UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE POLITICHE, GIURIDICHE E
STUDI INTERNAZIONALI
Corso di laurea *Magistrale* in
Scienze del governo e politiche pubbliche

Gli atti del minore nel mondo telematico: questioni di diritto privato.

Relatore: Prof. Arianna Fusaro

Laureanda: Francesca Puppoli
matricola N. 2003349

A.A. 2021/ 2022

Indice:

Introduzione.

La presente tesi ha per oggetto la stipulazione di contratti in rete da parte dei minori e i problemi che ciò comporta. Più ampiamente, però, l'analisi si concentrerà sulle motivazioni che spingono i minori ad avvicinarsi al mondo virtuale e alle opportunità che esso può offrire, ma anche sui pericoli e i rischi che essi corrono nel mondo telematico. Le considerazioni in merito vengono svolte per fornire un affresco realistico di molteplici situazioni in cui l'utente minorenne rischia di imbattersi, nonché delle soluzioni che possono essere adottate.

Con l'avvento di Internet nasce anche un nuovo modo di stipulare contratti in maniera più veloce. La velocità di stipulazione di tali contratti va di pari passo con la semplicità delle modalità con cui possono venire conclusi. In tale elaborato verrà trattato proprio il tema della stipulazione dei contratti telematici, delle motivazioni che possono spingere a tale risultato, e ad eventuali rischi e tutele collegati appunto al fatto che uno dei contraenti sia un soggetto minore d'età. Per analizzare simili fattispecie però è necessario partire da alcune premesse quali l'analisi della posizione giuridica del minorenne.

Il divario tra velocità di evoluzione del mondo digitale e velocità della sua regolamentazione è cresciuto durante il periodo pandemico, così come il numero di utenti che utilizzano la rete e i suoi servizi per comunicare, concludere contratti di compravendita, lavorare, ma anche partecipare alle lezioni.[1] I minori non fanno eccezione, infatti nella propria quotidianità utilizzano Internet sempre più spesso, come dimostrato da uno studio Istat che ha raccolto i dati relativi al triennio 2019-2021. In tale indagine sono stati coinvolti gruppi di 100 ragazzi con le medesime caratteristiche per differenti fasce d'età, tre delle quali sono relative a minorenni, in particolare: quella dei bambini da 6 a 10 anni; quella dei ragazzi da 11 a 14; nonché quelli da 15 a 17 anni. Interessante è osservare che l'uso giornaliero della rete aumenti al diminuire dell'età: da 10 unità nella fascia 15- 17 anni a 20 nella fascia inferiore. Questi dati aiutano a comprendere la quantità di tempo crescente

[1] Fonte: dati Istat raccolti grazie all'indagine campionaria "Multiscopo sulle famiglie: aspetti della vita quotidiana - parte generale" che fa parte di un sistema integrato di indagini sociali che rilevano le informazioni fondamentali relative alla vita quotidiana degli individui e delle famiglie.

che i giovanissimi trascorrono online, e come lo trascorrono, nonché i rischi connessi alla loro navigazione in solitaria. Infatti i minorenni, durante la loro attività online, dovrebbero essere supervisionati dai genitori o chi ne fa le veci nelle loro attività, sempre nel rispetto della loro libertà di espressione e della maturità che manifestano al fine di consentire la navigazione in rete senza rischi.

In rete infatti non si può dire che i rischi manchino, e possono essere i più vari: dal cyberbullismo allo *sharenting*[2], passando per pedopornografia, *phishing*, nonché per la conclusione, consapevole o meno, di contratti online da parte dei minori, che può arrecare danni non sempre risarcibili alle finanze familiari.

Può accadere anche che nel contratto non sia il minore la parte lesa, bensì il venditore qualora il minore, per concludere il contratto, attui dei raggiri ai danni del primo. Il danno nei confronti del contraente con cui il minore conclude il contratto tramite raggiro, consisterebbe nell'annullamento del contratto stesso da parte dal giudice, comportando per il venditore l'obbligo di versare alla famiglia del minore (o a chi per essa) l'importo pagato al momento della conclusione del contratto, con la conseguente restituzione del bene precedentemente venduto. Tuttavia il contratto stipulato da un soggetto minorenne non è annullabile nel momento in cui egli lo concluda tramite raggiri, eludendo quindi le misure volte a

[2] La parola "sharenting" è nata, nel 2010, dalla fusione di "share", ovvero "mostrare" e "parenting" traducibile col termine "genitorialità". Lo sharenting quindi consiste nella condivisione pedissequa online (da parte dei genitori) di contenuti che hanno per soggetti principali i figli.

scongiurare il verificarsi di simili casi, che il venditore deve dimostrare per legge di avere adottato.

I contratti che possono portare a questo genere di inconvenienti non sono solamente quelli di compravendita stipulati dai minorenni, ma possono consistere anche in accordi che prevedono la cessione di dati personali del minore in cambio della fruizione di un servizio, come accade ad esempio in caso di iscrizione ai social network. Questi ultimi, in cambio dei servizi (di comunicazione nonché libertà di espressione) forniti, prevedono un corrispettivo che non consiste in denaro ma in una cessione dei propri dati personali, la quale comporta maggiori rischi nel caso in cui l'utente sia un soggetto minorenne. Il pericolo per il minore può derivare sia dalla sua inesperienza, sia dal comportamento dei suoi genitori, che oltre ad educarlo al corretto uso della rete dovrebbero essere consapevoli dei rischi cui si va incontro navigando online. Nondimeno, il più delle volte non solo i genitori non conoscono le attività del figlio online, ma, secondo uno studio statunitense, il 69% dei genitori ignora che i figli possano tenere nascoste le loro attività online, fatto che quasi la metà dei figli (44%) in effetti ammette di fare[3]. La restante percentuale invece si preoccupa in merito a quanto gli viene nascosto dalla prole circa le proprie azioni online. I timori vengono alimentati soprattutto dagli articoli di giornale dotati di titoli sensazionalistici sui rischi della rete e dai fatti di cronaca nera. La scrittrice boyd riguardo al contesto americano afferma*:" alla politica spesso non importa risolvere i problemi ma far sembrare che si stia facendo qualcosa per risolverli*"[4]. In Italia sicuramente ci saranno persone che possono condividere tale affermazione, soprattutto coloro che hanno perso fiducia nelle istituzioni. È vero che alcune disposizioni di legge spesso non sono precise al dettaglio, ma questo consente che possano essere applicate con riferimento a più fattispecie diverse e concrete, in modo da non lasciare indifeso il cittadino.

[3] A. La Lumia, A. Dario, "Minori, internet e social network", Giuffrè, 2021, pag. 8 e ss.; d. boyd, "It's complicated", Castelvecchi, 2014, pag. 27.

[4] d. boyd, Castelvecchi, "It's complicated", 2014, pag. 93. L'autrice fa scrivere il proprio nome e cognome in maniera stilizzata con le lettere minuscole dai tempi del liceo a seguito del divorzio tra la madre e il patrigno.

Non è questa la sede per entrare nel merito della politica né tantomeno per essere polemici: in tale elaborato il focus è puntato sulle possibili soluzioni offerte dalle istituzioni specializzate nei problemi in cui ci si può imbattere navigando in rete. Tali criticità possono essere attinenti alla privacy, al fenomeno del cyberbullismo o a quello degli acquisti online.

Non sempre tuttavia il pericolo in rete proviene dall'attività del diretto interessato. Talvolta proviene dai suoi pari, come nel caso del cyber bullismo; altre volte ancora da adulti estranei che cercano di adescarlo, o proviene da individui che modificano le foto del minore montandole in video pedopornografici creandone di nuovi che hanno per protagonista il minore stesso, ignaro almeno quanto i suoi genitori circa le eventuali molteplici possibilità offerte dal mondo del fotomontaggio. Tale pratica a volte viene resa possibile anche grazie all'ignoranza dei genitori, in quanto sono essi stessi a fornire il materiale al pedofilo di turno pubblicando online senza alcuna cautela le foto dei loro figli alimentando così il fenomeno, o meglio, i casi di condotta denominata "*sharenting*".

