discussione e partecipazione sulle grandi sfide del futuro.

Convinto dell'importanza di continuare a far parte della Rete Europe Direct, ho approvato la recente candidatura del Comune di Livorno sul bando che la Commissione Europea ha pubblicato lo scorso autunno ai fini della selezione dei partner della nuova generazione dei centri Europe Direct, per il periodo 1° maggio 2021 - 31 dicembre 2025, candidatura che auspico possa essere approvata.

Ritengo che i contenuti di questo testo possano contribuire ad una migliore comprensione dei temi legati all'uso consapevole di internet, delle opportunità che la rete offre e dei suoi rischi, e per questo ringrazio il team dei giovani tirocinanti del nostro Centro che si sono impegnati nella realizzazione di questa pubblicazione.

Gianfranco Simoncini
Assessore allo Sviluppo Economico
e Fondi Unione Europea

INTRODUZIONE

L'era digitale, o era delle tecnologie dell'informazione, è caratterizzata dall'uso diffuso di computer e delle tecnologie digitali. L'utilizzo generalizzato di internet può apportare, senza ombra di dubbio, benefici significativi e visibili nella vita quotidiana di ogni individuo, tuttavia, nonostante i suoi molteplici vantaggi, l'era digitale pone anche difficili sfide per quanto riguarda la sicurezza degli utenti che navigano quotidianamente nel *world wide web*, soprattutto i più piccoli. Proprio per questo, le istituzioni dell'Unione Europea hanno sviluppato un quadro normativo specifico per la tutela degli individui ed hanno dato vita ad innumerevoli iniziative per la protezione dei propri cittadini, con un'accortezza maggiore per quanto riguarda bambini e adolescenti.

La presente pubblicazione si occupa proprio di queste tematiche attuali del mondo odierno, portando alla luce gli aspetti positivi dell'utilizzo massivo di Internet ed evidenziando altresì le ombre e le difficoltà ad esso collegate. Un occhio particolare è puntato sui più piccoli, verso i quali è necessaria una maggiore attenzione per la costruzione di una rete online più sicura in cui possono navigare e viaggiare serenamente. In quest'ottica sono analizzate problematiche significative come il bullismo e soprattutto lo sviluppo della sua versione più recente, alimentata dalla diffusione sempre maggiore di strumenti digitali alla portata di tutti, ossia il cyberbullismo.

Il tema della sicurezza è analizzato e sviluppato anche in un'ottica più ampia e onnicomprensiva, perciò si parlerà di cybersecurity, esaminando lo sviluppo del quadro normativo europeo in tale ambito, il contesto italiano ed il ruolo di primaria importanza assunto dalla polizia postale.

Con questa pubblicazione, il Centro EDIC Livorno si augura di poter offrire ulteriori spunti di riflessioni sul tema più che mai attuale del ruolo di Internet nell'odierna età digitale, con l'obiettivo comune finale di poter offrire un mondo online più sicuro per tutti i suoi utenti.

CAPITOLO I

INTERNET: LUCI ED OMBRE DELLA REALTÀ ONLINE

1. Internet: potenzialità ed utilizzo

Internet è una rete di telecomunicazioni ad accesso pubblico che connette vari dispositivi o terminali in tutto il mondo, e che fin dalla sua nascita ha rappresentato uno dei maggiori mezzi di comunicazione di massa, grazie all'offerta di una vasta serie di contenuti potenzialmente informativi e di servizi. L'origine di internet risale agli anni Sessanta, quando gli Stati Uniti d'America misero a punto un nuovo sistema di difesa e di controspionaggio durante la guerra fredda. Tuttavia, prima di trasformarsi in una realtà pubblica occorre attendere i primi anni Novanta, quando il fenomeno comincia ad espandersi su scala globale.

Oggigiorno Internet è uno strumento radicalmente diffuso in tutto il mondo e rappresenta la principale fonte di informazione per gli utenti di ogni latitudine. È utile sottolineare come l'impiego di tale strumento subisca alcune variazioni a seconda delle fasce d'età a cui facciamo riferimento. In particolare, fino ai 45 anni esso rappresenta la maggior fonte di informazione, ma è al contempo utilizzato come strumento di comunicazione e di intrattenimento. Gli utenti tra i 46 ed i 65 anni, invece, lo utilizzano per la maggioranza come fonte di informazione ma molto meno come forma di intrattenimento. Infine, per quanto riguarda le fasce d'età più avanzata, l'informazione è recepita in gran parte attraverso i media tradizionali come la televisione, i giornali o le radio[1]. In altri termini, tutti gli utenti utilizzano Internet come strumento di ricerca di informazioni, ovviamente in modalità e frequenze diverse, ma la maggiore differenza è riscontrabile nelle funzioni di intrattenimento, socializzazione e comunicazione, sfruttate spesso soltanto dalle fasce più giovani della popolazione.

Con l'avvento del nuovo millennio e delle tecnologie più innovative, Internet è ormai entrato a far parte della vita quotidiana di gran parte della popolazione mondiale, rivoluzionando radicalmente il modo di vivere delle persone, permeando ogni aspetto della vita quotidiana, da quelli più salienti a quelli più marginali. Innegabilmente, ha modificato il concetto stesso di divertimento, di svago e di intrattenimento, mettendo a disposizione degli utenti una gamma infinita di giochi, di canali musicali,

[1] Swedes and the internet 2014, *An annual study of the Swedish people's internet habits*, testo disponibile su https://web.archive.org/web/20170709190022/http://en.soi2014.se/information-and-facts/internet-is-the-most-important-source-of-information/.

radiofonici e televisivi. Specie con la creazione delle piattaforme streaming, fruibili attraverso qualsiasi dispositivo elettronico, gli iscritti hanno la possibilità di accedere ad infiniti contenuti, a qualsiasi ora ed in qualsiasi luogo. Per quanto possa risultare scontata questa considerazione, ciò ha definitivamente alterato e rivoluzionato la concezione di tempo libero. Che sia occasionale o assidua, la presenza di un numero sempre maggiore di individui su queste piattaforme è innegabile. I dati sullo streaming televisivo in Italia, infatti, non lasciano spazio a interpretazioni: il modo in cui gli italiani guardano la televisione è notevolmente cambiato e, al contrario di quanto si possa pensare, non è un cambiamento che riguarda soltanto i più giovani. Le ultime statistiche evidenziano che nove italiani su dieci guardano film, serie TV e programmi televisivi online. Più nel dettaglio, oltre la metà dei 18-34enni guarda ogni giorno contenuti televisivi online e quasi un over 55 su due dice di approfittare delle opportunità che vengono dalla TV on demand più volte durante la stessa settimana[2].

Gli strumenti digitali sono diventati parte integrante della quotidianità odierna, perciò è necessario prenderne atto. Dunque, per inquadrare meglio la portata di questo fenomeno è utile sottolineare che oggigiorno più di 4,54 miliardi di persone utilizzano Internet, con circa 3,80 miliardi di utenti presenti sui social media. Quasi il 60% della popolazione mondiale è già online e le ultime tendenze suggeriscono un ulteriore incremento futuro. A livello globale, più di 5,19 miliardi di persone utilizzano i telefoni cellulari e si stima che l'utente medio di Internet trascorra in media 6 ore e 43 minuti online ogni giorno[3].

Le statistiche riguardanti l'Italia mostrano dati in linea con la media mondiale. Infatti, più della metà della popolazione è attiva sui social, con circa 35 milioni di utenti. In riferimento alla frequenza giornaliera, si parla di circa 2 ore al giorno trascorse sui social media e di circa 3 ore utilizzate per la fruizione di TV e Video streaming, per un complessivo di circa 6 ore giornaliere trascorse su Internet[4].

Come sottolineato in precedenza, la comparsa di Internet ed il suo sempre più frequente utilizzo ha mutato molti aspetti della vita delle persone. Tra questi, uno che è irreversibilmente cambiato è sicuramente la comunicazione. Sia per quanto riguarda la condivisione online degli aspetti più intimi della propria vita privata, sia per quanto riguarda la comunicazione diretta tra gli utenti. Grazie alle applicazioni gratuite di messaggistica istantanea, le persone sono ora in grado di comunicare molto più rapidamente di quanto non potessero fare in precedenza.

La necessità di restare perennemente connessi, tuttavia, può avere talvolta risvolti patologici, tanto da arrivare a parlare di «nomofobia», ossia la paura incontrollata di rimanere disconnessi[5]. Tale fobia,

[2] V. Dara, Il successo dello streaming televisivo in Italia sta cambiando anche il modo di fare, oltre che di vedere, la TV?h, Inside Marketing full information, ttps://www.insidemarketing.it/streaming-televisivo-in-italia-dati-2019/.
[3] S. KEMP, Digital 2020 global digital overview, *We Are Social Inc.,* 30 JANUARY 2020, https://wearesocial.com/digital-2020.
[4] S. KEMP, Digital 2020 global digital overview, *We Are Social Inc*., 30 JANUARY 2020, https://wearesocial.com/digital-2020.
[5] Parlamento Europeo, Interrogazione con richiesta di risposta scritta E-006280-15 alla Commissione, 20 aprile 2015, consultabile su https://www.europarl.europa.eu/doceo/document/E-8-2015-006280_IT.html.

il cui nome deriva dal termine «*nomophobia*[6]», indica appunto il terrore di rimanere privi di una connessione, di trovarsi isolati dal mondo esterno. Il termine è ancora poco diffuso, ma il problema che indica è sempre più frequente e rappresenta un fenomeno preoccupante, sia in Italia che nella maggior parte dei Paesi industrializzati. Questo fenomeno affonda deducibilmente le sue radici nella storia attuale, la quale vede ormai da una decina di anni la diffusione massiva di *smartphone*, dispositivi mobili e *social network* in tutto il mondo. Tale paura può causare stati di ansia, malessere, irrequietezza e aggressività fino a generare una vera e propria dipendenza patologica. Secondo David Greenfield, professore di psichiatria all'università del Connecticut, l'attaccamento allo *smartphone* ha un funzionamento molto simile a quello di tutte le altre dipendenze. In breve, esso causa delle interferenze nella produzione della dopamina, il neurotrasmettitore che regola il circuito celebrale della ricompensa e che incoraggia le persone a svolgere attività che credono gli daranno piacere. Così, ogni volta che appare una notifica sul telefono cellulare, il livello di dopamina sale perché l'individuo crede di essere in procinto di vivere qualcosa di nuovo ed interessante. Tuttavia, non si può avere la certezza che ciò accadrà ogniqualvolta il telefono squilla, dunque, da ciò si crea l'impulso di controllare in continuazione lo schermo proprio dispositivo, innescando lo stesso meccanismo che si attiva in un giocatore di azzardo[7]. Diversi segnali marcano il confine tra un uso controllato e consapevole ed uno incontrollato della rete della telefonia mobile, sintomo di una vera dipendenza, tra cui il vivere stati di ansia e di nervosismo al solo pensiero di perdere il proprio cellulare. Secondo un'indagine svolta nel 2017 dall'Osservatorio nazionale per l'infanzia e l'adolescenza, la situazione risulta ancora più allarmante per quanto riguarda le fasce più giovani della popolazione. Infatti, si stima che 8 adolescenti su 10 soffrano di questa paura, e il 50% di questi afferma di provare ansia e malessere al solo pensiero che ciò possa accadere. L'uso e l'abuso di *internet* e dei *social media* da parte dei minori, quindi, risulta sempre più ossessivo e dipendente[8].

Riassumendo, smartphone e tablet hanno ampliato le coordinate spazio-temporali dell'uso di Internet, fornendo un accesso "*anywhere, anytime*[9]", con implicazioni sul piano delle nozioni di prossimità e distanza, delle norme sociali che regolano la privacy, la libertà e la sorveglianza interpersonale, ma anche sulla stessa esperienza online dei ragazzi. Le attività online, tuttavia, non sono né necessariamente positive né intrinsecamente rischiose, molto dipende dall'atteggiamento che i ragazzi hanno nei confronti della comunicazione online[10]. Ecco perché nella società odierna, perennemente connessa ed irreversibilmente interconnessa, preme sempre di più una sensibilizzazione globale per un utilizzo consapevole di Internet, con l'obiettivo finale di godere dei benefici che la rete può offrire e di prevenirne il più possibile i rischi.

[6] Nomo è l'acronimo di *no-mobile*, da cui deriva la costruzione della parola nomo-fobia, cioè paura di non avere il telefono.
[7] Greenfield D.N., Davis R.A., Lost in cyberspace: the web @ work. Cyberpsychol Behav., 2002.
[8] Camera dei Deputati, Proposta di legge n.1840, *Disposizioni per la prevenzione e la cura della nomofobia*, Presentata il 9 maggio 2019, testo integrale consultabile sul sito ufficiale della Camera dei Deputati https://www.camera.it/leg18/995?sezione=documenti&tipoDoc=lavori_testo_pdl&idLegislatura=18&codice=leg.18.pdl.camera.1840.18PDL0067960&back_to=https://www.camera.it/leg18/126?tab=2-e-leg=18-e-idDocumento=1840-e-sede=-e-tipo=.
[9] Mascheroni, G. & Ólafsson, K. (2014*) Net Children Go Mobile: Risks and opportunities* (2nd edn). Milano: Educatt, p.10.
[10] Mascheroni, G. & Ólafsson, K. (2014*) Net Children Go Mobile: Risks and opportunities* (2nd edn). Milano: Educatt, p.16.

2. Safety internet day

Con l'obiettivo di promuovere un utilizzo sempre più sicuro di Internet, l'Unione Europea ha istituito nel 2004 una giornata internazionale di sensibilizzazione per i rischi legati all'uso di tale strumento. Celebrato ogni anno a febbraio, questo evento internazionale promuove un utilizzo responsabile e consapevole della tecnologia online e dei telefoni cellulari da parte, soprattutto, di bambini e giovani di ogni nazionalità. Nato come iniziativa del progetto *EU SafeBorders*, ripreso dalla rete *Insafe*, il *Safer Internet Day* (SID) è cresciuto oltre la zona geografica tradizionale espandendosi in più di 140 paesi di tutto il mondo, raggiungendo così milioni di persone di ogni età.