Per un'efficace tutela dei minori si è quindi proposto di agire su due fronti: quello di prevenzione e quello volto alla tutela e al contrasto delle condotte pregiudizievoli.
Nel primo caso si fa riferimento all'azione congiunta di scuole, istituzioni e genitori nell'informazione fornita a ragazzi e famiglie circa le opportunità ed i rischi di Internet. In particolare l'obiettivo è quello dell'educazione dei figli ad un corretto uso della rete e dell'informazione dei genitori circa gli strumenti in loro possesso per tutelare i figli pur consentendogli la libertà d'informazione e di comunicazione tutelata dall'articolo 21 della Costituzione italiana, come ad esempio l'impostazione del "*parental control*" sui dispositivi usati dai minori.
Nel secondo caso invece l'attenzione si sposta sulle norme europee e su quelle italiane di recepimento di quanto disposto dalle prime ma non solo, che si occupano di definire quali siano le condotte pregiudizievoli, in cosa consistano e come vengano sanzionate dalle autorità competenti, anch'esse ben identificate.

Capitolo 1: Il soggetto

Introduzione al capitolo 1

Nel presente capitolo vengono introdotte le figure che costituiscono i soggetti principali della tesi nonché la rete di rapporti tra loro e il mondo online: i minorenni ed i loro genitori. Entrambi vengono definiti giuridicamente e sono oggetto di una breve analisi dal punto di vista sociologico. L'aspetto giuridico è utile al fine di fornire spiegazioni circa le azioni che i minorenni possono compiere. In questo modo si potranno arrivare ad identificare eventuali illeciti commessi da minori ai danni dei propri coetanei (ma non solo) e come questi vengano gestiti dalla legge. Quindi: di chi sia la responsabilità, quali siano le condanne o le sanzioni in merito e quali siano le possibili soluzioni da adottare sia dopo che l'illecito sia stato commesso sia le misure di prevenzione adottabili per impedire a monte che avvenga il fatto che cagioni danno. I danni ricevuti dai minori tramite l'attività online non solo sono riconosciuti e sanzionati da leggi ma in un'ottica più ampia di protezione dei giovani navigatori che ne comprende la preservazione da simili esperienze attraverso misure di prevenzione che sostanzialmente si concretizzano in progetti di educazione digitale. Infatti, tra le misure di prevenzione vi sono quelle relative all'educazione dei giovani al corretto uso dei media dal momento che la Convenzione ONU dei diritti dell'infanzia ha stabilito che i minori hanno il diritto inviolabile di partecipazione ai media. Per rendere questo diritto una realtà, il legislatore italiano non ha coinvolto solamente le scuole, che pure hanno un ruolo importante, ma con il Codice Civile si dà particolare risalto alla figura dei genitori nonché alle loro responsabilità.

Tuttavia, le tecnologie attuali sono nuove non solo per i ragazzi ma anche per i loro genitori che spesso trovano difficile affiancare i primi nel loro utilizzo, e può capitare si scoraggino a vedere che i propri figli sono particolarmente abili. Ma il punto non è l'abilità che dimostrano gran parte degli appartenenti alle giovanissime generazioni, e non è nemmeno che si richieda agli adulti che si occupano di loro di divenire esperti informatici, bensì la capacità degli adulti di aiutare i propri figli minori ad essere consapevoli delle proprie azioni compiute in

internet[5]. Al genitore viene richiesto di continuare ad essere una guida per la morale del ragazzo non per le conoscenze o le competenze in rete di quest'ultimo, che in certi casi potrebbero anche essere maggiori di quelle dei genitori, ma per la morale stessa del minore. È compito quindi del genitore permettere che il figlio si avvicini al mondo virtuale facendogli capire le regole che lo compongono, le norme etiche che lo reggono, nonché la tangibilità delle conseguenze di quanto si verifica al suo interno.

I pericoli infatti ad esempio, sono molto reali e hanno conseguenze nella vita offline: è quanto accade per le vittime di cyberbullismo, che possono arrivare a modificare le proprie abitudini di vita spinte dal reale timore che possa accadere qualcosa ai propri cari o a sé stesse; oppure è ciò che accade in caso di adescamento e pedopornografia online: la vittima anche se non ha avuto un contatto con il molestatore può avvertire un senso di disagio che può trasformarsi in uno stato d'ansia generalizzato sino a raggiungere il suo manifestarsi in episodi di attacchi di panico. La caratterizzazione psico-antropologica del taglio dato a tale capitolo però non si sofferma solamente sulle conseguenze delle azioni illecite online ma a cosa spinga i giovani ad avvicinarvisi: troppo spesso non è un amore non gestito bene per la tecnologia ma una motivazione più profonda, dalla richiesta di attenzione a quella di aiuto, passando per la necessità dei ragazzi di cercare propri spazi personali. Il pericolo quindi, qualora sia online, si manifesta anche offline.

La tutela del minore da tale pericolo (con tutte le sue sfumature prese in esame in questa sede) prevede anche degli aiuti per le figure genitoriali che spesso si trovano in difficoltà innanzi a tante opportunità da esplorare (il più delle volte in maniera più lenta rispetto alla propria prole a causa di scarse competenze o del poco tempo per poterlo fare), ad esempio tramite dei software in grado di indirizzare i figli verso siti dotati unicamente di contenuti consoni all'età nonché al corretto sviluppo psicologico dei più piccoli; oppure ancora tramite progetti di educazione digitale dei ragazzi che si tengono ne vari ordini di scuole. Perché i

[5] T. Maggi, "Giovani connessioni- orientarsi con i figli nel web", San paolo edizioni, 2020, pag. 37; d. boyd, "It's complicated", Castelvecchi, 2014, pag 104.

nativi digitali possono avere anche ampie capacità, ma queste non sempre coincidono con elevati livelli di consapevolezza e maturità nel gestire al meglio le possibilità offerte dalla rete assieme ai pericoli ad essa collegati, anzi, talvolta non hanno consapevolezza nemmeno delle proprie competenze in merito alla rete e ai suoi devices. Secondo una recente indagine dell'ICILS[6], infatti, i nativi sono spesso anche analfabeti digitali[7]. I dati riportati dalla stessa, evidenziano come solamente il 2% degli studenti tredicenni, pienamente compresi quindi nella recente concezione di "nativo digitale", ha un livello alto di competenze digitali. Ma l'aspetto che mette maggiormente in pericolo i ragazzi e i bambini è la loro falsa percezione circa l'elevatezza delle proprie competenze: sul campione oggetto di studio dell'ICILS, anche se l'84% di soggetti era convinto di avere conoscenze buone o molto buone circa la tecnologia ed i suoi strumenti, a seguito di un test ben il 49% di questi era risultato possedere competenze piuttosto scarse. Ecco quindi il motivo della necessità di collaborazione tra legislatori (europeo ed italiano), scuole e famiglie nella creazione di una rete che li protegga dalle proprie errate convinzioni circa le loro competenze, dai rischi di internet e allo stesso tempo consenta loro di esplorarlo, entro i limiti posti per la sicurezza dei minori, protagonisti principali di tale tesi.

[6] ICILS è l'acronimo di "Computer, International and Information Literacy Study"

[7] L'analfabeta digitale è colui che non sa né gestire la propria presenza online né comunicare e relazionarsi all'interno della società iperconnessa, così come non riesce ad applicare il pensiero critico ai contenuti online, tantomeno ad individuare le situazioni di rischio e le soluzioni da attuare per vivere il digitale in sicurezza. Fonte: articolo "Nativi digitali: analfabetismo che non ti aspetti", G. Dotta (giornalista, caporedattore che dal 1999 si occupa di articoli e collabora con riviste strettamente legate al mondo tecnologico), 19/10/2018, dal sito Punto informatico. Questo è una testata giornalistica online gratuita in lingua italiana che dal 1996 si occupa di nuove tecnologie, internet e comunicazione gestendo anche rubriche e forum di discussione su tali temi.

paragrafo 1.1 La posizione giuridica del minore.

Prima di parlare delle autorità che si occupano di tutelare l'interesse del minore è bene definire chi egli sia e quali siano gli interessi da tutelare, nonché in quali casi meritino di essere tutelati. Anzitutto, non tutti i minorenni sono uguali innanzi alla legge: alcuni possono validamente prestare il consenso al trattamento dei dati personali, iscrivendosi così ai social networks, altri no; alcuni possono aprire un profilo online con il consenso dei genitori, altri non ne hanno bisogno; alcuni ancora possono fare annullare un contratto concluso online mentre altri non ne hanno facoltà. Diventa quindi interessante esaminare cosa determini tutte queste differenze.

Giuridicamente il minore, sino ai diciotto anni è sprovvisto della capacità di agire, come peraltro riportato all'art. 2 del Codice Civile; tuttavia, presenta una "capacità giuridica attenuata"[8] dai 14 ai 18 anni tale da permettergli, nel rispetto dei regolamenti dello Stato in cui risiede, di possedere un proprio profilo social e prestare il proprio consenso relativo al trattamento dei dati personali in maniera valida (come si richiede nel caso di iscrizione a *social network*)[9].

Antecedentemente alla normativa attuale, si seguiva quella americana denominata COPPA[10] la quale imponeva che unicamente gli enti pubblici, escludendo quindi ogni persona giuridica, potessero utilizzare e raccogliere i dati

[8] "Capacità giuridica attenuata" è un'espressione particolarmente significativa riportata nell'articolo "Minori e contrattazione, anche online" della Dott.ssa Valentina Zani del 30 marzo 2022 pubblicato sul sito db HUB. Quest'ultimo è uno studio professionale composto da commercialisti e consulenti d'impresa in costante crescita.

[9]Gli Stati europei hanno deciso di derogare in maniera differente il limite dei 16 anni stabilito dall'articolo 8 del GDPR sono:
- Croazia, Germania, Lituania, Lussemburgo, Malta, Paesi Bassi, Romania, Slovacchia, Ungheria -> 16 anni
- Grecia, Repubblica Ceca, Slovenia, Francia -> 15 anni
- Austria, Bulgaria, Cipro, Italia, Lituania -> 14 anni
- Belgio, Regno Unito, Spagna, Svezia, Inghilterra, Danimarca, Estonia, Latvia, Lettonia, Finlandia, Polonia, Portogallo -> 13 anni. B. Saetta, articolo "Minori e protezione dei dati personali", 7/ 09/ 2018, Protezione dati personali- Data Protection

[10] COPPA: acronimo di Children's Online Privacy Protection Act indica la legge degli Stati Uniti in vigore dal 2000 che si applica alla raccolta online di informazioni personali da parte di enti pubblici sui minori d'età inferiore ai 13 anni, compresi i bambini all'infuori degli USA se la società ha sede in essi. Dai 13 anni in poi, anche altre persone o entità esterne agli enti pubblici possono raccogliere dati. Dott.ssa V. Zani, "Minori e contrattazione, anche online" della 30/ 03 /2022 pubblicato sul sito db HUB; A. Astone, "Dati personali del minore in rete" A. Astone, Giuffrè Francis Lefebvre, 2019, pag. 27.

dei minori con 13 anni. In Europa invece, non era previsto espressamente un vero e proprio limite, che tuttavia era ricavabile dai quadri normativi generali.
Il primo paragrafo dell'art. 8 del GDPR[11] enuncia che il consenso digitale del minore è valido a partire dai 16 anni, derogabile fino ad un'età minima di 13 anni negli Stati Membri, per quanto concerne solo i servizi di offerta diretta basati sul consenso informato dell'interessato e non qualunque trattamento online di dati dei minori. Allo stesso tempo è previsto che qualora il minore abbia compiuto 16 anni, il medesimo tipo di consenso sia valido se dato dai genitori del minorenne o comunque chi ne detenga la responsabilità genitoriale, in virtù dell'età stabilita dallo Stato nazionale di loro appartenenza.
Il GDPR ha stabilito che gli Stati nazionali potessero abbassare il limite d'età digitale dei 16 anni, raggiunti i quali viene ammesso il consenso dei minori per usufruire direttamente di un'offerta di servizi digitali come l'iscrizione a *social network* ed app di messaggistica. Il tutto senza la possibilità di scendere al di sotto della soglia di età di 13 anni, stabilita dal *Children Online Privacy Protection Act*, come limite minimo inderogabile per poter dare il consenso al trattamento dei dati. In Italia per esempio è previsto che l'età per prestare validamente il consenso relativo al trattamento dei dati è previsto non sia inferiore ai 14 anni.

La legislazione sul tema si è sviluppata maggiormente negli ultimi anni, conoscendo un'accelerazione riguardo alle necessità sempre maggiori che ha presentato la crescita di utenti in rete, in particolare dei più giovani e delle abilità che hanno sviluppato passando molto tempo online, nonché dei pericoli che ne minacciano la navigazione. Se infatti è vero che gli immigrati digitali hanno a difenderli una forma mentis derivante dall'epoca antecedente ai *social media* nonché *social network*[12], è altrettanto vero il fatto che ciò non vale per quelli che

[11] GDPR: acronimo di General Data Project Regulation, è il regolamento europeo 2016/679 in materia di privacy relativo alla protezione dei dati personali. Sottoscritto il 27/04/2016, pubblicato nella G.U. dell'Unione europea il 4/05/2016, è entrato in vigore il 25 maggio 2018, mentre in Italia è stato recepito con il d.lgs. n.101 il 10/08/2018.

[12] Tale modo di pensare della generazione antecedente a quella nominata di "nativi digitali", è caratterizzata dalla consapevolezza che per costruire conoscenza ci voglia del tempo, anche per assimilare i concetti; ogni notizia si era abituati a riceverla all'interno di un contesto, altrimenti non si aveva l'impressione di comprenderla. Qualsiasi domanda cerca la sua risposta in libri, parenti più anziani, non è un caso se spesso gli adulti ora parlino di "nonna" oppure "nonno" Internet nel vedere come i propri figli

vengono definiti “nativi digitali”. Questi ultimi presentano delle caratteristiche che non solo li accomunano, ma li rendono anche vulnerabili e possono venire ascritte nell’acronimo S.T.I.L.E.[13] le cui lettere stanno ad indicare, rispettivamente: socialità, trasparenza, istantaneità, libertà ed esperienza. Quest’ultima, assieme all’istantaneità, contribuisce alla necessità del ragazzo di comunicare e fornire la propria opinione senza prima acquisire quasi alcuna competenza nella materia sulla quale sta per esprimersi, rendendolo facile bersaglio di chi desidera manifestare un’opinione differente argomentandola meglio, o magari anche arrivando a toni di scherno che possono sfociare in cyberbullismo, oppure di chi vuole avvicinarlo con scopi illeciti. L’istantaneità infatti consiste nel fatto che i minori hanno necessità di comprendere impazientemente ciò che gli interessa per formulare giudizi immediati, come da loro abitudine. Tuttavia, parlando di argomenti non conosciuti e dando opinioni su essi possono non solo incorrere nei pericoli sopra descritti, ma rischiano anche di diffondere informazioni distorte. Inoltre, non esprimendosi correttamente potrebbero alimentare la disinformazione facendo passare le loro opinioni per informazioni. La caratteristica dell’esperienza invece, consiste nel fatto che i “nativi digitali”[14] vivono immersi nelle cose, autorappresentandosi in continua

d’istinto cerchino di soddisfare le proprie curiosità al volo tramite esso. Termine e concetto trattato da A. Cazzullo con R. e F. Maletto Cazzullo, nel libro “Metti via quel cellulare”, Mondadori, 2017, pag. 13.

[13] Acronimo spiegato da G. Riva, del libro” Nativi digitali- crescere e apprendere nel mondo dei nuovi media“, ilMulino, 2014, pag. 66, in cui ogni lettera indica una caratteristica propria dei “nativi digitali”. Nativi digitali vengono identificati come coloro che parlano lo stesso linguaggio digitale con caratteristiche comuni racchiuse nell’acronimo s.t.i.l.e. le cui lettere significano:

Socialità -sempre connessi, intrattengono relazioni continue anche se mediate da infrastrutture

Trasparenza -esprimono narcisisticamente, in totale libertà, la loro opinione in un circuito che esige la coerenza, pena la smentita del popolo web

Istantaneità -hanno necessità di comprendere impazientemente ciò che gli interessa e sono allenati a formulare giudizi immediati

Libertà -come condizione ordinaria

Esperienza -vivono immersi nelle cose, autorappresentandosi in continua interazione con followers e amici virtuali.