Dal cyberbullismo alla rete sociale in generale, ogni anno il SID mira ad affrontare le tematiche più attuali e le problematiche ad esse correlate che influenzano gli utenti online, specialmente quelli più giovani. Internet è uno strumento potente, ricco di enormi opportunità di apprendimento, miglioramento delle proprie capacità e acquisizione di nuove abilità e conoscenze. Tuttavia, legati all'opportunità esistono anche enormi rischi ed è opportuno sviluppare nell'utente medio una piena consapevolezza di questa correlazione. Per questo il SID ha l'obiettivo non solo di promuovere la consapevolezza degli utenti, ma anche di sviluppare azioni concrete per creare una realtà online più sicura per tutti, offrendo a bambini, giovani studenti, insegnanti, genitori, responsabili politici, manager di azienda e chiunque altro di intervenire nella co-creazione di un Internet migliore.

Il mondo digitale non è soggetto a confini e ciò rende necessario l'unione e la collaborazione tra gli individui, con il fine ultimo di poter assicurare una migliore esperienza digitale per tutti. In quest'ottica, la celebrazione del *Safer Internet Day* del 2020 riprende il tema dell'anno precedente, ossia "*Insieme per un Internet migliore*", con lo scopo di sottolineare come tutti possano e debbano giocare un ruolo nella creazione di un siffatto mondo virtuale. Anche gli slogan degli anni precedenti restavano fedeli a questa missione, ad esempio, quello del 2018 era "*Crea, connettiti e condividi il rispetto: un'Internet migliore inizia con te*", nato sulla scia di quello dell'anno 2017, ossia "*Sii il cambiamento: uniti per un internet migliore*". Anche i SID precedenti riprendono questa visione, sottolineando l'importanza della collaborazione e dell'unità ed incoraggiando ognuno a fare la propria parte e ad assumersi le responsabilità nelle proprie mani[11]. Un obiettivo comune, dunque, per cui è necessaria una piena partecipazione da parte di tutti gli utenti, attraverso impegno ed azioni concrete.

3. Better internet for kids

Internet non è stato originariamente concepito come prodotto per bambini, tuttavia, oggi il 75% di essi ne fa uso, di cui un terzo attraverso la telefonia mobile. Per questo, i giovani hanno bisogno di un ambiente sicuro e stimolante mentre trascorrono il loro tempo online ed utilizzano le nuove tecnologie, obiettivo che la Commissione Europea vuole raggiungere attraverso l'elaborazione di un

[11] European Commission, Policies, *Safer Internet Day (SID)*, consultabile su https://ec.europa.eu/digital-single-market/en/safer-internet-day-sid.

piano, ossia la cosiddetta St*rategia per un Internet migliore per i bambini*[12], destinato a fornire ai bambini le competenze e gli strumenti necessari per beneficiare pienamente ed in modo sicuro del mondo digitale. La nuova strategia consiste nello sviluppo di un mercato dei contenuti online interattivi, creativi ed educativi, in collaborazione fra la Commissione europea e gli Stati membri, gli operatori di telefonia mobile, i fabbricanti di telefoni cellulari e i prestatori di servizi di socializzazione in rete.

Nonostante i buoni propositi, l'esistenza di approcci nazionali diversi fa sì che i bambini di varie parti dell'Unione Europea godano di livelli diversi di emancipazione e protezione online, situazione che crea difficoltà anche per le imprese che desiderano commercializzare in tutta l'Unione servizi e prodotti adatti all'infanzia. Per superare questi ostacoli, la Commissione ha delineato una serie di misure che saranno attuate con modalità diverse e che dovrebbero portare a soluzioni flessibili e rapide in questo campo. In sintesi, le azioni si articolano intorno a quattro obiettivi principali. Il primo è quello di stimolare la produzione di contenuti online creativi ed educativi per i bambini e sviluppare piattaforme per l'accesso a contenuti appropriati in funzione dell'età. Il secondo è l'incremento delle azioni di sensibilizzazione e formazione sulla sicurezza online in tutte le scuole dell'Unione Europea, per sviluppare la dimestichezza e la responsabilità online dei bambini nei confronti del mondo digitale e mediatico. Il terzo, invece, mira a creare un ambiente sicuro per i bambini in cui i genitori e i bambini stessi dispongano degli strumenti necessari per garantire la loro protezione online, quali meccanismi di facile impiego per denunciare i contenuti e i comportamenti nocivi online, impostazioni predefinite di privacy in funzione dell'età e controlli parentali facili da usare. Il quarto, infine, si impegna a lottare contro i materiali relativi ad abusi sessuali di bambini online promuovendo la ricerca su soluzioni tecniche innovative e il loro impiego nelle indagini svolte dalle forze dell'ordine[13].

[12] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions , European Strategy for a Better Internet for Children, Bruxelles, 2 maggio 2012, consultabile su https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2012%3A0196%3AFIN.

[13] Commissione Europea, L'angolo della stampa, Comunicato stampa, *Agenda digitale: una nuova strategia per internet più sicura e migliori contenuti internet per bambini e adolescenti*, 2 maggio 2012, gratuitamente consultabile su https://ec.europa.eu/commission/presscorner/detail/it/IP_12_445.

Nell'era odierna, un utente di Internet su tre è un bambino. Questa è una realtà che non può e non deve essere in alcun modo ignorata, poiché evidenzia come sia ormai radicalmente mutata l'esperienza di crescita dei bambini e degli adolescenti. Questi ultimi trascorrono sempre più tempo connessi, giocando online, navigando su Internet o comunicando attraverso i social media. Nuove tecnologie come l'intelligenza artificiale o la realtà virtuale hanno determinato un cambiamento importante nel modo in cui i bambini partecipano ed interagiscono con la società in generale. Come sottolineato precedentemente, Internet offre infinite opportunità di apprendimento, comunicazione, creatività ed intrattenimento che non è giusto demonizzare a priori, anzi, al contrario è utile sfruttare. Tuttavia, porta con sé anche numerosi rischi, innegabili e non ignorabili, soprattutto per gli utenti più vulnerabili come i bambini. Essi, infatti, possono essere esposti a contenuti e/o comportamenti dannosi come il cyberbullismo, le molestie sessuali, la pornografia, la violenza o l'autolesionismo. Proprio per questo sono necessarie risposte congiunte ed efficaci, proprio per prevenire conseguenze negative che rischino di ripercuotersi sul loro sviluppo cognitivo, sociale ed emotivo[14].

Questo è l'obiettivo finale della *Strategia Europea per un Internet migliore per i bambini* sviluppata dalle istituzioni dell'Unione Europea, in concomitanza con gli Stati membri, nel cui programma si prevede anche il finanziamento ed il supporto, sia a livello europeo che a livello nazionale, per la creazione di poli di riferimento nazionali sul tema, i cosiddetti *Safer Internet Cente*r (SIC), cioè centri nazionali per la sicurezza in rete. Il loro compito principale è quello di accrescere la consapevolezza e di promuovere l'alfabetizzazione digitale tra minori, genitori ed insegnanti; impegnandosi, inoltre, nella lotta contro il materiale pedopornografico online e le varie insidie che il *world wide web* nasconde. Come canale di comunicazione e punto di ingresso unico per le risorse e la condivisione di pratiche migliori in tutta Europa è stato creato anche il portale Better Internet for Kids.

Insafe[15] e *INHOPE*[16] lavorano congiuntamente attraverso una rete di Centri di sicurezza esistenti in tutta Europa, i quali comprendono generalmente un centro di sensibilizzazione, una linea di assistenza, una linea diretta ed un gruppo di giovani. In linea di massima, i centri di sensibilizzazione

[14] European Commission, Shaping Europe's digital future, Policies, *Creating a Better Internet for Kids*, disponibile su https://ec.europa.eu/digital-single-market/en/content/creating-better-internet-kids-0.

[15] Network europeo composto da Safer Internet Centres (SICs – Centri nazionali per la sicurezza in rete) che ha tra gli obiettivi quelli di offrire a bambini/e ragazzi/e strumenti utili per promuovere l'utilizzo sicuro e responsabile di internet e delle tecnologie digitali., Ministrero dell'Istruzione, co-financed by European Union, connecting Europe Facility, Generazioni connesse, Safer Internet center, Insafe, su https://www.generazioniconnesse.it/site/it/0000/00/00/insafe/.

[16] Rete di 51 hotlines di 45 Paesi in tutto il mondo. Si occupa della lotta contro i contenuti illegali online, con lo scopo di contrastare gli abusi sessuali sui minori in Internet, grazie al finanziamento e sostegno della Commissione Europea nell'ambito del Programma Safer Internet. Le Hotlines afferenti alla rete INHOPE offrono agli utenti della rete la possibilità di segnalare in forma anonima materiale internet illegale, tra cui materiale pedopornografico. Ministrero dell'Istruzione, co-financed by European Union, connecting Europe Facility, Generazioni connesse, Safer Internet center, *INHOPE*, su https://www.generazioniconnesse.it/site/it/0000/00/00/inhope/.

nazionali conducono campagne per fornire a bambini, giovani, genitori, tutori ed insegnanti le capacità, le conoscenze e le strategie per rimanere al sicuro online, sfruttando le innumerevoli opportunità offerte da Internet e dalla tecnologia mobile. Al contempo, i servizi di assistenza telefonica forniscono informazioni, consigli ed aiuto sulla gestione di contenuti o comportamenti dannosi riscontrati online. È altresì prevista la possibilità di segnalare contenuti illegali in maniera anonima che verranno immediatamente trasmessi ed analizzati dagli organismi competenti per l'azione. Infine, esistono anche dei gruppi in cui i giovani possono esprimere le proprie opinioni al riguardo e scambiare conoscenze ed esperienze sull'uso delle tecnologie online, nonché suggerimenti su come navigare in sicurezza[17].

Anche in Italia è presente un *Safer Internet Center*, coordinato dal Ministero dell'Istruzione, i cui partner principali sono le organizzazioni più rilevanti a livello nazionale come Autorità italiana per l'infanzia e l'adolescenza, Ministero dell'Interno, Ministero dei Beni Culturali, Università di Firenze, Università di Roma La Sapienza, Save the Children, SOS Telefono Azzurro, Cooperativa EDI, DIRE News Agency, Skuola.net e Giffoni Film Festival[18]. Il progetto *Safer Internet Centre – Generazioni Connesse*[19], co-finanziato dalla Commissione Europea nell'ambito del programma *Connecting Europe Facility (CEF) - Telecom*, nasce per fornire informazioni, consigli e supporto a bambini, ragazzi, genitori, docenti ed educatori che hanno esperienze, anche problematiche, legate a Internet e per agevolare la segnalazione di materiale illegale online. L'obbiettivo generale è quello di sviluppare servizi dal contenuto innovativo e di più elevata qualità, al fine di garantire ai giovani utenti la sicurezza nell'ambiente on line, considerando, al contempo, il connesso investimento come un'occasione virtuosa per una crescita sociale ed economica dell'intera collettività[20].

Il 30 settembre 2020 è stato pubblicato un bollettino ufficiale di *Better Internet for Kids* in cui vengono riaffermate le priorità di questa strategia europea, essenziali soprattutto in seguito alla situazione straordinaria creata dalla pandemia di coronavirus, dove le tecnologie sono state al centro della risposta a tale emergenza ed hanno consentito a miliardi di persone di mantenere una parvenza di normalità, continuando a restare in contatto con i propri cari, lavorando, studiando, creando ed imparando. Come prevedibile, l'altra faccia della medaglia è stato l'intensificarsi di rischi come il cyberbullismo, un'escalation di disinformazione, truffe ed illegalità online. Entrambi i risvolti, tanto quelli positivi quanto quelli negativi, correlati alla presenza online dei bambini testimoniano la grande importanza delle azioni proposte e sviluppate sotto l'egida di *Better Internet for Kids*[21].

Per completare il quadro delle iniziative e degli sforzi portati avanti dall'Unione Europea nel campo

[17] Better Internet for Kids, *INSAFE and INHOPE*, interamente e gratuitamente consultabile sul sito ufficiale di https://www.betterinternetforkids.eu/web/portal/policy/insafe-inhope.
[18] Better Internet for Kids, Italian Safer Internet Centre, About the organisation, maggio 2020, consultabile su https://www.betterinternetforkids.eu/web/italy/profile.
[19] Per ulteriori informazioni consultare il sito ufficiale https://www.generazioniconnesse.it/site/it/home-page/.
[20] Ministrero dell'Istruzione, co-financed by European Union, connecting Europe Facility, Generazioni connesse, *Il Safer Internet Centre Italia*, su https://www.generazioniconnesse.it/site/it/safer-internet-centre/.
[21] Better Internet for Kids, September 2020 BIK bulletin - *Reaffirming BIK priorities through a range of actions*, 30 settembre 2020, consultabile su https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail? articleId=6484717.

della sicurezza online, è opportuno citare anche un'iniziativa di autoregolamentazione progettata per migliorare l'ambiente online per i più piccoli, ossia la cosiddetta "*Alleanza per una migliore protezione dei minori online", o "Alliance to better protect minors online*". A seguito dell'invito della Commissione europea a prendere parte ad uno sforzo congiunto, le principali società operanti nel settore delle tecnologie dell'informazione, della comunicazione e dei media, le organizzazioni non governative e l'UNICEF[22] hanno lanciato ufficialmente l'Alleanza in occasione del *Safer Internet Day* del 2017. Il quadro dell'iniziativa è definito nella *Dichiarazione di intenti dell'Alleanza*[23], la quale concentra la propria azione su tre macroaree: i contenuti dannosi, ad esempio contenuti violenti o di sfruttamento sessuale; la condotta dannosa, di cui l'emblema è rappresentato dal cyberbullismo; ed infine il contatto dannoso, ad esempio la coercizione o l'estorsione a carattere sessuale. Lo scopo dichiarato dell'Alleanza è quello di identificare le possibili aree, all'interno delle categorie di cui sopra, che possono beneficiare di un approccio coordinato tra le parti firmatarie ed altre parti interessate in questi settori, rafforzando gli sforzi verso la realizzazione di un modello di innovazione che metta la sicurezza dei minori ed i loro diritti al centro delle attività. All'interno del documento ufficiale viene riconosciuto che il mondo in espansione di Internet e lo sviluppo della tecnologia digitale hanno il potenziale per svolgere un enorme ruolo positivo nella vita dei minori, nella comunità europea e più in generale nel mondo.

Tuttavia, il fatto che questi cambiamenti dinamici stiano avvenendo ad un ritmo incredibile presenta alle società contemporanee la sfida di individuare il modo migliore di abbracciare questo progresso, garantendo un ambiente sicuro per i minori e proteggendo i loro diritti e le loro libertà. Ecco lo scopo dell'Alleanza, di affrontare questi nuovi e reali rischi contemporanei, cercando al contempo di cogliere le opportunità offerte dalle nuove tecnologie. In occasione del *Safer Internet Day* del 2019, è stato pubblicato uno studio di valutazione dell'attuazione della Dichiarazioni di intenti dell'Alleanza[24], il quale valuta i punti di forza e di debolezza dell'Alleanza nei suoi primi diciotto mesi di vita e funzionamento, nonché la sua pertinenza, efficacia, impatto, coerenza e valore aggiunto dell'Unione Europea.

[22] UNICEFF è l'acronimo di United Nations Children's Fund, cioè il Fondo delle Nazioni Unite per l'Infanzia. Si tratta di un organo sussidiario delle Nazioni Unite, in principio è stato creato, nel 1946, con lo scopo di aiutare i bambini vittime della seconda guerra mondiale. Adesso il suo ruolo è stato ampliato e si occupa di fornire assistenza umanitaria per i bambini e le loro madri in tutto il mondo, principalmente nei paesi in via di sviluppo L'UNICEF. La sua sede centrale è a New York, ma ha sedi in 190 paesi. Per ulteriori informazioni, consultare il sito ufficiale https://www.unicef.org/.

[23] Statement of Purpose, *Alliance to Better Protect Minors Online*, Testo integrale disponibile su https://ec.europa.eu/digital-single-market/en/alliance-better-protect-minors-online.

[24] European Commission, Reports and studies, *Report on the independent evaluation of the "Alliance to better protect minors online"*, 5 febbraio 2019, consultabile su https://ec.europa.eu/digital-single-market/en/news/report- independent-evaluation-alliance-better-protect-minors-online.

4. Altre iniziative per la navigazione sicura

Ogni anno l'Unione Europea cura la campagna annuale dedicata alla promozione della sicurezza informatica tra cittadini e organizzazioni e alla fornitura di informazioni aggiornate sulla sicurezza online attraverso la sensibilizzazione e la condivisione di buone pratiche, la *cosiddetta European Cybersecurity Month* (ECSM), coordinata dall'Agenzia dell'Unione europea per la sicurezza informatica (ENISA) e dalla Commissione europea, e supportata dagli Stati membri dell'UE e da centinaia di partner europei quali governi, università, gruppi di riflessione, ONG, associazioni professionali, imprese del settore privato. Per l'intero mese di ottobre, si svolgono centinaia di attività in tutto il territorio dell'Unione, tra cui conferenze, workshop, corsi di formazione, webinar, presentazioni e altro, con l'obiettivo di promuovere la sicurezza digitale e l'igiene informatica. L'ENISA funge da *"hub"* per tutti gli Stati membri partecipanti e per le istituzioni dell'UE, fornendo suggerimenti e consigli di esperti, generando sinergie, promuovendo messaggi comuni tra cittadini, imprese e pubblica amministrazione dell'UE, e pubblicando nuovi materiali sulla tematica. Sin dagli albori nel 2012[25], il mese europeo della sicurezza informatica ha raggiunto le sue priorità chiave riunendo parti di tutta Europa sotto lo slogan *«la sicurezza informatica è una responsabilità condivisa»* per unirsi contro le minacce informatiche[26]. Proprio nel contesto del mese di ottobre, mese appunto dedicato alla cyber-security, la Commissione Europea ha lanciato, in collaborazione con Operazione Risorgimento digitale e Cisco Networking Academy, la campagna *#DigitalNinja*[27], con l'obiettivo di sensibilizzare i cittadini, soprattutto i più giovani, sui rischi della rete e per fornire loro dei consigli su come sfruttare al meglio le opportunità legate alle nuove tecnologie[28].

Un'altra iniziativa degna di nota è stata compiuta dall'ENISA, che ha lanciato un gruppo di lavoro *ad hoc* sullo *European Cybersecurity Skills Framework* con l'obiettivo di riunire un gruppo multidisciplinare di esperti per promuovere l'armonizzazione nell'ecosistema dell'istruzione, della formazione e dello sviluppo della forza lavoro in materia di cybersecurity e per sviluppare una lingua europea comune nel contesto delle competenze di cybersecurity. I membri dei gruppi di lavoro *ad hoc* saranno selezionati secondo i più alti standard di competenza, basandosi sulle capacità personali, con l'obiettivo di garantire un adeguato equilibrio in base alle specifiche questioni. Lo

[25] Ulteriori informazioni su *ECSM Through the Years*, https://cybersecuritymonth.eu/about-ecsm/ecsm- through-the-years.
[26] European Cybersecurity Month, *What is ECSM?*, https://cybersecuritymonth.eu/about-ecsm/.
[27] Commissione europea – Rappresentanza in Italia, *#DigitalNinja: piccoli accorgimenti per navigare in rete in tutta sicurezza*, video disponibile su https://www.facebook.com/watch/?v=3368101243226289. E #DigitalNinja: i crimini informatici più diffusi e come contrastarli, video disponibile su https://www.facebook.com/watch/? v=345559806673308.
[28] Commissione Europea, Rappresentanza in Italia, *#DigitalNinja: consigli e opportunità sulla cyber-security*, 12 ottobre 2020, https://ec.europa.eu/italy/news/20201012_Ue_DigitalNinja_consigli_e_opportunita_sulla_cybersicurezza_it.

scopo di questo gruppo di lavoro *ad hoc* è quello di consigliare e aiutare l'ENISA nello sviluppo di un quadro europeo delle competenze in materia di sicurezza informatica, che consenta una comprensione comune dei ruoli, delle competenze, delle abilità e delle conoscenze utilizzate da individui, datori di lavoro e fornitori di formazione negli Stati membri dell'UE. Inoltre, si impegna nella sensibilizzazione e nell'identificazione delle lacune nel panorama della sicurezza informatica che possono essere colmate con la creazione di un quadro comune europeo delle competenze in materia di sicurezza informatica[29].

Come più volte evidenziato, le istituzioni dell'Unione Europea si impegnano a creare e sviluppare contenuti indirizzati ad ogni target di cittadino, proprio perché l'utilizzo consapevole di Internet è un argomento che influisce ed attraversa trasversalmente ogni generazione di individui. In quest'ottica, ad esempio, è stato realizzato il gioco Happy Online, un kit di strumenti per costruire e sviluppare sicurezza e conoscenza sull'uso, l'uso eccessivo e l'abuso di Internet[30]. Bambini e adulti possono così riflettere e costruire insieme competenze in materia di sicurezza in Internet e migliori pratiche per l'uso e la mediazione; diventare cittadini consapevoli del digitale che valutano rischi e opportunità online e partecipare attivamente alla ricerca fornendo il proprio feedback sul toolkit *Happy Onlife*. Si tratta di un gioco da tavolo ispirato al tradizionale "*Snakes and Ladder game*", combinato con domande a quiz sull'argomento, progettati per stimolare la discussione e consentire al moderatore di guidare i giocatori verso un modo responsabile ed equilibrato di utilizzare i media digitali[31].

5. Bullismo e cyberbullismo: definizione e quadro normativo

Nei paragrafi precedenti abbiamo più volte sottolineato come le potenzialità di Internet si accompagnino ad una moltitudine di rischi a cui gli utenti, specialmente quelli più giovani, si trovano ad essere soggetti. Sicuramente, una delle difficoltà maggiori è quella di interfacciarsi, combattere ed eliminare un fenomeno che è pericolosamente in aumento, ossia il cyberbullismo.

Prima di approfondire il suddetto termine è necessario fare cenno al fenomeno nella sua accezione più generale, ossia al bullismo. Quest'ultimo non identifica una presa in giro o un atto di aggressione e/o violenza una tantum, anche se tali comportamenti possono sfociare infine in comportamenti di bullismo; esso è, piuttosto, una forma ripetitiva e prolungata di comportamento aggressivo e/o violento nei confronti di una o più persone portato avanti con il preciso scopo di danneggiare, ferire, intimidire, umiliare, escludere, isolare, discriminare o opprimere gli individui colpiti. Una vittima di bullismo può essere presa di mira per i motivi più disparati: *background* culturale, religione, *status* socioeconomico, lingua, opinione politica, aspetto fisico o abilità, corporatura, capacità intellettuali, sesso, età, orientamento sessuale, ecc. Qualsiasi sia la tematica, il comportamento di bullo ha una funzione sociale, che deriva da e/o stabilisce uno squilibrio di potere all'interno di un gruppo sociale, classe e/o comunità. Ha lo scopo di imporre una gerarchia di relazioni di potere all'interno di una società, gruppo, classe e/o comunità, dove una persona o un gruppo di persone affermano la propria

[29] European Union Agency for Cybersecurity, *Ad Hoc Working Group on the European Cybersecurity Skills Framework*, in European Cybersecurity Skills Framework, https://www.enisa.europa.eu/topics/cybersecurity- education/european-cybersecurity-skills-framework/adhoc_wg_calls.

[30] Complementare alla versione cartacea, il gioco è disponibile in olandese, francese, inglese, italiano e spagnolo come applicazione online basata su Unity 3D e funzionante nel browser Firefox su https://web.jrc.ec.europa.eu/happyonlife/. Inoltre, è disponibile la versione mobile su App Store, Google Play, Windows Phone.

[31] European Commission, *Happy Onlife - a game and toolkit to build and develop safety and knowledge on Internet use*, overuse and abuse, in EU Science Hub, Scientific tool, https://ec.europa.eu/jrc/en/scientific-tool/happy-onlife- game-raise-awareness-internet-risks-and-opportunities.

posizione di potere sugli altri membri. Il perpetuarsi di questi comportamenti getta le vittime, le quali non in grado di difendersi autonomamente, in un vortice di intimidazioni e violenza da cui non sono in grado di uscire. A lungo termine, il bullismo porta a conseguenze dannose per le sue vittime; esso lede il loro benessere emotivo e la loro autostima, nuoce alla loro salute fisica e psicologica, intaccando la loro capacità di formare relazioni significative, di apprendere ed ottenere buoni risultati a scuola o al lavoro[32].

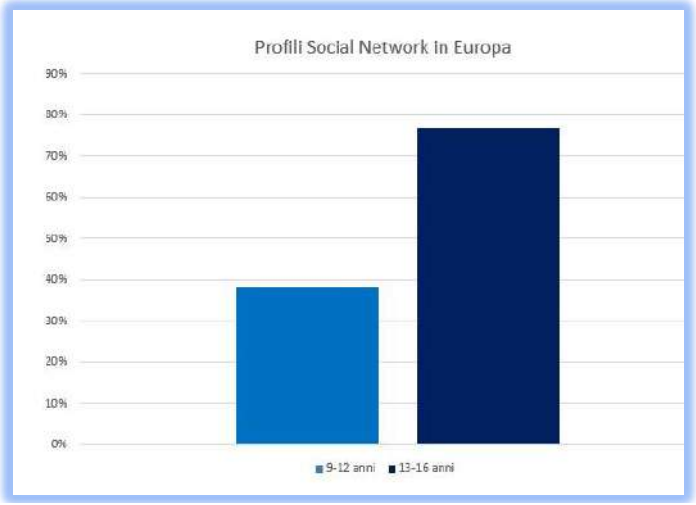
Il bullismo perpetrato attraverso le moderne tecnologie di informazioni, quali ad esempio social media, e-mail, telefoni cellulari o analoghi dispositivi, prende il nome di cyberbullismo. Tale fenomeno ha caratteristiche leggermente differenti rispetto a quello previamente analizzato, innanzitutto perché viene portato avanti attraverso degli schermi che offrono al carnefice la possibilità di celare la propria identità. Dunque, la forza dell'aggressione non risiede più nelle sue personali caratteristiche fisiche o sociali, ma soltanto nella capacità di produrre materiale e contenuti digitali che possano raggiungere potenzialmente miliardi di utenti nello stesso momento. Ecco che la condivisione di video, fotografie, disegni o chat vengono utilizzati per promuovere l'umiliazione della vittima[33].

Il termine "*cyberbullismo*" è ampiamente utilizzato, sia nell'uso colloquiale che in quello più formale. Pur essendo stato coniato per la prima volta nel 1999, tutt'ora non esiste un consenso generale su una sua definizione, sebbene le diverse versioni di solito includano l'uso della tecnologia digitale per infliggere ripetutamente danni o atti di bullismo[34]. Alcuni studiosi lo hanno definito come *«danno volontario e ripetuto inflitto attraverso l'uso di computer, telefoni cellulari o altri dispositivi elettronici»*, altri invece come *«l'uso di tecnologie di comunicazione elettronica per intimidire gli altri»*. L'uso di diverse definizioni operative ha inevitabilmente influenzato gran parte delle ricerche svolte sul tema e, di conseguenza, sui tassi di prevalenza riportati nelle derivanti statistiche, i quali mostrano un'ampia variazione tra di loro. La maggior parte delle definizioni di cyberbullismo si è modellata sulla definizione più ampiamente condivisa di bullismo tradizionale, da ciò emerge come vi sia una certa sovrapposizione tra i due fenomeni. Un fattore complicante per la definizione del cyberbullismo è che le tre caratteristiche che definiscono il bullismo tradizionale, ossia intento, ripetizione e squilibrio di potere, non sempre si traducono facilmente nei comportamenti digitali. Dunque, le qualità specifiche degli ambienti digitali spesso rendono il cyberbullismo e il bullismo diversi in circostanze, motivazioni e risultati[35].