[14] Nativi digitali, insieme a immigrati digitali, è un’espressione coniata dallo scrittore statunitense Marc Prensky il quale ha svolto le attività di consulente e innovatore nei campi di educazione ed apprendimento. Entrambe le espressioni di cui sopra sono state inserite e spiegate la prima volta nel suo articolo “Digital Natives, Digital Immigrants” per il magazine “On the Horizon”, 2001. Inizialmente, il “nativo digitale” era considerato, in accordo con la definizione dell’autore, come colui che, nato dopo il 1985, sin da neonato è venuto a contatto con mezzi di comunicazione digitali nonché tutte le altre innovazioni tecnologiche fiorite copiosamente nei decenni successivi. Quindi, mentre i nativi digitali sono madrelingua a livello digitale, gli “immigrati digitali” sono coloro che si sono affacciati al linguaggio digitale

interazione con amici virtuali e followers e diviene pericolosa quando i ragazzi iniziano a considerare più importanti le amicizie virtuali rispetto alle amicizie reali con persone che conoscono in carne ed ossa. Il pericolo nasce dal fatto che, il più delle volte, gli utenti non possono essere sicuri che i loro nuovi amici di chat siano chi dicono di essere ed i malintenzionati sono abilissimi a selezionare le loro vittime, a coccolarle con il processo *grooming*, per poi fargli fare ciò che più desiderano trasformandosi da confidenti ad aguzzini.

Senza contare che a volte i falsi amici online altro non sono che abili truffatori, pronti a carpire quante più informazioni possibili sulla vittima e la sua famiglia al fine di *hackerare*[15] dispositivi multimediali, impossessarsi di immagini private, dell'importo del conto in banca, o più semplicemente, dell'identità digitale della vittima. È qui che entra in gioco la possibilità per il minore ultraquattordicenne di richiedere, al gestore del sito internet o del social, la rimozione dei contenuti pregiudizievoli che lo riguardano come riportato nella legge 29 /2017[16].

Per scongiurare anche queste evenienze sarebbe auspicabile la costruzione di una cultura digitale[17] che consenta a tutti gli utenti di aumentare la conoscenza delle tecnologie digitali nonché quelle legate ai pericoli della rete affinché ognuno possa autodeterminarsi e sviluppare le proprie potenzialità. Il processo di educazione civica digitale[18] non dovrebbe avere per destinatari unicamente i più giovani ma sarebbe necessario si rivolgesse anche agli utenti adulti per fornire loro strumenti tali da consentirgli una navigazione in rete sicura, e da poter essere

in un'altra fase di vita, molto successiva a quella neonatale dei cosiddetti "nativi". V. Lavecchia, articolo "chi sono i nativi digitali? Quali sono le loro caratteristiche?", altrevista.org .

[15] Hackerare, secondo la definizione riportata sul dizionario Oxford languages, significa "violare un sistema informatico per danneggiarlo o acquisire informazioni riservate".

[16] La L. 29 maggio 2017, n. 71, Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo, pubblicata in Gazzetta Ufficiale il 3 giugno 2017. Entrata in vigore il 18 giugno 2017.

[17] Cultura digitale: processo necessario da avviare che consenta a adulti e minori di aumentare la conoscenza delle tecnologie digitali/ pericoli della rete affinché possano autodeterminarsi e sviluppare liberamente le loro potenzialità.

[18] Educazione civica digitale: modalità e tipologia di educazione che rende necessario il coinvolgimento di tutte le generazioni di utenti che si avventurano online, fondamentale per utilizzare consapevolmente la rete senza finirvi intrappolati. È l'educazione da dare ai nativi digitali per consentirgli di navigare in maniera sicura nel mondo virtuale immateriale e molto pericoloso. Lo scopo quindi è quello di consentire ai ragazzi di navigare liberi e nello stesso tempo protetti grazie anche al controllo familiare. C. Cernicchiaro, "La sicurezza online dei minori in rapporto all'età del <<consenso digitale>>", Altalex, 18/12/2020.

a propria volta delle guide affidabili per i ragazzi. Questi ultimi, in uno studio americano hanno dichiarato copiosamente di aver avuto più volte avuto necessità di un consiglio circa la propria attività di navigazione online ma di non aver trovato genitori supportivi[19]. Per non parlare dei genitori contrari al fatto che i figli abbiano un'attività online a prescindere, demonizzandola e condannando qualunque riferimento ad essa, con l'unico risultato di lasciare avventurare i propri figli da soli in un mondo che per quanto virtuale presenta pericoli assolutamente reali. Il minore infatti, spesso non desiste dall'intento di accedere al mondo online e non è certo a corto di occasioni per farlo, anche se i genitori glielo dovessero proibire. È innegabile d'altra parte che le TIC[20] abbiano accentrato l'attenzione su di sé anche grazie al fatto che hanno creato occupazione e benessere economico dal momento che incentivano innovazione e creatività.

L'educazione civica digitale, servirebbe proprio a consentire una navigazione più sicura possibile, consentendo agli utenti di apprezzare tutte le possibilità che il mondo virtuale può offrire, compresi i servizi della società dell'informazione, ovvero qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, a richiesta individuale di un destinatario di servizi.

Il tutto senza rimanere imbrigliati nelle reti di qualche malintenzionato, né di qualche multinazionale o azienda che fa parte degli "*over the top*[21]" che si serve dei dati personali dell'utente per offrirgli servizi mirati sulla base delle tracce che lascia attraverso la sua attività online bombardandolo di pubblicità.

[19] Come indicato da A. Lumia, A. Dario, "Minori, internet e social network", Giuffrè editore, 2021, pag. 7.

[20] TIC: tecnologie dell'informazione e della comunicazione, identificabili come l'insieme di metodi e tecniche per trasmettere, recepire ed elaborare informazioni. A. Lumia, A. Dario, "Minori, internet e social network", Giuffrè editore, 2021, pag. 8 e ss.

[21] "Over the top" (OTT), sono le imprese che tramite la rete forniscono servizi, contenuti nonché applicazioni che fatturano grazie alla vendita di servizi, spazi pubblicitari, o contenuti ad utenti finali tramite concessionari, senza che l'azienda in questione debba pagare costi di trasmissione ovvero gestione della rete. Per il fatto di agire al di sopra delle reti vengono indicate con tale acronimo che letteralmente verrebbe tradotto in modo assai evocativo con l'espressione "oltre la cima". Il loro potere è potenzialmente enorme dal momento che detengono un'enorme mole di dati e sono assolutamente interessate al fenomeno dei Big Data tanto che il rapporto che hanno con i loro utenti è fortemente sbilanciato a causa dell'asimmetria tra i dati che forniscono gli utenti per navigare o con la navigazione stessa e quanto questi ultimi sanno circa la raccolta nonché l'uso che ne verrà fatto. A. Astone, "I dati personali del minore in rete- dall'internet delle persone all'internet delle cose", Giuffrè, 2019, pag. 5 e ss.; AGCM.

Quando si parla di "*over the top*", si fa riferimento alla definizione data da Manuel Castells[22] per indicare i soggetti privati che hanno beneficiato di notevole libertà nelle loro attività online, resa possibile dalla difficoltà del legislatore di regolamentare velocemente i cambiamenti tipici dei nuovi mezzi di comunicazione. Sono soggetti privati come questi a rivestire un ruolo egemone nell'apparente democraticità dell'agorà virtuale e a servirsi dell'illusione di uguaglianza e orizzontalità che essa dona ai suoi utenti. Illusione, poiché ogni utente è libero di usare la rete liberamente, facendo valere e condividendo le proprie idee e opinioni, costruendo inoltre attorno a sé (con l'ausilio, spesso non conosciuto, degli algoritmi dei social) un gruppo di sostenitori per effetto del meccanismo di creazione delle "*echo chambers"*[23]. Tuttavia è altrettanto vero che questa illusione di orizzontalità altro non fa che alimentare la asimmetria, tra utente e multinazionali del web, sia di potere economico, sia di informazioni. Sono proprio queste ultime a generare la vulnerabilità degli utenti, che si amplifica maggiormente nel caso in cui siano inesperti, troppo fiduciosi verso interlocutori sconosciuti, e soprattutto, nel caso di utenti minori d'età.

Il sistema giuridico diventa quindi un'importante risorsa per i minorenni, dal momento che serve a garantire equilibrio tra libertà e controllo. Gli utenti infatti, sono liberi di esprimersi e di accedere alle informazioni di loro interesse, mentre il controllo si riferisce all'uso dei dati degli utenti che vengono raccolti da quelle che Stefano Rodotà ha definito come "*strapotenti società multinazionali*" riferendosi a Google, Microsoft, Facebook in quanto acquisiscono continuamente

[22] Castells Olivàn Manuel è un sociologo spagnolo naturalizzato statunitense che nelle opere in cui espone la propria teoria integrale dell'informazione si riferisce alle grandi aziende perlopiù americane con l'espressione "Over the top". La sua teoria infatti non tratta solamente dell'aspetto culturale ma anche di quelli politici ad economici ad essa collegati in un processo ciclico d'influenza tra gli stessi. Fonte: Enciclopedia Treccani online.

[23] "Echo chambers": letteralmente "camere dell'eco", sono delle "camere virtuali" in cui ogni utente trova ciò che è di suo interesse ed in linea con le idee che ha già manifestato durante la navigazione, inoltre entra in contatto con altri utenti simili a lui per questi aspetti. I social network hanno questo meccanismo quasi automatico che sulla base del proprio algoritmo mettono in contatto persone che si muovono in maniera simile sui social e su questo meccanismo si rinforzano i contatti tra tali persone che forti del fatto di essere in gruppo a condividere idee simili le reputano come corrette evitando il dialogo per un eventuale confronto perché non disposte ad adottare un punto di vista diverso dal proprio. W. Quattrociocchi, A. Vicini, "Misinformation – Guida alla società dell'informazione e della credulità", FrancoAngeli, 2016, pag. 92.

un'enorme mole di dati personali che utilizzano per i più diversi scopi[24]. Il legislatore ha provveduto in tal senso con l'articolo 7 del GDPR dove viene stabilito il principio di finalità, ovvero: il trattamento dei dati personali deve essere necessario nonché calibrato sugli scopi da perseguire che sono stati indicati prima che l'utente presti il proprio consenso.

D'altro canto, non basta che il minore abbia l'età prevista dalla legge per poter legittimamente prestare il consenso. In base a quanto stabilito dalla commissione del lavoro del 2009, è prevista la responsabilità del titolare del trattamento circa la verifica dei requisiti che rendano valido il consenso prestato. Inoltre, l'articolo 12 del GDPR prevede che il trattamento dati venga strettamente legato al servizio erogato e comunicato in maniera chiara e comprensibile al minore che sta per sottoscrivere il contratto; il tutto nell'interesse dell'utente minorenne (*Best interest of child*).

È il medesimo interesse che ha mosso il Ministero delle comunicazioni a fare in modo che venisse sottoscritto dalle principali emittenti televisive il Codice di regolamentazione TV e minori, nel febbraio 2003. Questo codice è stato adottato allo scopo di garantire una gestione delle programmazioni attenta alle fasce orarie dei telespettatori, con una particolare attenzione per i minorenni e la loro fascia d'età che va dagli zero ai quattordici anni.

L'articolo 40 del GDPR infatti prevede che il titolare del trattamento dei dati debba obbligatoriamente adottare il codice di condotta che garantisca la trasparenza sul trattamento dati. È anche vero che il WP29[25] ha ricordato che non sono necessarie tecniche troppo invasive per accertare la validità del consenso per un trattamento che non comporti gravi rischi per le persone. Tuttavia la guida da seguire è costituita dall'articolo 7 del GDPR, secondo il quale la prestazione di

[24] A. Astone, "I dati personali dei minori in rete- dall'internet delle persone all'internet delle cose", Giuffrè, 2019, pag. 25 e ss.

[25] WP29 è l'acronimo dell'art.29 del Working Party che stabilisce la non necessarietà di adozione di tecniche troppo invasive al fine di accertare la validità del consenso qualora il trattamento non comporti gravi rischi per le persone. V. Zani, "Minori e contrattazione, anche online", dbHUB, 31/03/2022. L'altro nome con cui l'acronimo è conosciuto è quello di direttiva europea 95/46 che è stata sostituita dall'European Data Protection Board, ovvero un gruppo di lavoro comune delle autorità nazionali di vigilanza e protezione dati. B. Saetta, "Protezione Dati personali14/06/2018 (ultima modifica nel 2020).

servizi è condizionata dalla prestazione di un trattamento dei dati, che costituiscono il prezzo per accedere ai contenuti digitali. I dati sono costituiti in una sorta di rete di informazioni relative all'utente e alle tracce informatiche che lascia online e ne compongono il corpo informatico[26], maggiormente soggetto a rischi se appartenente a un nativo digitale piuttosto che ad un immigrato digitale.

paragrafo 1.2 I genitori o tutori del minore e la responsabilità genitoriale.

Dal momento che si suppone i minori non siano in grado di codificare criticamente un messaggio, si rende indispensabile il controllo presente ed attento dei genitori o di chi ne fa le veci. Dopo avere definito quindi chi siano i minorenni e averli distinti in base a quali azioni possano compiere legalmente, è tempo di dedicare l'attenzione a chi si occupa di loro; in particolare, tutori o genitori. I tutori sono le persone designate nella cura dei minori da parte del genitore che per ultimo ha esercitato la potestà per testamento, atto pubblico, o per scrittura privata autenticata[27]. L'importanza di un adulto a fianco del minore, viene dettata dall'inesperienza e dall'ingenuità di quest'ultimo, che viene tutelato anche a livello legale con molteplici strumenti: uno di questi è il Codice di autoregolamentazione per i servizi Internet. Elaborato dall'AIIP[28], all'art 4, lett. c, prevede i principi di tutela della dignità umana e dei minori: "*La protezione dei minori impone il rifiuto di tutte le forme di sfruttamento, in particolare quelle di carattere sessuale, e di*

[26] Per corpo informatico si intende un secondo corpo che coesiste con quello fisico della persona, composto dalle informazioni che lascia la nostra attività online in forma di tracce informatiche. A. Astone, "I dati personali del minore in rete- dall'internet delle persone all'internet delle cose", Giuffrè, 2019, pag. 5 e ss.

[27] Fonte: Codice Civile italiano.

[28] AIIP: acronimo dell'Associazione Italiana Internet Provider nata nel giugno 1985 quasi insieme alla rivoluzione di Internet che ha avuto luogo in Italia. Essa è stata generata dall'aggregazione di piccoli e medi operatori che si occupano di garantire la copertura della rete su tutta la Penisola accomunati da 4 principali obiettivi: "

- La definizione e la diffusione di standard qualitativi e regole di comportamento nell'ambito dell'offerta Internet
- La promozione della rete Internet come strumento produttivo ed efficace per le aziende come per gli utenti residenziali
- Il coordinamento di iniziative di ricerca di interesse comune per gli Associati, su argomenti tecnologici e di mercato
- L'istituzione di rapporti con organizzazioni internazionali con simili finalità"

Fonte: sito ufficiale dell'associazione aiip.it

tutte le comunicazioni ed informazioni che possono sfruttare la loro credulità; il rispetto della sensibilità dei minori impone inoltre cautela particolare nella diffusione al pubblico di contenuti potenzialmente nocivi".

Solitamente, sono proprio i responsabili dei minorenni quelli identificabili come immigrati digitali[29]. Da un lato, sono meno vulnerabili dei più piccoli ai rischi della rete, qualora siano abbastanza maturi da mettere in dubbio ogni notizia letta, dall'altro, il più delle volte, non hanno dimestichezza con i *media devices*[30]. Questo può portare a differenti tipi di conseguenze, a seconda che siano consapevoli o meno delle proprie competenze nel mondo virtuale: dal genitore che si rifiuta di imparare e demonizza a prescindere questo mondo, cercando di conseguenza di impedire al figlio di accedervi; a quello che ritiene di essere abbastanza competente sia in materia, sia circa le attività online del figlio; passando per quello che non si pone il problema e una volta online, solo perché vede un contenuto condiviso, scambia opinioni altrui (spesso prive di qualsivoglia base di conoscenza) per informazioni attendibili. I genitori, secondo l'autrice Tamara Maggi, possono essere distinti in tre tipologie in base al proprio atteggiamento verso il mondo digitale e le sue potenzialità; in particolare essa distingue i genitori in:

- Analogici;
- Migranti digitali;
- Digitali.

I primi riconoscono di non avere dimestichezza col mondo digitale, lo guardano con diffidenza e vedono nel divieto al relativo utilizzo la soluzione più efficace per dormire sonni tranquilli.

I secondi ed i terzi non solo non ne vietano l'uso ai propri figli, ma sono in prima linea sempre connessi, anche se con competenze differenti.

---

[29] "Immigrati digitali" termine coniato da Marc Prensky nell'articolo del 2001 (vedi nota n.8) anche se la sua spiegazione completa viene fornita in un articolo uscito 8 anni dopo dal titolo "H. sapiens digital: from digital immigrants and digital natives to digital wisdom" attraverso un confronto tra le differenze che intercorrono fra nativi ed immigrati digitali. Il confronto principalmente non si basa sull'età, bensì sulla saggezza digitale: il nativo digitale infatti, anche se abile, non sempre è anche saggio e la saggezza è data dalla sua capacità di fare un uso appropriato della tecnologia.