Con la crescente ubiquità di Internet, dei social media e delle piattaforme online, il modo in cui le persone interagiscono, in particolare i giovani, è cambiato radicalmente. Mentre gli sviluppi

[32] Cofinanciado por el programa Erasmus+ de la Unión Europea, From Peer to Peer, European Schools Cooperating to be Bullying Free 20161ES01KA201025501, B*aseline study on the state of art of bullying in Europe*, p.4.
[33] Cofinanciado por el programa Erasmus+ de la Unión Europea, From Peer to Peer, European Schools Cooperating to be Bullying Free 20161ES01KA201025501, B*aseline study on the state of art of bullying in Europe*, p.5.
[34] Smith PK, Mahdavi J, Carvalho M, Fisher S, Russell S, Tippett N, *Cyberbullying: its nature and impact in secondary school pupils*. J Child Psychol Psychiatry. 2008;49(4):376–385pmid:18363945.
[35] E. Englander, E. Donnerstein, R. Kowalski, C. A. Lin and K. Parti, *Defining Cyberbullying*, in Pediatrics, Official Journal of the American Accademy of Pediatrics, novembre 2017, articolo interamente disponibile e consultabile su https://pediatrics.aappublications.org/content/140/Supplement_2/S148#ref-4.

tecnologici offrono a bambini e adolescenti nuove opportunità di sviluppo e crescita personale, presentano anche sfide per la loro salute ed il loro benessere. Questo scenario ha aperto le porte a preoccupazioni e paure, con un conseguente incremento dell'attenzione globale sul fenomeno del cyberbullismo. Come già sottolineato, esso può includere l'invio di messaggi o commenti offensivi online, la diffusione di voci, l'esclusione delle vittime da gruppi online e altre forme di molestie[36] . Come il bullismo, l'esposizione al cyberbullismo è stata correlata aun'ampia gamma di esiti negativi, tra cui stress e pensieri suicidi[37], depressione eansia[38].



La presenza delle tecnologie dell'informazione e della comunicazione (TIC) in tutti gli ambiti della vita quotidiana colpisce inevitabilmente un numero crescente di bambini ed adolescenti, i quali hanno a disposizione un numero sempre maggiore di strumenti con cui restare connessi, sia a casa attraverso l'accesso ad Internet tramite computer e dispositivi intelligenti, sia in giro con smartphone o tablet. Per comprendere la portata della massiva presenza degli adolescenti online è opportuno sottolineare che, grazie alle ultime statistiche svolte in Europa, è stato stimato che circa il 38% dei ragazzi tra i 9 ed i 12 anni e circa il 77% tra i 13 ed i 16 anni posseggono un profilo sui social network. Certo è che le nuove tecnologie della società digitale attuale offrono maggiori opportunità e vantaggi agli utenti più giovani, ma è altresì vero che li pongono davanti anche a sfide significative. Infatti, sempre più adolescenti stanno diventando vittime di aggressioni tramite le TIC e ciò rende questa problematica un tema molto dibattuto ad ogni livello, nazionale ed internazionale. Il cyberbullismo non rispetta i confini, ma la percezione del problema dipende fortemente da aspetti tra cui la cultura, la storia, il contesto sociale e la storia politica del paese o dell'area in questione. In Europa, ad esempio, sono state prese diverse decisioni politiche, definiti ed implementati numerosi programmi per prevenire il cyberbullismo. Tuttavia, l'enorme impatto che questo fenomeno ha sull'intera collettività testimonia l'esigenza per le istituzioni europee di continuare a ricercare, legiferare ed incoraggiare azioni collettive ed individuali al fine di affrontarlo[39].

[36] OECD (2017), PISA 2015 Results (Volume III): Students' Well-Being, PISA, OECD Publishing, Paris, http:// dx.doi.org/10.1787/9789264273856-en.

[37] Kowalski, R. et al. (2014), Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth, Psychological Bulletin, Vol. 140/4, pp. 1073-1137, http:// dx.doi.org/10.1037/a0035618.

[38] Fahy, A. et al. (2016), Longitudinal Associations Between Cyberbullying Involvement and Adolescent Mental Health, Journal of Adolescent Health, Vol. 59/5, pp. 502-509, http://dx.doi.org/10.1016/ j.jadohealth.2016.06.006.

[39] C. Rizza, A. M. G. Pires Pereira, *Social Networks and Cyber-bullying among Teenagers*, Joint Research Centre, Luxembourg: Publications Office of the European Union, 2013, disponibile su https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/social-networks-and-cyber-bullying- among-teenagers.

In riferimento al quadro normativo per la tutela dei minori, esistono diverse basi giuridiche a cui è possibile fare riferimento. Innanzitutto, la *Convenzione delle Nazioni Unite sui diritti dell'infanzia*[40], approvata dall'Assemblea Generale il 20 novembre 1989, che esprime un consenso su quali siano gli obblighi degli Stati e della comunità internazionale nei confronti dell'infanzia. Negli articoli iniziali, gli Stati firmatari si assumono gli obblighi ivi previsti con il fine ultimo di una maggiore tutela dei bambini, termine con cui si intende ogni essere umano di età inferiore ai diciotto anni[41]. Gli Stati Parte rispettano e assicurano i diritti enunciati nella presente Convenzione a ciascun bambino entro la loro giurisdizione senza discriminazioni di alcun tipo, indipendentemente dalla razza, colore, sesso, lingua, religione del bambino o dei suoi genitori o tutore legale, opinione politica o di altro tipo, origine nazionale, etnica o sociale, proprietà, disabilità, nascita o altro stato. Inoltre, adottano tutte le misure appropriate per garantire che il bambino sia protetto contro ogni forma di discriminazione o punizione sulla base dello status, delle attività, delle opinioni espresse o delle convinzioni dei genitori, dei tutori legali o dei membri della famiglia del bambino[42]. Negli articoli successivi sono enunciate ulteriori garanzie a favore dei bambini, tra cui ad esempio il divieto di essere soggetti ad interferenze arbitrarie o illegali nella loro privacy, casa o corrispondenza; con il correlato obbligo per gli Stati parti di garantire loro una protezione legislativa contro tali interferenze[43]. Ancora, gli Stati parti adottano tutte le misure legislative, amministrative, sociali ed educative appropriate per proteggere il bambino da tutte le forme di violenza fisica o mentale, lesioni o abuso, negligenza o trattamento negligente, maltrattamento o sfruttamento, incluso l'abuso sessuale[44].

Per quanto riguarda l'Unione Europea, esistono diverse basi legali a cui poter fare riferimento, che variano a seconda delle diverse situazioni a cui ci troviamo di fronte. Alcune delle Direttive più importanti sono le seguenti:

- Direttiva 2012/29/UE del Parlamento europeo e del Consiglio, del 25 ottobre 2012, che stabilisce norme minime in materia di diritti, sostegno e protezione delle vittime di reato[45];

[40] United Nations Human Rights, Office of the High Commissioner, *Convention on the Rights of the Child*, testo integrale soncultabile su https://www.ohchr.org/en/professionalinterest/pages/crc.aspx.

[41] *«Ai fini della presente Convenzione, per bambino si intende ogni essere umano di età inferiore ai diciotto anni a meno che, in base alla legge applicabile al bambino, la maggioranza non venga raggiunta prima»*, United Nations Human Rights, Office of the High Commissioner, *Convention on the Rights of the Child*, testo interamente e gratuitamente consultabile su https://www.ohchr.org/en/professionalinterest/pages/crc.aspx.

[42] Art.2 of *Convention on the Rights of the Child*.

[43] Art.16 of *Convention on the Rights of the Child*.

[44] Art.19 e Art.34 of *Convention on the Rights of the Child*.

[45] EUR-Lex, Official Journal of the European Union, *Directive 2012/29/EU of the European Parliament and of the Council, 25 ottobre 2012, establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA*, testo integrale disponibile su https://eur- lex.europa.eu/legal-content/EN/TXT/?qid=1486939704096&uri=CELEX:32012L0029.

- Direttiva 2011/92/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011, sulla lotta contro l'abuso e lo sfruttamento sessuale dei bambini e la pornografia infantile[46];

- Direttiva (UE) 2016/800 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, sulle garanzie procedurali per i minori che sono indagati o imputati in procedimenti penali[47];

- Decisione quadro del Consiglio 2008/913/ GAI, del 28 novembre 2008, sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale[48];

- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati[49].

In riferimento al quadro normativo italiano, il bullismo può rappresentare una violazione dei principi fondamentali della Costituzione italiana[50]che attribuisce allo Stato il compito di promuovere e favorire il pieno sviluppo della persona umana secondo i seguenti principi: uguaglianza (art. 3), libertà di istruzione (art. 33), diritto all'istruzione (art. 34). A seconda di come viene espresso il comportamento, la violenza può anche essere considerata una violazione del codice penale[51], ad esempio: percosse (art. 581), lesioni (art. 582), danni a cose (art. 635), ingiurie (art. 594) o diffamazione (art. 595), molestie o disturbo alle persone (art. 660), minaccia (art. 612), atti persecutori e Stalking (art. 612 bis), furto d'identità (art. 494 cp). Le azioni di bullismo possono altresì infrangere le regole del diritto privato, rappresentando un illecito civile, il cui riferimento legale è riscontrabile nell'art. 2043 del Codice Civile[52] in cui viene definito come *«qualunque fatto doloso o colposo, che cagiona ad altri un danno ingiusto»* ed *«obbliga colui che ha commesso il fatto a risarcire il danno».*

[46] EUR-Lex, *Official Journal of the European Union, Directive 2011/92/EU of the European Parliament and of the Council, on combating the sexual abuse and sexual exploitation of children and child pornography*, and replacing Council Framework Decision 2004/68/JHA, 13 dicembre 2011, testo integralmente disponibile sul sito https://eur- lex.europa.eu/legal-content/EN/TXT/?qid=1486939746460&uri=CELEX:32011L0093.

[47] EUR-Lex, *Official Journal of the European Union, Directive (EU) 2016/800 of the European Parliament and of the Council, on procedural safeguards for children who are suspects or accused persons in criminal proceedings*, 11 maggio 2016, testo integrale disponibile su https://eur-lex.europa.eu/legal-content/EN/TXT/? qid=1486939841600&uri=CELEX:32016L0800.

[48] EUR-Lex, Official Journal of the European Union, Council Framework Decision, 2008/913/JHA, on combating certain forms and expressions of racism and xenophobia by means of criminal law, 28 novembre 2008, testo integrale disponibile su https://eur-lex.europa.eu/legal-content/EN/TXT/? qid=1486939877073&uri=CELEX:32008F0913.

[4949] EUR-Lex, *Official Journal of the European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (General Data Protection Regulation), 26 aprile 2016, testo integrale disponibile su https://eur-lex.europa.eu/legal-content/EN/TXT/? qid=1486939913107&uri=CELEX:32016R0679.

[50] Senato della Repubblica Italiana, Costituzione della Repubblica italiana, edizione 2012, disponibile su https://www.senato.it/documenti/repository/istituzione/costituzione.pdf.

[51] Gazzetta Ufficiale della Repubblica Italiana, *Codice Penale*, Regio Decreto, 19 ottobre 1930 , n. 1398, disponibile su https://www.gazzettaufficiale.it/anteprima/codici/codicePenale.

[52] Gazzetta Ufficiale della Repubblica Italiana, Codice Civile, *Regio Decreto, 16 marzo 1942*, n. 262, disponibile su https://www.gazzettaufficiale.it/anteprima/codici/codiceCivile.

Più nello specifico, con un decreto specifico del Presidente della Repubblica[53] è previsto che le scuole adottino un proprio regolamento disciplinare con il quale vengono affrontate le problematiche legate al *mobbing*, prevedendo anche procedure sanzionatorie. Inoltre, a seguito di gravi fatti di cronaca che hanno visto alcuni giovanissimi arrivare a gesti estremi dopo essere stati oggetto di insulti e diffamazioni su Internet, è stata recentemente approvata la prima bozza del Codice di Autoregolamentazione per la prevenzione e il contrasto del fenomeno del cyberbullismo[54]. Ultimo, ma non per importanza, è stata approvata una legge per la prevenzione ed il contrasto del fenomeno del cyberbullismo, soprattutto nel contesto minorile[55]. Si tratta della Legge n.71/2017[56], che ha introdotto nuove forme di tutela degli adolescenti colpiti da tale fenomeno. Tra queste ricordiamo, innanzitutto, l'informativa alle famiglie, che impone al dirigente scolastico che venga a conoscenza di atti di cyberbullismo di informare tempestivamente i soggetti esercenti la responsabilità genitoriale ovvero i tutori dei minori coinvolti e attiva adeguate azioni di carattere educativo, salvo che il fatto costituisca reato. Esiste poi il diritto di oscuramento, che prevede che il minore che abbia compiuto almeno 14 anni, o i genitori o gli esercenti la responsabilità sul minore, possano inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco di qualsiasi altro dato personale del minore, diffuso nella rete internet. Se non si provvede entro 48 ore, l'interessato può rivolgersi al Garante della Privacy che interviene direttamente entro le successive 48 ore[57].

A livello regionale, la Toscana è attivamente impegnata nella campagna di sensibilizzazione sul tema. Proprio contro il cyberbullismo è nata, infatti, una piattaforma online per la formazione degli insegnanti e l'utilizzo di strumenti operativi, grazie ad una collaborazione tra il MIUR, Direzione generale per lo studente, e il Dipartimento di Scienze della Formazione e Psicologia dell'Università di Firenze. La *Piattaforma ELISA*[58] doterà le scuole e i docenti di strumenti per intervenire efficacemente contro il bullismo e il cyberbullismo.

A conclusione di questo capitolo, preme sottolineare come sia errato inquadrare l'avvento delle nuove

[53] Gazzetta Ufficiale della Repubblica Italiana, *Decreto del Presidente della Repubblica n.249, Regolamento recante lo statuto delle studentesse e degli studenti della scuola secondaria*, testo integralmente disponibile su 24 giugno 1998, https://www.gazzettaufficiale.it/eli/id/1998/07/29/098G0305/sg.