[30] Strumenti digitali che consentono di collegarsi alla rete: degli esempi possono essere pc, tablet, smartphone, notebook, iPad.

I genitori "migranti digitali" ricorrono spessissimo ad internet, possiedono anche profili social con cui pubblicano foto di famiglia talvolta imbarazzanti per i figli, i quali a volte li accusano di avere sempre il telefono in mano e di dare il cattivo esempio; i genitori digitali (o *digital parents*) invece sono definiti come utenti modello che hanno il difficile compito di trovare un equilibrio tra essere guide autorevoli e allo stesso tempo dei genitori che danno fiducia rispettando lo spazio dei figli.[31]

Si renderebbe quindi necessario educare in primis i genitori oppure i tutori all'uso corretto della rete, a riconoscere i pericoli che essa cela, non solo per intervenire in prima persona finché i figli non sono in grado di difendersi da soli, ma anche per renderli delle valide guide che possiedano le competenze di insegnare ai minori sotto la loro tutela a rendersi autosufficienti e in grado di sfruttare al meglio le opportunità che il mondo online offre.[32] In uno studio condotto negli Stati uniti molti ragazzi hanno dichiarato che più volte nel corso della loro attività online avrebbero preferito fare riferimento alle competenze di un adulto della famiglia, ma non trovando dei genitori aperti al dialogo o con le competenze necessarie hanno dovuto fare fronte alle proprie necessità in maniera autonoma.[33] Prima di concedere al figlio uno strumento che gli funga da porta d'ingresso sul mondo online, il genitore dovrebbe prima accertarsi di avergli impartito una buona educazione: l'utenza online non è esente da sconosciuti come quelli che si potrebbero incontrare per strada, ecco quindi che nasce la necessità che il minore sappia distinguere chi siano gli amici, chi i conoscenti e come comportarsi con gli estranei; così come è opportuno che sia in grado di gestire le proprie emozioni nonché di esprimersi educatamente. Inoltre, non meno importante è che i ragazzini siano consci che tutto ciò che viene condiviso nel mondo virtuale resta rintracciabile, indelebile, e genera conseguenze: si rende pertanto urgente la necessità della loro conoscenza circa quali contenuti sia opportuno condividere e quali meno.

---

[31] T. Maggi, "Giovani connessioni- orientarsi con i figli nel web", San paolo edizioni, 2020, pag. 102.

[32] A. Cazzullo con R. e F. Maletto Cazzullo, "Metti via quel cellulare- un papà, due figli, una rivoluzione", Mondadori, 2017, pag. 84 e ss.

[33] A. La Lumia e A. Dario, "Minori, internet e social network", Giuffrè, 2021, pag. 10 e ss.

La stessa Commissione parlamentare per l'infanzia ha riconosciuto la presenza di problemi ed esigenze tra i giovani e la rete, operando un distinguo tra quelle dei bambini e quelle degli adolescenti, e proponendo come forma di prevenzione al pericolo dei corsi di educazione al linguaggio degli strumenti multimediali.
La maggiore competenza dell'adulto di riferimento dovrebbe consentirgli di fare fronte al proprio dovere d'impartire al minorenne un'adeguata educazione all'uso dei mezzi di comunicazione, nonché di compiere un'attività di vigilanza sul minore per quanto concerne il suddetto utilizzo, secondo quanto stabilito da una pronuncia del Tribunale di Caltanissetta del 8/ 10/ 2019[34].
Il fatto di aver impartito una corretta educazione al figlio diviene fondamentale, se dimostrato in sede di giudizio, per permettere al genitore di sottrarsi alla responsabilità genitoriale[35], nonché all'accusa di culpa in educando, qualora riesca a dimostrare anche di aver vigilato adeguatamente sul figlio che, al momento della conclusione del contratto era incapace di intendere e di volere.
Altra fattispecie concerne la capacità del genitore di sfuggire all'accusa di culpa in vigilando: in questo caso è necessario che il genitore o tutore dimostri di non aver potuto impedire il fatto compiuto dal minore, come stabilito dall'art. 1427 del codice civile.[36]

[34] Sentenza del tribunale di Caltanisetta in merito ad un caso di bullismo. La fattispecie concreta ha consistito in molestie da parte di un minore in concorso con altri, ai danni di una loro coetanea arrivando a causarle un permanente stato di ansia e paura, costringendola a cambiare le proprie abitudini di vita poiché preoccupata per l'incolumità propria e dei suoi cari. In sede di giudizio il molestatore e la propria madre hanno dimostrati di aver compreso la gravità della condotta posta in essere e manifestato l'intenzione di non fare più accadere tali circostanze incresciose. Il Tribunale pertanto esprime la necessità dell'educazione in quanto prezioso strumento per la tutela dei minori: l'uso di internet da parte di tali giovani utenti, per quanto digitalmente abili, li espone a rischi che l'educazione e la vigilanza poste in essere dai genitori dovrebbero consentire quantomeno a minimizzare. L'educazione inoltre deve essere finalizzata ad un uso corretto delle opportunità della rete, e consapevole delle conseguenze cagionate dalle azioni compiute online, che hanno ripercussioni sulla vita offline delle persone che coinvolgono. È compito del genitore vigilare sulle attività online del figlio nonché sull'acquisizione dei valori impartiti allo stesso di genitori ottemperando ai doveri posti dalla propria responsabilità genitoriale. Inoltre, nella sentenza viene fatto riferimento alla giurisprudenza circa cosa si intenda per dovere di vigilanza dei genitori, ovvero una limitazione non solo qualitativa ma anche quantitativa dell'accesso in rete da parte dei minori sotto la loro tutela. L'esito di tale processo tenutosi presso il Tribunale di Caltanisetta ha visto l'affiancamento dei Servizi Sociali locali competenti in materia alla madre del cyberbullo per verificarne le capacità educative e di vigilanza proprie di quest'ultima.
[35] Art 2048 Codice Civile.
[36] A. Astone, "I dati personali del minore in rete- dall'internet delle persone all'internet delle cose", Giuffrè, 2019, pag. 50 e ss.

Questi sono i due metodi principali a disposizione del genitore per sfuggire all'accusa di *culpa in vigilando* e *culpa in educando*[37], che non consentirebbero l'annullamento del contratto concluso tra il minore e il venditore, a questo punto da definirsi truffato.

In base all'articolo 1425 del codice civile infatti, un contratto è annullabile se una delle due parti era incapace di contrarlo ed in questo caso il minore risponde perfettamente alla descrizione di soggetto incapace di contrarre. È da tenere bene a mente però, che la possibilità del minore ultraquattordicenne di stipulare un trattamento dei dati che gli consenta di avere un proprio profilo social, non si estende anche alla stipulazione di contratti di compravendita online. Nel caso in cui un minore adotti questa condotta, il contratto risulta annullabile in virtù degli articoli 1425, 1427, 1428 del codice civile già citati, esistono tuttavia fattispecie particolari che non rendono possibile tale soluzione.

L'art. 1425 del codice civile, infatti, si occupa di disciplinare questa eventualità, prevedendo che il contratto non sia annullabile qualora il minore abbia occultato la sua età con raggiri. Questo ultimo termine è stato al centro di numerose discussioni, in quanto non esiste nessuna norma che specifichi a cosa faccia riferimento in maniera puntuale; l'unica certezza è che nel caso il minore si dichiari maggiorenne per poter concludere il contratto, non sta ponendo in essere un raggiro[38]. Questo viene stabilito dal momento che spetta all'altro contraente verificare l'identità dell'acquirente, con le metodologie più diverse allo scopo di

[37] Culpa in vigilando indica la colpa del genitore oppure del tutore per non essere riuscito ad educare il figlio impartendogli i valori necessari alla convivenza civile in uso presso la loro società. Tale espressione è strettamente collegata alla responsabilità genitoriale, che nasce nel momento in cui si diventa genitori, e consiste nell'imputabilità genitoriale in caso di danno causato dai figli minori non emancipati o dai conviventi soggetti a tutela. L'esonero dalla responsabilità avviene se il genitore riesce a dimostrare di non aver potuto impedire concretamente il fatto che ha causato danno. La culpa in vigilando invece, è la colpa, relativa ad un fatto illecito compiuto dal soggetto su cui si doveva vigilare, che consegue dalla mancanza di sorveglianza nei casi in cui questa rientri espressamente nei propri doveri di responsabilità oggettiva. Il soggetto che rende necessaria la sorveglianza sulle sue azioni solitamente è una persona reputata non in grado di rendersi conto delle proprie azioni in maniera completa. Da notare è che questo tipo di colpa non è sempre e solo dei genitori o tutori dei minori ma più in generale di tutti coloro a cui questi ultimi sono stati affidati su cui, in vista dell'età e della potenza degli strumenti tecnologici nelle loro mani, si rende necessaria la sorveglianza. Fonti: artt. 20148, 2049, 2947 Codice Civile; A. Astone, "I dati personali del minore in rete- dall'internet delle persone all'internet delle cose", Giuffrè, 2019, pag. 50 e ss; T. Maggi, "Giovani connessioni- orientarsi con i figli nel web", San paolo edizioni, 2020, pag. 114 e ss.