[54] Governo Italiano, Ministero dello Sviluppo Economico, *Cyberbullismo: online il Codice di Autoregolamentazione*, 08 gennaio 2014 https://www.sviluppoeconomico.gov.it/index.php/it/component/content/article?id=2029886.

[55] Camera dei Deputati, *Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo*, 17 maggio 2017, disponibile su https://www.camera.it/leg17/126?tab=1&leg=17&idDocumento=3139- b&sede=&tipo=.

[56] Gazzetta ufficiale della Repubblica italiana, Legge 29 maggio 2017, n. 71 *Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo*. (17G00085) (GU Serie Generale n.127 del 03-06- 2017), testo integrale disponibile su https://www.gazzettaufficiale.it/eli/id/2017/06/3/17G00085/sg.

[57] Commissariato di P.S. online, sportello per la sicurezza degli utenti del web, *Che cos'è il Cyberbullismo?*, consultabile su https://www.commissariatodips.it/approfondimenti/cyberbullismo/che-cose-il-cyberbullismo/index.html.

[58] Piattaforma ELISA, su https://www.piattaformaelisa.it/elisa/cose-elisa/.

tecnologie e l'espansione del nuovo mondo *online* tanto in maniera catastroficamente negativa, quanto in maniera eccessivamente positiva. È opportuno cercare, invece, di comprenderne le enormi potenzialità, sfruttandole a favore delle nuove generazioni, per migliorare e facilitare il loro sviluppo cognitivo e relazionale. Tuttavia, ciò non deve far sottovalutare le insidie che questa nuova realtà porta con sé. È necessaria una piena consapevolezza del ruolo assunto negli ultimi anni dai siti di social network, che ampliano in maniera significativa le reti sociali dei giovani di oggi e possono rappresentare lo spazio privilegiato per la nascita di dinamiche malsane che rischiano di svilupparsi anche *off-line.* In quest'ottica, è fondamentale il rafforzamento dell'azione di tutela dei minori riguardo ai contenuti presenti in rete ed ai comportamenti da essi stessi adottati nell'utilizzarla, ignari o scarsamente coscienti dei meccanismi di protezione della privacy e dei rischi a cui sono esposti rendendo pubblici dettagli e comportamenti inerenti alla propria vita privata e quella dei loro coetanei[59].

[59] Governo italiano, Ministero dello Sviluppo Economico, *Bozza del Codice di Autoregolamentazione*, 08 gennaio 2014 https://www.sviluppoeconomico.gov.it/index.php/it/component/content/article?id=2029886.

CAPITOLO II
LA CYBERSECURITY NELL'AMBITO EUROPEO, NAZIONALE E REGIONALE

1. Cybersecurity: tra definizioni e contraddizioni

Il termine *cyber security* è di uso piuttosto recente ed è stato diffuso principalmente dal *National Institute for Standards and Technologies (*NIST[60]) degli Stati Uniti. Lacosiddetta *cyber security* è focalizzata principalmente sulla protezione dei sistemi informatici (computer, reti di telecomunicazione, smartphone, ecc.) e dell'informazione in formato digitale da attacchi interni e soprattutto esterni. Altri termini utilizzati precedentemente ed in alternativa sono *IT security*, *ICT security*, *sicurezza informatica* e *sicurezza delle informazioni*. Quest'ultima comprende anche la protezione delle informazioni in formato non digitale, ad esempio cartaceo. Al netto dell'informazione in formato cartaceo, sono tutti termini abbastanza interscambiabili, a meno che non si stia discutendo in un contesto estremamente specialistico[61].

Molti professionisti, tuttavia, sottolineano la mancata esistenza di un termine univoco e onnicomprensivo sull'argomento. Il termine "*cybersecurity*" acquista infatti accezioni differenti a seconda dell'ambiente in cui viene utilizzato. Il governo del Montenegro[62] sottolinea la lacuna presente in questo settore e dedica al suddetto argomento un'intera sezione della sua strategia di sicurezza informatica[63]. Sebbene il documento affermi di presentare definizioni conformi ai significati di base intesi nei paesi dell'Unione Europea, purtroppo non fornisce effettivamente una conclusione sul termine *sicurezza informatica*, ma cita piuttosto varie definizioni da altre fonti. Difatti, il documento stesso evidenzia il rischio di una terminologia incerta e mira a fornire chiarimenti sulle posizioni relative alla sicurezza informatica e alla sicurezza delle informazioni.

---

[60] Il National Institute of Standards and Technology (NIST), fondato nel 1901, fa parte del Dipartimento del Commercio degli Stati Uniti ed è uno dei più antichi laboratori di scienze fisiche della nazione. National Institute for Standards and Technologies, about NIST, https://www.nist.gov/about-nist.

[61] J. Khamlichi, M. Lai, A. Pennasilico, M Santini, C. Telmon, *Cyber security: cos'è e come garantire la sicurezza dei sistemi informatici e delle reti*, in Cybersecurity360, https://www.cybersecurity360.it/cybersecurity- nazionale/cyber-security-la-guida-definitiva-per-la-corretta-implementazione-in-azienda/.

[62] Government of Montenegro. (2013).
National Cyber Security Strategy for Montenegro 2013-2017. Podgorica Retrieved https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Montenegro_2013_Cyber%20Security%20Strategy%20for%20Montenegro.pdf.

[63] Montenegro, National cyber security strategy for Montenegro 2013-2017, Podgorica, July 2013, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Montenegro_2013_Cyber%20Security%20Strategy%20for%20Montenegro.pdf.

Poste tali premesse, "***Cybersecurity***" è emerso negli ultimi anni come un termine ampiamente utilizzato, con una sempre maggiore adozione da parte di professionisti e politici. Tuttavia, come con molti gerghi alla moda, sembra esserci pochissima comprensione di quale sia il suo reale significato. Sebbene questo possa non risultare un problema quando viene utilizzato in un contesto puramente informale, ciò può invece potenzialmente causare notevoli difficoltà nel contesto della strategia organizzativa, degli obiettivi aziendali o degli accordi internazionali[64]. È interessante sottolineare come molti studi si focalizzino sulla ricerca di una definizione univoca, base necessaria per la creazione di azioni comuni o accordi internazionali in tale ambito. In altre parole, affinché gli Stati possano mettere in atto azioni concrete per il perfezionamento della *cibersicurezza,* è assolutamente necessaria una previa definizione, universalmente riconosciuta, di ciò a cui facciamo effettivamente riferimento quando utilizziamo tale termine. In quest'ottica, alcuni studiosi propongono una definizione interessante di *cybersicurezza*[65], ripresa da quella fornita dalla Repubblica Sudafricana[66], intesa come "l'*approccio e le azioni associati ai processi di gestione dei rischi per la sicurezza seguiti dalle organizzazioni e dagli stati per proteggere la riservatezza, l'integrità e la disponibilità dei dati e delle risorse utilizzati nel cyber-spazio. Il concetto include linee guida, politiche e raccolte di salvaguardie, tecnologie, strumenti e formazione per fornire la migliore protezione per lo stato dell'ambiente cibernetico e dei suoi utenti*".

2. Sviluppo del quadro normativo europeo

L'Unione Europea ha iniziato ad occuparsi di cybersecurity agli inizi degli anni 2000. I primi documenti cercano di individuare le aree di priorità in ambito di sicurezza delle reti e restano significativi proprio per l'idea che forniscono dell'impostazione e delle priorità originarie dell'Unione. È importante evidenziare che il termine specifico "*cybersecurity*" non compare all'interno di questi primi documenti e non comparirà fino all'elaborazione della relazione del 2008[67] sull'implementazione della strategia europea in materia di sicurezza del 2003[68]. Fino a quel momento, infatti, si parlerà di cybercrime e di protezione dei dati personali e delle infrastrutture critiche, senza esplicito

[64] Schatz, Daniel, Bashroush, R. and Wall, J. 2017. *Towards a More Representative Definition of Cyber Security*. Journal of Digital Forensics, Security and Law. 12 (2), pp. 53-74 . https://doi.org/10.15394/jdfsl.2017.1476.

[65] Schatz, Daniel, Bashroush, R. and Wall, J. 2017. *Towards a More Representative Definition of Cyber Security*. Journal of Digital Forensics, Security and Law. 12 (2), pp. 53-74 . https://doi.org/10.15394/jdfsl.2017.1476.

[66] Republic of South Africa, Government Gazette Staatskoerant, *Draft cybersecurity policy of South Africa*, 19 febbraio 2010, p.15.

[67] Consiglio dell'Unione Europea, *Strategia europea in materia di sicurezza, un'Europa sicura in un mondo migliore*, Ufficio delle pubblicazioni dell'Unione europea, Lussemburgo, 2009, testo integralmente e gratuitamente disponibile su https://www.consilium.europa.eu/media/30812/qc7809568itc.pdf.

[68] Il Consiglio europeo ha adottato la strategia europea in materia di sicurezza nel dicembre 2003. Per la prima volta, ha stabilito principi e fissato obiettivi chiari per portare avanti gli interessi dell'UE in materia di sicurezza in base ai nostri valori fondamentali. La strategia adotta un approccio globale e rimane pienamente pertinente. Questa relazione non sostituisce la strategia europea in materia di sicurezza, ma la rafforza. Politica estera e di sicurezza comune (2003). Gazzetta Ufficiale dell'Unione Europea, *Risoluzione del Parlamento europeo sulla relazione annuale del Consiglio al Parlamento europeo relativa agli aspetti principali e alle scelte di base della politica estera e di sicurezza comune (PESC), comprese le implicazioni finanziarie per il bilancio generale delle Comunità europee* — 2003 (8412/2004 — 2004/2172(INI)), 9 febbraio 2006, Testo integrale su https://eur- lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52005IP0132&from=DA.

riferimento al concetto più comprensivo di cybersecurity[69].

Nel 2000 la Commissione ha elaborato una comunicazione sul cybercrime[70] che tratta due questioni fondamentali della cybersecurity: la sicurezza delle infrastrutture dell'informazione e la lotta al crimine informatico. Questi macro-aspetti della cybersecurity costituiscono il nocciolo duro della visione europea, che dal 2000 mantiene queste due priorità in cima alla *to do list* per la sicurezza cibernetica.

Nel 2001 la Commissione ha presentato un documento[71] interamente dedicato alla definizione della *Network and Information Security* (NIS), che si propone la realizzazione di una politica europea in materia. Il testo è stato approvato nel mese di giugno, dunque prima dell'attentato alle torri gemelle, e per questo esso testimonia la volontà autonoma dell'Unione di seguire un proprio percorso in questo campo. All'interno del documento si trova una definizione della NIS, che viene intesa come *«la capacità di una rete o di un sistema d'informazione di resistere, ad un determinato livello di riservatezza, ad eventi imprevisti o atti dolosi che compromettono la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei servizi forniti o accessibili tramite la suddetta rete o sistema[72]»*.

Nei primi anni 2000 altri due documenti hanno segnato l'inizio di un interessamento europeo alle dinamiche scaturite dal processo di digitalizzazione: il documento *eEurope[73]* del 2000 e quello *eEurope 2005[74]* del 2002. Questi si inseriscono all'interno della visione presentata dalla strategia di Lisbona del 2000, intesa a far diventare l'Europa l'economia basata sulla conoscenza *«più competitiva e più dinamica del mondo»* entro il 2010, ed esprimono la necessità per l'Europa di dotarsi di moderni servizi pubblici offerti sulla rete e di un'affidabile infrastruttura di protezione dell'informazione[75].

---

[69] C. Cencetti, *Cybersecurity: Unione europea e Italia, Prospettive a confronto*, Quaderni IAI, Istituto Affari Internazionali (IAI), Edizioni Nuova Cultura, Roma, 2014, p.22, https://www.consilium.europa.eu/media/30812/qc7809568itc.pdf.

[70] EUR-Lex, Access to European Union Law, *Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle Regioni - Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica* - eEurope 2002, https://eur-lex.europa.eu/legal-content/it/ALL/?uri=CELEX%3A52000DC0890.

[71] EUR-Lex, Access to European Union Law, *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach COM(2001)298*, gratuitamente disponibile su https://eur- lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52001DC0298.

[72] C. Cencetti, *Cybersecurity: Unione europea e Italia, Prospettive a confronto*, Quaderni IAI, Istituto Affari Internazionali (IAI), Edizioni Nuova Cultura, Roma, 2014, p.23, https://www.consilium.europa.eu/media/30812/qc7809568itc.pdf.

[73] EUR-Lex, Access to European Union Law, Commissione delle Comunità Europee, eEurope, *Una società dell'informazione per tutti Per il Consiglio europeo straordinario sull'occupazione, le riforme economiche e la coesione sociale - Per un'Europa basata sull'innovazione e sulle conoscenze*, Bruxelles, 8 marzo 2000, disponibile su https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52000DC0130&from=ES.

[74] EUR-Lex, Access to European Union Law, *Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle regioni - eEurope 2005: una società dell'informazione per tutti - Piano d'azione da presentare per il Consiglio europeo di Siviglia 21 e 22 giugno 2002*. /* COM/2002/0263 def. */, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:52002DC0263.

[75] C. Cencetti, *Cybersecurity: Unione europea e Italia, Prospettive a confronto*, Quaderni IAI, Istituto Affari Internazionali (IAI), Edizioni Nuova Cultura, Roma, 2014, p.24, https://www.consilium.europa.eu/media/30812/qc7809568itc.pdf.

Ancora nel 2002 sono state approvate tre importanti direttive in materia di NIS: la direttiva 2002/21/CE[76], che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica; la direttiva 2002/19/CE[77], relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate e all'interconnessione delle medesime; e la direttiva 2002/20/CE[78], relativa alle autorizzazioni per le reti ed i servizi di comunicazione elettronica. Esse sono state tutte abrogate, in seguito all'approvazione nel 2009 di una nuova direttiva "*framework*", di cui si dirà più avanti.

Nel 2003 l'UE ha elaborato una propria strategia in materia di sicurezza in cui non viene fatta alcuna menzione del termine "*cybersecurity*", ma in cui viene però individuato una *«dipendenza europea da un'infrastruttura interconnessa nel settore dei trasporti, dell'energia, dell'informazione ed altri, e la conseguente vulnerabilità dell'Europa sotto questo profilo»*. Nonostante una relazione sulla sua implementazione pubblicata nel 2008[79], la strategia europea per la sicurezza non ha subito modifiche sostanziali.