[38] Art 1426 Codice Civile.

accertarsi che sia giuridicamente capace di concludere il contratto. Non sono insoliti i casi in cui i minorenni riescono ad impossessarsi delle informazioni necessarie per acquistare prodotti e servizi online, come, ad esempio, i codici delle carte virtuali associate ai conti bancari dei genitori. Qualora ciò comporti un pregiudizio economico alla famiglia, o più semplicemente, un genitore manifesti il disappunto sull'acquisto fatto, può richiedere l'annullamento del contratto in virtù dell'articolo 1425 del codice civile. A quel punto il venditore potrebbe opporsi, in quanto non può o non vuole restituire il denaro guadagnato facendo appello alla *culpa in vigilando* e *in educando* dei genitori del minore autore dell'acquisto. Per superare il problema del minore che si appropria dell'identità digitale di uno dei genitori o del proprio tutore, il venditore potrebbe intensificare il livello di controllo dell'identità degli utenti per non incorrere in annullamenti indesiderati di contratto.

Negli Stati Uniti, ad esempio, si usa un sistema di riconoscimento facciale: qualora un acquirente stia facendo un acquisto online, la piattaforma richiede l'inserimento del documento di identità e un selfie scattato al momento, per accertarsi della sua identità.[39]

Tuttavia, un sistema più efficace deriverebbe dalla consapevolezza del ragazzo circa quello che può e non può compiere online; questa consapevolezza gli sarebbe utile per autodeterminarsi, anche in virtù di quanto gli viene spiegato a riguardo. Sarebbe importante per il minore avere delle figure di riferimento competenti, non solo a scuola, per quanto siano importanti i progetti didattici che prevedono una maggiore informazione dei ragazzi circa rischi e opportunità del mondo virtuale; ma anche a casa, con dei genitori in grado di affiancarlo e di dargli il loro supporto. Anche e soprattutto qualora sia necessario un acquisto online, facendo vedere al minorenne che solo l'adulto può farlo, ma che non gli

[39] In vigore dal 2015, anno a partire dal quale i genitori possono manifestare il proprio consenso all'accesso ai servizi online da parte dei propri figli minorenni grazie ad un sistem di matching tra foto personale identificativa e un selfie scattato tramite smartphone. A. Astone, "I dati personali del minore in rete- dall'internet delle persone all'internet delle cose", Giuffrè, 2019, pag 57 e ss. Il riconoscimento facciale è considerato la nuova frontiera del marketing sia dal versante digitale, dal momento che consente di vedere se il viso di chi sta pagando online con una carta di credito ne è l'effettivo proprietario, sia dal punto di vista fisico con implicazioni relative alla sicurezza nonché al controllo in tempo reale della soddisfazione dei clienti. R. Mantovani, articolo online "Il supermercato ti riconosce dalla faccia ", Focus, 23/04/2017.

preclude la possibilità di fare acquisti anche in base alle sue necessità, pertanto il ragazzo invece di compiere un illecito può tranquillamente fare affidamento sui genitori.

In questo modo, gli adulti responsabili del minorenne dovrebbero riuscire a fare acquisire al minore la conoscenza relativa al corretto utilizzo della rete e sviluppare un'etica relativa ad esso. Non si sta parlando quindi solamente di abilità informatiche ma soprattutto di educazione civica alle norme di buona condotta da rispettare anche nel mondo virtuale, nonché delle competenze circa le conseguenze legali di ogni azione compiuta online. Tale tipo di cultura civica digitale è utile che venga trasmessa alle giovani generazioni dal momento che è proprio sui loro genitori o tutori che ricadrebbero alcune responsabilità; ad esempio quelle dei contratti online stipulati dal figlio in virtù del concetto di *parental responsibility*. Per rendere questa educazione una realtà in grado di tutelare gli utenti minorenni, i loro genitori, ed i professionisti, è necessario tuttavia che anche i responsabili dei minori facciano parte della cultura digitale utile a conoscere e comprendere la realtà virtuale e a consentire ai genitori di farglici avvicinare in tutta sicurezza i propri figli.

Particolare attenzione meritano gli oggetti che consentono di collegarsi online, tra cui anche i giocattoli. Spesso dedicati ai più piccoli, vengono trovati accattivanti anche dagli adulti che li regalano, magari con l'intento non solo di intrattenere i più piccoli, ma anche di avvicinarli in maniera giocosa alla rete. Una rete in cui potrebbero rimanere imbrigliati comunque. È stato questo il caso degli acquirenti di una bambola nel 2016. La bambola in questione si chiamava Cayla[40], e l'agenzia federale tedesca aveva disposto il suo ritiro dal commercio e la sua distruzione o quantomeno la disattivazione da parte dei proprietari, in quanto celava un sistema di trasmissione, vietato dalla legge tedesca, che raccoglieva illecitamente i dati dei bambini e li trasmetteva ad una società privata autrice dell'applicazione che accompagnava il giocattolo (*Nuance Communications*). Inoltre, possedendo un microfono collegabile via *bluetooth*

[40] Il caso è presentato da A. Astone, nel saggio "I dati personali del minore in rete- dall'internet delle persone all'internet delle cose", Giuffrè, 2019, pag. 93.

con qualsiasi *smartphone* nel raggio di 10 metri, le si imputava il fatto che qualsiasi estraneo avrebbe potuto ascoltare quanto dicevano i bambini o addirittura entrarvi in contatto parlando attraverso la bambola, come successo in alcuni casi. Per quanto accattivante e utile quindi, anche l'*internet of things* (IoT)[41] può presentare risvolti pericolosi, proprio perché oggetti diversi dal nostro pc o dal nostro *smartphone*, potrebbero raccogliere i nostri dati anche a nostra insaputa, come nell'esempio della bambola sopra citata.

È positivo dunque che gli adulti si dimostrino interlocutori comprensivi verso i minori che manifestino curiosità e volontà di avvicinarsi al mondo virtuale, tuttavia è bene non eccedano neanche in questo senso e che l'avvicinamento sia graduale. Capita ancora troppo spesso che i titolari della responsabilità genitoriale siano i primi a fare bruciare le tappe ai propri figli ad esempio non facendo loro rispettare il limite d'età riguardo all'iscrizione ad un'app di messaggistica piuttosto nota, come Whatsapp. Anche per questa, l'età minima che per legge ne consente l'utilizzo sarebbe di 16 anni, ma i genitori permettono anche ai figli con meno anni di usare l'app, sentendosi abbastanza tranquilli nel concedergli di esplorare le possibilità della chat online, primo passo per desiderare l'esplorazione di altri social, altre possibili funzionalità e così via. È anche vero che la stessa è un'applicazione gratuita e al genitore fa comodo non dover pagare gli sms e poter sempre rintracciare il figlio magari spendendo anche meno per una ricarica di cellulare che consente un certo numero (elevato) di chiamate e un certo numero di giga (che consente moltissimi messaggini e attività online). La tranquillità dei genitori sta nella familiarità che hanno con questa applicazione ormai entrata nel quotidiano di tutti, sebbene non considerino forse con l'attenzione che meritano i pericoli in agguato: tutto il mondo della rete è stato studiato per un'utenza adulta, anche se vi si affaccia un popolo sempre più