Il 2004 è stato un anno molto importante per l'avanzamento della cybersecurity in Europa, poiché l'Unione ha approvato il regolamento (CE) 460/2004 che istituisce l'Agenzia europea di sicurezza delle reti e dell'informazione[80], o *European Network and Information Security Agency (ENISA)* meglio conosciuta con l'acronimo inglese ENISA, il cui scopo è quello di *«assicurare un alto ed efficace livello di sicurezza delle reti e dell'informazione nell'ambito della Comunità e di sviluppare una cultura in materia di sicurezza delle reti e dell'informazione»*. L'Agenzia ha il compito di assistere la Commissione e la comunità degli stati membri, accrescendone le capacità di prevenire e affrontare i problemi di sicurezza delle reti e dell'informazione e di reagirvi, fornendo loro assistenza e consulenza e contribuendo allo sviluppo generale di un alto livello di competenze.

Inoltre, l'agenzia contribuisce a promuovere e diffondere una nuova cultura della sicurezza, affinché la questione della cybersecurity venga adeguatamente affrontata a livello europeo e soprattutto nazionale, tramite la predisposizione degli strumenti legali opportuni. Nel maggio 2013, con il

[76] EUR-Lex, Access to European Union Law, Direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (direttiva quadro), https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32002L0021.

[77] EUR-Lex, Access to European Union Law, *Direttiva 2002/19/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate, e all'interconnessione delle medesime* (direttiva accesso), https://eur-lex.europa.eu/legal-content/IT/ALL/? uri=CELEX%3A32002L0019.

[78] EUR-Lex, Access to European Union Law, *Direttiva 2002/20/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica* (direttiva autorizzazioni), https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32002L0020.

[79] Consiglio dell'Unione Europea, *Strategia europea in materia di sicurezza, un'Europa sicura in un mondo migliore*, Segretariato generale del Consiglio, Bruxelles, 2009, https://www.consilium.europa.eu/media/30812/qc7809568itc.pdf.

[80] EUR-Lex, Access to European Union Law, *Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione*, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32004R0460.

regolamento (UE) 526/201318[81], la Commissione ha esteso e rafforzato il mandato dell'ENISA fino al 2020, facendo così dell'agenzia il vero punto di riferimento europeo per la cybersecurity[82].

Nel 2008 l'Unione ha presentato la Relazione sull'attuazione della Strategia europea in materia di sicurezza, già citata in precedenza, che nella sua versione in lingua inglese contiene finalmente il termine "*cybersecurity*". Nello specifico, la sicurezza informatica viene presentata come un aspetto rilevante delle questioni di terrorismo e criminalità organizzata. Dunque, viene fatto formalmente riferimento alla cybersecurity, considerando la possibilità che attacchi di natura cibernetica aventi come bersaglio sistemi informatici privati o governativi, possano divenire una nuova potenziale arma economica, politica e militare. Sebbene la cybersecurity ricopra una parte ristretta del documento, la relazione è senza dubbio importante per quanto riguarda lo sviluppo della trattazione europea di questa materia[83].

Nel 2010 sono stati pubblicati altri due importanti documenti, ovvero l'*Agenda digitale europea*[84] e la *Strategia di sicurezza interna*[85]. La prima si prefigge lo scopo di *«ottenere vantaggi socioeconomici sostenibili grazie a un mercato digitale unico basato su internet veloce e superveloce e su applicazioni interoperabili»*. Nello specifico, l'Agenda individua le linee d'azione da seguire nei due macrosettori del "mercato digitale unico e dinamico" e dell'"interoperabilità e standard". La realizzazione di un mercato unico e sicuro, da una parte, incrementa la sicurezza dei cittadini europei e, dall'altra, attrae investimenti a beneficio di domanda ed offerta. L'obiettivo è, dunque, quello di conseguire dei vantaggi dal punto di vista sociale ed economico, a partire dall'attuale situazione di interconnessione costante e digitalizzazione crescente. La strategia di sicurezza interna, invece, cerca di delineare le attuali minacce alla tenuta del complesso europeo, così individuando alcune tappe verso un'Europa più sicura. Inoltre, si sottolinea l'importanza di collaborare con il settore privato e di conseguire progressi in campo tecnologico, per garantire una risposta efficace ai *cyber attack*, una partnership pubblico-privata ed una capability building, condizioni imprescindibili per la cybersecurity[86].

---

[81] EUR-Lex, Access to European Union Law, *Regolamento (UE) n. 526/2013 del Parlamento europeo e del Consiglio, del 21 maggio 2013 , relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA)* e che abroga il regolamento (CE) n. 460/2004, https://eur-lex.europa.eu/legal- content/IT/TXT/?uri=CELEX%3A32013R0526.

[82] C. Cencetti, Cybersecurity: Unione europea e Italia, Prospettive a confronto, Quaderni IAI, Istituto Affari Internazionali (IAI), Edizioni Nuova Cultura, Roma, 2014, pp. 25-26, https://www.consilium.europa.eu/media/30812/qc7809568itc.pdf.

[83] C. Cencetti, *Cybersecurity: Unione europea e Italia, Prospettive a confronto*, Quaderni IAI, Istituto Affari Internazionali (IAI), Edizioni Nuova Cultura, Roma, 2014, p. 29, https://www.consilium.europa.eu/media/30812/qc7809568itc.pdf.

[84] EUR-Lex, Access to European Union Law, Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni*, Un'agenda digitale europea*, 26 agosto 2010, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:IT:PDF.

[85] EUR-Lex, Access to European Union Law, *Comunicazione della Commissione al Parlamento Europeo e al Consiglio, La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura*, 22 novembre 2010, https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:52010DC0673.

[86] C. Cencetti, *Cybersecurity: Unione europea e Italia, Prospettive a confronto*, Quaderni IAI, Istituto Affari Internazionali (IAI), Edizioni Nuova Cultura, Roma, 2014, pp. 32-34, https://www.consilium.europa.eu/media/30812/qc7809568itc.pdf.

Il 9 giugno 2016 il Consiglio adotta delle *Conclusioni sul tema della lotta contro le attività criminali nel ciberspazio*[87]. Suddette conclusioni[88] definiscono misure concrete per future azioni in tre principali settori: primo, la razionalizzazione delle procedure di assistenza giudiziaria reciproca; secondo, il miglioramento della cooperazione con i fornitori di servizi; terzo, l'avvio di un processo di riflessione su possibili criteri di collegamento per la competenza esecutiva nel ciberspazio[89].

Il 20 dicembre 2017 le istituzioni dell'Unione Europea hanno compiuto un ulteriore importante passo in avanti con il rafforzamento della loro cooperazione nella lotta ai ciberattacchi, concludendo un accordo interistituzionale[90] che istituisce una squadra permanente di pronto intervento informatico (CERT-UE[91]) per l'insieme delle istituzioni, degli organi e delle agenzie dell'UE. L'obiettivo è quello di potenziare la task force esistente trasformandola in una squadra permanente ed efficace, responsabile di garantire una risposta coordinata dell'UE ai ciberattacchi mossi contro le sue istituzioni. Per questo, il CERT-UE collabora molto strettamente con le squadre interne di sicurezza informatica delle istituzioni dell'UE e mantiene i contatti con le squadre di pronto intervento informatico e le società di sicurezza informatica negli Stati membri e altrove, scambiando informazioni sulle minacce e sui modi per affrontarle, collaborando, inoltre, con le sue controparti in sede di NATO[92].

Successivamente, il 19 novembre 2018, il Consiglio ha adottato una versione aggiornata del *quadro strategico dell'Unione Europea in materia di ciberdifesa*[93]. Quest'ultimo aggiornamento consente all'Unione di tener conto delle mutevoli sfide in materia di sicurezza sorte successivamente all'adozione del quadro iniziale il 18 novembre 2014, facendo particolare riferimento a misure restrittive volte a scoraggiare i ciberattacchi ed a permettere una risposta tempestiva ed efficace,

[87] Council of the European Union, *Council conclusions on improving criminal justice in cyberspace*, Lussemburgo, 9 giugno 2016, https://www.consilium.europa.eu/media/24300/cyberspace-en.pdf.
[88] Council of the European Union, *Council conclusions on the European Judicial Cybercrime Network*, Lussemburgo, 9 giugno 2016, https://www.consilium.europa.eu/media/24301/network-en.pdf.
[89] Consiglio dell'Unione europea, *La cibersicurezza in Europa: norme più severe e migliore protezione*, Politiche, https://www.consilium.europa.eu/it/policies/cybersecurity/.
[90] Gazzetta ufficiale dell'Unione europea, *Accordo tra il Parlamento europeo, il Consiglio europeo, il Consiglio dell'Unione europea, la Commissione europea, la Corte di giustizia dell'Unione europea, la Banca centrale europea, la Corte dei conti europea, il Servizio europeo per l'azione esterna, il Comitato economico e sociale europeo, il Comitato europeo delle regioni e la Banca europea per gli investimenti sull'organizzazione e il funzionamento della squadra di pronto intervento informatico delle istituzioni, degli organi e delle agenzie dell'Unione* (CERT-UE), 13 gennaio 2018, https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/? uri=CELEX:32018Q0113(01)&from=LV.
[91] The Computer Emergency Response Team for the EU Institutions, bodies and agencies
[92] Consiglio dell'Unione europea, *Cibersicurezza: le istituzioni dell'UE rafforzano la loro cooperazione per contrastare i ciberattacchi*, in Comunicati Stampa, 20 dicembre 2017, consultabile su https://www.consilium.europa.eu/it/press/press-releases/2017/12/20/cybersecurity-eu-institutions-strengthen- cooperation-to-counter-cyber-attacks/.
[93] Consiglio dell'Unione europea, *Quadro strategico dell'UE in materia di ciberdifesa* (aggiornato nel 2018), Bruxelles, 19 novembre 2018, https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/it/pdf.

contribuendo a migliorare la capacità degli Stati membri nel settore della cibersicurezza[94].
A seguito di un accordo provvisorio tra la presidenza ed il Parlamento Europeo siglato il 19 dicembre 2018, il Consiglio ha adottato, il 9 aprile 2019, il regolamento anche noto come *regolamento sulla cibersicurezza*[95] il quale, da una parte, introduce un insieme di sistemi di certificazione a livello di Unione Europea per prodotti, servizi e processi digitali, dall'altra, rinnova e rafforza l'attuale Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA), trasformandola in un'agenzia permanente dell'UE per la cibersicurezza[96].

In riferimento al quadro europeo di certificazione della cibersicurezza[97], esso consente la creazione di sistemi di certificazione dell'UE su misura e basati sui rischi, i quali svolgono un ruolo fondamentale nell'aumentare la fiducia e la sicurezza nei prodotti e servizi, elementi fondamentali per il mercato unico digitale. L'obiettivo è quello di fornire dei sistemi di certificazione a livello dell'Unione Europea come un insieme completo di regole, requisiti tecnici, standard e procedure. In altri termini, tutti i prodotti riguardanti le tecnologie dell'informazione e della comunicazione (TIC) dovranno essere certificati conformemente agli schemi previamente stabiliti e condivisi. In particolare, ogni schema europeo dovrebbe specificare: a) le categorie di prodotti e servizi coperti, b) i requisiti di cibersicurezza, ad esempio facendo riferimento a standard o specifiche tecniche, c) il tipo di valutazione (es. Autovalutazione o valutazione di terzi), ed) il livello di garanzia previsto (ad esempio, di base, sostanziale e / o elevato). Il certificato risultante sarà riconosciuto in tutti gli Stati membri dell'UE, rendendo più facile per le imprese il commercio transfrontaliero e per gli acquirenti comprendere le caratteristiche di sicurezza del prodotto o servizio. Per quanto riguarda l'attuazione del quadro di certificazione, le autorità degli Stati membri sono riunite nell'*European Cybersecurity Certification Group (ECCG)*[98], che ha il compito di consigliare ed assistere la Commissione nelsuo lavoro per garantire l'attuazione e l'applicazione coerenti della legge sulla cibersicurezza, in particolare per quanto riguarda il programma di lavoro continuo dell'Unione, le questioni politiche in materia di certificazione della cibersicurezza, il coordinamento degli approcci politici e la preparazione di sistemi europei di certificazione della cibersicurezza. Inoltre, esso assiste, consiglia e coopera con l'ENISA e facilita la cooperazione tra le autorità nazionali di certificazione della cibersicurezza attraverso il rafforzamento delle capacità e lo scambio di informazioni[99].

Per quanto riguarda l'ENISA, invece, essa ha un ruolo chiave nella creazione e nel mantenimento del quadro europeo di certificazione della sicurezza informatica preparando la base tecnica per schemi di certificazione specifici ed informando il pubblico sugli schemi di certificazione e sui certificati

[94] Consiglio dell'Unione europea, *Ciberdifesa: il Consiglio aggiorna il quadro strategico*, in Comunicati Stampa, 19 novembre 2018, su https://www.consilium.europa.eu/it/press/press-releases/2018/11/19/cyber-defence-council-updates-policy-framework/.
[95] Gazzetta ufficiale dell'Unione europea, Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»), 7 giugno 2019, https://eur-lex.europa.eu/legal- content/IT/TXT/PDF/?uri=CELEX:32019R0881&from=IT.
[96] Consiglio dell'Unione europea, *La cibersicurezza in Europa: norme più severe e migliore protezione*, Politiche, https://www.consilium.europa.eu/it/policies/cybersecurity/.
[97] Per ulteriori informazioni, Consiglio dell'Unione europea, *Un'Unione europea più forte in materia di cibersicurezza: il Consiglio approva un accordo sulla certificazione comune e sul potenziamento dell'agenzia*, in Comunicato Stampa, 19 dicembre 2018, https://www.consilium.europa.eu/it/press/press-releases/2018/12/19/eu-to- become-more-cyber-proof-as-council-backs-deal-on-common-certification-and-beefed-up-agency/.
[98] European Commission, *The EU cybersecurity certification framework*, in Policies, https://ec.europa.eu/digital- single-market/en/eu-cybersecurity-certification-framework.
[99] European Commission, *The European Cybersecurity Certification Group*, in Policies, https://ec.europa.eu/digital- single-market/en/european-cybersecurity-certification-group.

emessi attraverso un sito web dedicato. Inoltre, ha il compito di aumentare la cooperazione operativa a livello dell'UE, aiutando gli Stati membri che lo richiedano a gestire gli incidenti di cibersicurezza e sostenendo il coordinamento dell'UE in caso di crisi e attacchi informatici transfrontalieri su larga scala. Questa attività si basa proprio sul ruolo dell'ENISA come segretariato della rete nazionale dei gruppi di risposta agli incidenti di sicurezza informatica (CSIRT), istituita dalla direttiva sulla sicurezza delle reti e dei sistemi informativi (direttiva NIS).

La *direttiva NIS*[100], adottata il 6 di luglio 2016 (in vigore da agosto 2016), rappresenta una pietra miliare importante verso la costruzione della resilienza della sicurezza informatica a livello europeo, essendo il primo regolamento in tutta l'Unione Europea sulla sicurezza informatica. L'obiettivo della direttiva è quello di raggiungere un elevato livello comune di sicurezza delle reti e dei sistemi informativi all'interno dell'Unione, mediante migliori capacità di cibersicurezza a livello nazionale, maggiore cooperazione e gestione dei rischi a livello unionale, obblighi di segnalazione degli incidenti per gli operatori di servizi essenziali e fornitori di servizi digitali.

L'artico 12 della sopracitata direttiva istituisce la rete *Computer Security Incident Response Team* (CSIRT) *«al fine di contribuire allo sviluppo della fiducia e della fiducia tra gli Stati membri e per promuovere una cooperazione operativa rapida ed efficace».* La rete di CSIRT è composta da rappresentanti dei CSIRT degli Stati membri e del CERT-UE, mentre la Commissione Europea partecipa alla rete in qualità di mero osservatore. L'ENISA ha il compito di sostenere attivamente la cooperazione dei CSIRT, provvedere al segretariato e fornire supporto attivo per il coordinamento degli incidenti quando richiesto. In breve, la rete CSIRT fornisce un forum in cui i membri possono cooperare, scambiare informazioni e creare fiducia, con il fine ultimo di permettere agli Stati membri di migliorare la gestione degli incidenti transfrontalieri e persino discutere su come rispondere in modo coordinato a specifici incidenti[101].

Come già evidenziato, la direttiva NIS è il primo atto legislativo dell'UE sulla sicurezza informatica e fornisce, appunto, misure legali fondamentali per aumentare il livello generale di sicurezza informatica nell'UE. Essa garantisce una preparazione degli Stati membri richiedendo loro di essere adeguatamente attrezzati, ad esempio tramite un gruppo di risposta agli incidenti di sicurezza informatica (CSIRT) e un'autorità NIS nazionale competente. Inoltre, assicura una cooperazione attiva tra tutti gli Stati membri, al fine di sostenere e facilitare la cooperazione strategica e lo scambio di informazioni tra gli Stati membri. Quest'ultimi dovranno inoltre creare una rete CSIRT, al fine di promuovere una cooperazione operativa rapida ed efficace su specifici incidenti di cibersicurezza e condividere informazioni sui rischi.

[100] EUR-Lex, *Access to European Union Law, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, 19 luglio 2016, il testo di legge integrale è gratuitamente consultabile su https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.

[101] European Union Agency for Cybersecurity, CSIRTs Network, https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network.

Poiché il panorama delle minacce alla sicurezza informatica è in rapida evoluzione, il 13 settembre 2017 la Commissione ha adottato una comunicazione[102] che mira a sostenere gli Stati membri nei loro sforzi per attuare la direttiva in modo rapido e coerente in tutta l'Unione Europea. Dunque, essa fornisce informazioni pratiche agli Stati membri, ad esempio fornendo spiegazioni ed interpretazioni di disposizioni specifiche della direttiva per chiarire come dovrebbe funzionare nella pratica[103].

Riassumendo, dunque, il *Cybersecurity Act* dell'Unione Europea agisce su tre versanti distinti, diversi tra loro ma intrinsecamente interconnessi. Primo, esso crea un quadro europeo di certificazione della sicurezza informatica per prodotti, servizi e processi TIC, da cui i cittadini guadagnano sulla trasparenza delle caratteristiche di sicurezza di prodotti e servizi ed, al contempo, da cui i venditori e fornitori acquisiscono un vantaggio competitivo per soddisfare la crescente esigenza di soluzioni digitali più sicure. Secondo, rafforza l'ENISA, l'agenzia dell'UE per la sicurezza informatica. Terzo, integra la direttiva sulla sicurezza delle reti e dei sistemi informativi (direttiva NIS)[104].

3. Contesto italiano

Con il Decreto Legislativo 18 maggio 2018[105], n.65, pubblicato sulla Gazzetta Ufficiale n. 132 del 9 giugno 2018, l'Italia ha dato attuazione, recependola nell'ordinamento nazionale, alla Direttiva (UE) 2016/1148, cd. Direttiva NIS, intesa a definire le misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi. Il decreto si applica agli Operatori di Servizi Essenziali (OSE) e ai Fornitori di Servizi Digitali (FSD). In breve, gli OSE sono i soggetti, pubblici o privati, che forniscono servizi essenziali per la società e l'economia nei settori sanitario, dell'energia, dei trasporti, bancario, delle infrastrutture dei mercati finanziari, della fornitura e distribuzione di acqua potabile e delle infrastrutture digitali. Gli FSD, invece, sono le persone giuridiche che forniscono servizi di e-commerce, cloud computing o motori di ricerca, con stabilimento principale, sede sociale o rappresentante designato sul territorio nazionale. Gli obblighi

[102] EUR-Lex, Access to European Union Law, *Communication from the Commission to the European Parliament and the Council Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union*, 28 ottobre 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0546.

[103] European Commission, *The Directive on security of network and information systems (NIS Directive),* in Policies, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

[104] European Commission, *The EU Cybersecurity Act at a glance*, in News, 25 giugno 2019, https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-glance.

[105] Gazzetta Ufficiale della Repubblica Italiana, *Decreto Legislativo 18 maggio 2018, n. 65 Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*. (18G00092) (GU Serie Generale n.132 del 09- 06-2018), Testo integrale gratuito disponibile su https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2018-06-09&atto.codiceRedazionale=18G00092&elenco30giorni=false.

previsti per gli FSD non si applicano alle imprese che la normativa europea definisce "piccole" e "micro", quelle cioè che hanno meno di cinquanta dipendenti e un fatturato o bilancio annuo non superiore ai 10 milioni di euro. Tanto gli OSE che gli FSD sono chiamati ad adottare misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi ed a prevenire e minimizzare l'impatto degli incidenti a carico della sicurezza delle reti e dei sistemi informativi, al fine di assicurare la continuità del servizio. Entrambi hanno, inoltre, l'obbligo di notificare, senza ingiustificato ritardo, gli incidenti che hanno un impatto rilevante, rispettivamente sulla continuità e sulla fornitura del servizio, al *Computer Security Incident Response Team* (CSIRT) italiano, informandone anche l'Autorità competente NIS di riferimento. In più, gli FSD sono tenuti ad applicare le prescrizioni dettate dal decreto di recepimento a partire dal 24 giugno 2018, data di entrata in vigore del provvedimento, valutando la rilevanza degli incidenti sulla base dei criteri e delle soglie indicati nel Regolamento (UE) 2018/151 del 30 gennaio 2018[106]. Inoltre, i soggetti giuridici non identificati come OSE e che non sono FSD possono comunque inoltrare al CSIRT delle notifiche volontarie riguardo gli incidenti che abbiano un impatto rilevante sulla continuità dei servizi da loro erogati. Questo accade perché l'intento della Direttiva NIS, e del relativo decreto di recepimento, è quello di favorire la più ampia diffusione di una consapevole cultura nel campo della cybersecurity e di un conseguente accrescimento dei relativi livelli di sicurezza, anche attraverso un maggiore scambio di informazioni[107].

In riferimento al *Computer Security Incident Response Team* italiano, esso è stato istituito presso la Presidenza del Consiglio dei ministri, nello specifico in seno al Dipartimento delle informazioni per la sicurezza (DIS), ed ha assunto i compiti del CERT Nazionale e del CERT-PA. Nello specifico, esso si occupa di definire le procedure per la prevenzione e la gestione degli incidenti informatici e di ricevere le notifiche di incidente, informandone il DIS, quale punto di contatto unico e per le attività di prevenzione e preparazione a eventuali situazioni di crisi e di attivazione delle procedure di allertamento affidate al Nucleo per la Sicurezza Cibernetica. Inoltre, è tenuto a fornire al soggetto che ha effettuato la notifica le informazioni utili a facilitare la gestione efficace dell'evento; informando, inoltre, gli Stati membri dell'UE eventualmente coinvolti nel suddetto incidente, impegnandosi a tutelare la sicurezza e gli interessi commerciali dell'OSE o del FSD nonché la riservatezza delle informazioni fornite. Infine, il CSIRT garantisce la collaborazione nella rete di CSIRT, attraverso l'individuazione di forme di cooperazione operativa, lo scambio di informazioni e la condivisione di *best practice.*

Le autorità competenti NIS, individuate come responsabili dell'attuazione del decreto, sono diverse ed ognuna di esse esplica funzioni in base al loro ambito di competenza. Tra queste ricordiamo il Ministero dello sviluppo economico, il Ministero delle infrastrutture e dei trasporti, il Ministero dell'economia e delle finanze ed il Ministero dell'ambiente e della tutela del territorio e del mare. Quest'ultimi vigilano sull'applicazione del Decreto ed esercitano le relative potestà ispettive e sanzionatorie; inoltre, possono predisporre linee guida per la notifica degli incidenti e dettare

[106] Gazzetta ufficiale dell'Unione europea, *Regolamento di Esecuzione (Ue) 2018/151 della Commissione del 30 gennaio 2018 recante modalità di applicazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio per quanto riguarda l'ulteriore specificazione degli elementi che i fornitori di servizi digitali devono prendere in considerazione ai fini della gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi e dei parametri per determinare l'eventuale impatto rilevante di un incidente*, 31 gennaio 2018, Testo integrale consultabile su https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32018R0151&from=IT.

[107] Sistema di informazione per la sicurezza della Repubblica, a protezione degli interessi politici, militari, economici, scientifici ed industriali dell'Italia, *La NIS in pillole*, consultabile su https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2018/06/La-NIS-in-pillole.pdf.

specifiche misure di sicurezza[108]. Per comprendere appieno la portata del fenomeno, è utile quantificarlo attraverso l'analisi dei report ufficiali. In quest'ottica, il report del DIS al Parlamento del 2018[109] riporta informazioni sull'entità e sul peso dell'attività di cybersecurity in termini di distribuzione percentuale degli attacchi alle infrastrutture pubbliche e private del nostro paese. Tra i punti salienti del documento, vi è il fatto che nel 2018 il numero complessivo di azioni ostili sia più che quintuplicato rispetto al 2017, prevalentemente a danno dei sistemi informatici di pubbliche amministrazioni centrali e locali, con una percentuale che raggiunge il 72% rispetto al totale. Il fenomeno che sta emergendo sulle PA centrali e locali esprime un fatto già rilevato anche nei report degli anni precedenti[110], ossia che le PA italiane sono molto lente nell'aggiornamento dei software e questo rende estremamente vulnerabili i loro sistemi anche rispetto a minacce più "obsolete".

In riferimento alla tipologia degli attacchi informatici, il rapporto del DIS al Parlamento[111] evidenzia come le finalità degli attacchi maggiormente rilevate siano quelle di propaganda (circa il 72,9%), mentre il puro spionaggio scende al 12%. In generale, i settori più colpiti sono quello sanitario e gli enti regionali ed i ministeri, quest'ultimi rappresentano il 63% degli attacchi subiti in Italia nel settore pubblico. Contrariamente a quanto si è verificato nel resto del mondo, l'Italia registra in generale un grado di attenzione minore verso i settori privati.

In merito alle azioni di attacco, il DIS le registra soprattutto in tre ambiti specifici. Il primo è lo spionaggio digitale, in cui le azioni si sono tradotte in sottrazione di informazioni su dossier di sicurezza internazionale e danneggiamento dei sistemi informatici di operatori nazionali ed esponenti del mondo accademico. In questo ambito, gli attaccanti si sono serviti di infrastrutture tecniche quali impiego di domini web e servizi hosting di diversa collocazione geografica andando poi a colpire figure apicali di istituzioni e settori privati. Il secondo ambito è il cosiddetto *hacktivism*, le cui azioni si sono concretizzate nella sottrazione di dati da sistemi istituzionali a danno di strutture come quelle del lavoro, sanità, sindacati, forze dell'ordine, comuni e regioni. Il terzo, di minore rilevanza rispetto agli altri, è quello che viene identificato come cyberterrorismo, in cui gli attaccanti si sono concentrati per lo più nell'operare

[108] Sistema di informazione per la sicurezza della Repubblica, a protezione degli interessi politici, militari, economici, scientifici ed industriali dell'Italia, *La NIS in pillole*, disponibile su https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2018/06/La-NIS-in-pillole.pdf.

[109] Sistema di informazione per la sicurezza della Repubblica, a protezione degli interessi politici, militari, economici, scientifici ed industriali dell'Italia, *Relazione al Parlamento 2018*, disponibile per approfondimenti e consultazione su https://www.sicurezzanazionale.gov.it/sisr.nsf/relazione-annuale/relazione-al-parlamento-2018.html.

[110] Cyber Intelligence and Information Security, Sapienza Università di Roma, Laboratorio Nazionale CINI di Cybersecurity, Consorzio Interuniversitario Nazionale per l'Informatica, *2016 Italian Cybersecurity Report*, Controlli Essenziali di Cybersecurity, Italia, Marzo 2017, https://www.cybersecurityframework.it/sites/default/files/csr2016web.pdf.

[111] Sistema di informazione per la sicurezza della Repubblica, a protezione degli interessi politici, militari, economici, scientifici ed industriali dell'Italia, *Relazione Annuale*, il testo integrale è consultabile interamente e gratuitamente su https://www.sicurezzanazionale.gov.it/sisr.nsf/category/relazione-annuale.html.

tramite azioni mirate di propaganda tramite piattaforme social[112].

Anche il Rapporto Clusit 2020[113] è utile per quantificare il fenomeno dei *cyber attacks*. Nello specifico, tra gennaio e dicembre 2019 ci sono stati in media, a livello mondiale, 139 attacchi cyber al mese, cioè il +47,8% in più del periodo 2014-2018, durante il quale la media degli attacchi mensili era invece di 94[114]. Nel 2019 sono stati messi a segno circa 1.670 attacchi informatici, dato che rappresenta un incremento del 7,6% rispetto al 2018 ed un incremento maggiore, ossia del 91.2% rispetto ai dati del 2014, con una prevalenza di minacce legate al cyber crime.

A conclusione, quello della cybersicurezza è un tema molto attuale, che necessita di una sempre maggiore attenzione, vista la sua rilevanza all'interno della vita quotidiana di ogni individuo, di ogni ente o di ogni azienda privata. La cybersecurity è, infatti, una questione di fondamentale importanza nella società odierna, sempre più digitalizzata ed interdipendente dalla tecnologia. Vivere in un mondo costantemente connesso rende necessario lo sviluppo di una consapevolezza dei suoi rischi, così come l'incremento di mezzi per difendersi, posti a disposizione degli individui, e indispensabili per una tutela dei propri dati personali e della propria vita privata.

A livello locale, è presente il Centro di Competenza in Cybersecurity Toscano (C^3T) fondato da cinque istituzioni toscane di formazione e ricerca di concerto con la Regione Toscana [Nello specifico, le Università di Firenze, Pisa e Siena, il CNR e la Scuola IMT di Lucca]. Esso coinvolge 12 diversi dipartimenti o istituti delle 5 organizzazioni, coordina attività di ricerca e trasferimento tecnologico nel campo della sicurezza informatica con l'obiettivo di informare, sensibilizzare, formare e rispondere alle esigenze dei cittadini, dei professionisti, delle piccole e medie imprese, degli enti pubblici su conoscere, comprendere e reagire alle minacce di sicurezza informatica. Inoltre, fornisce consulenza in merito ai servizi di certificazione del software e contribuisce alla predisposizione di progetti di ricerca e di trasferimento tecnologico a livello regionale, nazionale ed europeo. Il C3T supporta la Regione Toscana nella definizione dei programmi di finanziamento partendo dall'analisi dei fabbisogni di cybersecurity delle Pubbliche Amministrazioni e delle PMI Toscane; aiuta nella predisposizione di programmi di formazione, educazione e sensibilizzazione in materia di cybersecurity rivolti alle scuole, ai cittadini e alle aziende. Infine, collabora con gli atenei membri alla promozione e creazione di nuovi corsi laurea, master universitari e di dottorato in cybersecurity[115].

[112] G. Di Fusco, L. Franchina, *Le tendenze dei cyber attacchi in Italia: gli ultimi dati a confronto*, NetworkDigital360, https://www.agendadigitale.eu/sicurezza/le-tendenze-dei-cyber-attacchi-in-italia-gli-ultimi-dati-a-confronto/.
[113] Clusit, associazione italiana per la sicurezza informatica, Rapporto Clusit 2020, https://clusit.it/rapporto-clusit/.
[114] N. Pisanu, *Cyber attacchi, ecco le minacce peggiori: il report Clusit 2020*, dispobile su cybersecurity360, https://www.cybersecurity360.it/news/cyber-attacchi-ecco-le-minacce-peggiori-il-report-clusit-2020/.
[115] C3T, *Chi siamo*, in https://www.c3t.it/chisiamo/.

Degno di nota è il *Progetto Cyber*[116], finanziato da *Interreg Europe*[117], il cui obiettivo è quello di favorire la competitività delle piccole e medie imprese (PMI) attive nel campo della cybersecurity, grazie al miglioramento delle politiche pubbliche a supporto del settore. Il progetto affronta tre macro-barriere comuni, identificate a livello europeo: carenza di coordinamento degli attori regionali, frammentazione del mercato e mancanza di talenti[118].

L'ambito della cybersecurity può offrire altresì nuove occasioni anche a livello lavorativo, per questo la Regione Toscana ha completamente finanziato un'opportunità di formazione destinata a disoccupati e inoccupati per incentivarli all'ingresso nel settore della sicurezza informatica aziendale, attraverso un corso attivato da Cedit, agenzia formativa di Confartigianato Toscana, dal titolo "S*cudo, Responsabile della sicurezza informatica aziendale, esperto della protezione di data base locali e in cloud*". Nel corso delle lezioni verranno toccati argomenti come la normativa sulla sicurezza e la privacy dei dati aziendali, i rischi della connettività dell'impresa digitale, framework per la progettazione e la gestione della sicurezza digitale, prevenzione e difesa dalle minacce e dai danni dolosi e accidentali, comunicazione di rischio e comunicazione di crisi, tecnologia e laboratorio di Cyber Sicurezza, architetture e protezione dei Data base in locale e in Cloud[119].

4. Il ruolo della polizia postale

In uno scenario nel quale la continua evoluzione tecnologica influenza ogni azione del nostro vivere quotidiano, lo sforzo della Polizia Postale e delle Comunicazioni nell'anno 2019 è stato costantemente indirizzato alla prevenzione e al contrasto della criminalità informatica in generale, con particolare riferimento ai reati di precipua competenza di questa Specialità.
Il ritmo frenetico delle innovazioni tecnologiche e dei nuovi mezzi di comunicazione, conseguenti alla diffusione di Internet su larga scala e, in particolare, la progressiva diffusione di *smartphones* e *tablets* tra i minori, sono solo alcuni degli elementi che agevolano le forme di aggressione in rete verso l'infanzia e l'adolescenza, determinando, di conseguenza, un notevole incremento non solo di reati che vedono coinvolti i minori online, quali la pornografia minorile e il cyberbullismo, ma anche della diffusione di altre forme di aggressione nei loro confronti, come le condotte autolesioniste, le c.d. *challenges* (es. *Blue Whale*, *Binge Drinking*), etc. Considerato che uno degli aspetti propri del web che caratterizzano tali fenomeni, nonché tutte

[116] Regione Toscana, Agenda digitale Toscana, *Progetto Cyber*, ulteriori informazioni su https://www.regione.toscana.it/-/progetto-cyber.
[117] Interreg Europe, https://www.interregeurope.eu/.
[118] Regione Toscana, Giunta Regionale, *Rapporto generale di monitoraggio strategico 2019*, p.90, https://www.regione.toscana.it/documents/10180/23123470/RN-DEFR_6_RMS_2019.pdf/29f603fc-40e5-d619- 753b-5ba857c2e10c?t=1576136484672.
[119] MET, Notizie delle pubbliche amministrazioni della città metropolitana di Firenze, *Lavoro: arginare la disoccupazione formando nel campo della cyber sicurezza*, Opportunità gratuita di Cedit finanziata dalla Regione Toscana: 12 posti disponibili, 18 febbraio 2019, http://met.provincia.fi.it/archivio/nl1.aspx? num=5408&nm=75&anno=2019#indice.

le comunità virtuali, è l'assenza di confini e, quindi, la sovranazionalità, che implica la presenza di utenti che si connettono dall'estero con server attestati in altri Paesi, l'attività di cooperazione internazionale, instaurata nel corso degli anni dal Centro Nazionale per il Contrasto alla Pedopornografia Online (C.N.C.P.O.) tramite EUROPOL e INTERPOL, sia con paesi dell'UE, sia extraeuropei, è di assoluta importanza, in quanto consente uno scambio info investigativo, nonché di condivisione di nuove tecniche di indagine e buone prassi nella materia.

In tale contesto, risulta di assoluto rilievo il ruolo svolto dalla Polizia Postale e delle Comunicazioni, in particolare, nell'ambito dei reati relativi allo sfruttamento sessuale dei minori online e nell'impegno in campagne di sensibilizzazione e prevenzione sui rischi e pericoli connessi all'utilizzo della rete internet, rivolte soprattutto alle giovani generazioni. Nello specifico si evidenzia la settima edizione della campagna itinerante della Polizia Postale e delle Comunicazioni "*Una Vita da Social*[120]", grazie alla quale sino ad oggi sono stati incontrati oltre 2 milioni di studenti, 220.000 genitori, 125.000 insegnanti per un totale di 17.000 Istituti scolastici e 300 città italiane. Un progetto dinamico, innovativo e decisamente al passo con i tempi, che si avvicina alle nuove generazioni evidenziando sia le opportunità del web che i rischi di cadere nelle tante trappole dei predatori della rete, confezionando un vero e proprio "manuale d'uso", finalizzato ad evitare il dilagante fenomeno del cyberbullismo e tutte quelle forme di uso distorto della rete in generale e dei social network. A disposizione degli utenti è presente la pagina facebook[121] e twitter[122] di questo progetto, gestita direttamente dalla Polizia Postale e delle Comunicazioni, dove vengono pubblicati gli appuntamenti, le attività, i contributi e dove i giovani internauti possono "postare" direttamente le loro impressioni ad ogni appuntamento. Uno strumento agevole che consente al cittadino, da casa, dal posto di lavoro o da qualsiasi luogo si desideri, di entrare nel portale ed usufruire dei medesimi servizi di segnalazione, informazione e collaborazione che la Polizia Postale e delle Comunicazioni quotidianamente ed ininterrottamente offre agli utenti del web è quello del portale del Commissariato di P.S. online, divenuto il punto di riferimento specializzato per chi cerca informazioni, consigli, suggerimenti di carattere generale, o vuole scaricare modulistica e presentare denunce. Di particolare importanza sono state le denunce e le segnalazioni giunte anche sul sito del Commissariato di P.S. on- line per i reati di cyberbullismo, perpetrati soprattutto in ambito scolastico da parte di studenti nei confronti di compagni e perpetrati attraverso i social media, con atti denigratori e diffamatori nei confronti delle giovani vittime. Alcune attività sono sfociate

[120] Commissariato di P.S. online, sportello per la sicurezza degli utenti del web, "Una Vita da Social": un viaggio nella Rete senza pericoli, in Notizie su https://www.poliziadistato.it/articolo/una-vita-da-social---un-viaggio-nella-rete-senza- pericoli.
[121] https://www.facebook.com/unavitadasocial/.
[122] https://twitter.com/unavitadasocial.

nell'emissione da parte dei Questori di provvedimenti di ammonimento anche al fine di responsabilizzare minori autori del reato[123].

Nell'aprile 2018, inoltre, è stata creata una piattaforma in cui far confluire tutte le segnalazioni provenienti da banche e Forze di polizia su transazioni sospette che avvengono in Rete, in modo da poter analizzare e condividere in tempo reale ogni informazione e bloccare così le operazioni illegali. Si tratta di *European Union Online Fraud Cyber Centre Expert Network, o* "*Eu-of2cen*", un progetto ideato appunto dalla Polizia di Stato, gestito dalla Polizia postale e delle comunicazioni, e finanziato dall'Unione europea per il contrasto al cybercrime finanziario. Il suo obiettivo è duplice: dal punto di vista strategico, la partnership tra banche e Forze di polizia, con il coinvolgimento di Europol, consente di avere a disposizione in tempo reale le possibili attività criminose aggiornate sui modus operanti e sui trend degli attacchi cibernetici, con miglioramento dello scambio di informazioni; dal punto di vista più strettamente operativo ci sarà un incremento della capacità di rilevare bloccare in tempo reale le transazioni sospette, migliorando la capacità di identificazione dei gruppi criminali internazionali e anticipando le truffe attraverso l'analisi delle minacce emergenti. Solo nel 2017, grazie a Eu-of2cen, sono state bloccate transazioni, frutto di frodi telematiche commesse attraverso sofisticati strumenti informatici, per oltre 22 milioni di euro e recuperata una somma pari a 900 mila euro[124].

[123] Commissariato di P.S. online, sportello per la sicurezza degli utenti del web, *Tiriamo le somme di un'intensa attivita' lavorativa. ci consente di verificare i risultati ottenuti e, soprattutto, pianificare quello che puo' essere migliorato. la polizia postale e delle comunicazioni e' sempre con voi!*, in Notizie su https://www.commissariatodips.it/notizie/articolo/tiriamo-le-somme-di-unintensa-attivita-lavorativa-ci-consente-di-verificare-i-risultati-ottenuti/index.html.

[124] Polizia di Stato, *Cyber-security: progetto antifrode Eu-of2cen*, in Ufficio stampa, consultabile interamente su https://www.poliziadistato.it/articolo/cyber-security-progetto-antifrode-eu-of2cen.

Con l'avvento del nuovo millennio e delle tecnologie più innovative, Internet è ormai diventato parte integrante della vita quotidiana di gran parte della popolazione mondiale, rivoluzionando radicalmente il modo di vivere e di comunicare delle persone. Ecco perché nella società odierna, perennemente connessa ed irreversibilmente interconnessa, preme sempre di più una sensibilizzazione globale per un utilizzo consapevole di Internet, con l'obiettivo finale di godere dei benefici che la rete può offrire e di prevenirne il più possibile i rischi. È l'obiettivo di questo elaborato, che analizza il tema dal punto di vista europeo, nazionale e locale.

Sei interessato alle tematiche e alle opportunità Europee?
Scopri tutte le iniziative ed altre informazioni sulla pagina Facebook di Europe Direct Livorno, oppure vienici a trovare.

https://www.facebook.com/EuropeDirectLivorno/

https://www.instagram.com/europe_direct_livorno/

Europe Direct Largo del Cisternino, 13
57123, Livorno, Italia
Tel. +39 0586 824148
europedirect@comune.livorno.it

Stampa: Centro Stampa del Comune di Livorno,

COMUNE DI LIVORNO

Co-funded by the European Union