[41] IoT è l'acronimo di "internet delle cose" e indica tutti gli oggetti dotati di una connessione internet necessaria al loro funzionamento ottimale. Esse possiedono 3 principali caratteristiche: la prima è che gli oggetti o meglio, i dispositivi, siano connessi ad una rete; la seconda riguarda il fatto che la rete connette tra loro questi dispositivi in una rete cloud ed è quest'ultima ad immagazzinare in modo sicuro i dati di chi utilizza tali oggetti dotati di connessione online. L'argomento viene trattato da A. La Lumia e A. Dario, A. Cazzullo e R. e F. Maletto Cazzullo, "Minori, internet e social network", Giuffrè, 2021, pag. 70; "Metti via quel cellulare- un papà, due figli, una rivoluzione", Mondadori, 2017, pag. 188; P. Bianchi, "4.0 La nuova rivoluzione industriale", ilMulino, 2018, pag. 112.

giovane. Sicuramente per un ragazzo è molto più funzionale avere a che fare con un adulto disposto ad ascoltarlo e ad illustrargli le basi per una navigazione sicura, al posto di un genitore chiuso a qualsivoglia forma di dialogo, che neghi i bisogni e le curiosità del figlio senza nemmeno dargli una spiegazione. Sono molteplici i casi di genitori che si fanno complici dei figli circa le iscrizioni online a *social network*: è questo il caso che porta alla nascita dei *baby- influencers*. Questi ultimi infatti, sono minori cui i genitori o tutori aprono profili social e ne postano le attività, riscuotendo enorme successo dovuto all'attenzione degli utenti in rete simpatizzanti per i più giovani, in alcuni casi, proprio piccoli: si pensi che nel 2020, lo *youtuber* americano più pagato, è stato un bambino di nove anni. Il segreto del suo successo sta nei suoi video, dove scarta giocattoli, che hanno fatto il pieno di visualizzazioni facendo guadagnare nel medesimo anno alla sua famiglia ben trenta milioni di dollari. Ma il fenomeno dei *baby- influencers*[42] non è confinato solo all'America: non ha confini e persino in Italia ne abbiamo non pochi casi, anche se, purtroppo, il diritto arranca nel tentativo di regolamentarne l'attività per tutelare i gestori del profilo del *baby influencer* ed il protagonista stesso.

Questa difficoltà del legislatore a stare al passo con i tempi della rapidissima evoluzione del mondo virtuale e delle possibilità che esso offre, rende ancora maggiore l'importanza delle figure responsabili del minore dal momento che non solo si occupano della creazione nonché gestione di eventuali profili social, ma anche del minorenne sotto la loro tutela. Quando si parla di *parental responsibility*, quindi, si intende sia la responsabilità dei genitori per i contratti online stipulati dai figli, come anche la responsabilità del controllo dei mezzi che potrebbero usare i minori per compiere illeciti, ad esempio rubando l'identità di un genitore per concludere un contratto online, inserendo i dati della sua carta di credito. Ecco perché la *parental responsibility* si estende anche alla custodia della carta di credito[43]: qualora il genitore non la conservasse in un luogo sicuro

[42] "Baby- influencers": ragazzi e bambini con un proprio profilo social seguito da migliaia di followers. "Minori, internet e social network", A. La Lumia e A. Dario, Giuffrè, 2021, pag. 11.

[43] Carta di credito e bancomat sono strumenti personali che i clienti, degli istituti di credito che glieli hanno rilasciati, sono tenuti a custodire e utilizzare con adeguate diligenza e correttezza, nonché comunicando

inaccessibile al figlio, quest'ultimo potrebbe utilizzarla arrecando danni talvolta irreparabili al patrimonio economico familiare, dal momento che concludere un contratto online rubando l'identità di un adulto consiste in un raggiro tale per cui il contratto in questione non può essere annullato. Il genitore o tutore ha un "ufficio privato" che comporta poteri e doveri personali e patrimoniali da esercitare nell'interesse esclusivo del minore. In Italia come anche in Francia, il responsabile del ragazzo che violi tale diritto alla *privacy* va incontro a sanzioni pecuniarie nonché alla possibile reclusione per il periodo di un anno.[44]

Dalla suddetta forma di responsabilità deriva il parental control, che consiste nel dovere dell'adulto responsabile del loro comportamento di controllarlo, nel rispetto dell'età, le attitudini, il contesto sociale, ed il grado di educazione impartito al minorenne. Alcuni strumenti elettronici hanno anche una funzione omonima che sta ad indicare un software in grado di controllare ed eventualmente bloccare l'accesso a certe attività del bambino e di definire l'arco temporale dell'uso di pc, tv, *smartphone* e altri *media devices* a disposizione del minorenne. In questo caso, la funzione appena descritta viene impostata dal genitore sul device in uso del minore e talune app, come ad esempio youtube, non possono venire aperte né tantomeno esplorate dal minore dal momento che gli si richiede un codice di accesso che solo il genitore ha, oltre che l'indirizzo mail del genitore stesso. Anche nel caso in cui il ragazzo tenti di scaricare app sul proprio dispositivo elettronico, al genitore viene inviata una mail di conferma per consentire il *download*; qualora questa non arrivasse, il minore non può scaricare alcunché.

Il grande dilemma che sembra scuotere la comunità online riguarda proprio la necessità di garantire la libertà di informazione ed espressione, anche per i più piccoli, tutelata legalmente, così come la loro sicurezza dal rischio di imbattersi in contenuti poco consoni alla loro età. La soluzione che consenta di mantenere in equilibrio queste due esigenze ugualmente importanti, sembra essere stata

tempestivamente alla banca un eventuale uso indebito da parte di terzi; come stabilito negli artt. 7 e 12 del d.lgs. n. 11/2010.

[44] A. Astone, "I dati personali del minore in rete- dall'internet delle persone all'internet delle cose", Giuffrè, 2019, pag. 60 e ss.

riconosciuta nel sistema dei filtri. Il suddetto sistema vede la propria efficacia nel fatto di venire gestito dai genitori dei minori, che possono gestire autonomamente cosa possano vedere o meno i propri figli senza rendere necessario l'intervento pubblico, non ben accetto qualora venga attuato, come nel caso della Cina. In quest'ultimo Stato infatti, è il Governo a censurare piattaforme, programmi, e quanto concerne le attività in rete, senza dare ai privati la possibilità di eludere queste decisioni. Dal momento che in Europa, invece, i privati desiderano poter esercitare i proprio libero arbitrio, o almeno così credono, e sentono di sapere e volere scegliere autonomamente i contenuti da escludere dalla visione dei propri figli, il *software* gode di grande considerazione e sostegno in quanto riconosciuto come il modo più efficace per risolvere i problemi specifici di Internet tenendo conto delle differenze nei canoni di gusto e decenza tra paesi, comunità e famiglie.

Ad aiutare ulteriormente i genitori nel loro compito di tutela dei figli, intervengono anche servizi a pagamento che funzionano online come ad esempio: America Online; Compuserve; Prodigy; Microsoft Networks che hanno la particolarità di compiere controlli adatti alla fascia d'età selezionata che siano anche aggiornati. Anche questi ultimi sono ascrivibili alla tipologia dei software citati nel paragrafo precedente, che sono distinti in tre tipologie diverse sulla base delle modalità di funzionamento differenti: il modello di *blacklisting*, quello di *whitelisting*, ed infine quello di etichettatura neutrale. Il *blacklisting* comporta l'elencazione da parte dell'utente dei siti a cui egli intende negare l'accesso al figlio; funzionamento opposto rispetto al *whitelisting*, dove invece vengono indicati dal genitore solamente i siti cui viene concessa la navigazione al minore sotto sua tutela. L'etichettatura neutrale[45] invece, classifica i siti lasciando all'utente la decisione relativa a quali bloccare o meno.

[45] Le categorie che compongono questo sistema sono state create dall'associazione ICRA (Internet Content Rating Association) successivamente inglobata nel 2007 da FOSI (: Family Online Safety Institute), un'associazione internazionale no profit nata nel 2007 che tra i suoi obiettivi prevede il miglioramento della sicurezza relativa alla navigazione in rete per i giovani e le loro famiglie. Nel sito ufficiale FOSI.org viene riportata la mission dell'organizzazione, ovvero rendere la navigazione su web più sicura mediante:

- Collaborazioni con autorità leader dell'industria digitale
- Promozione della cultura della responsabilità online
- Diffondendo il concetto di cittadinanza digitale.

Di seguito una tabella riassuntiva dei tre modelli di software[46] appena trattati e le loro funzionalità:

	Blacklisting	Whitelisting	Etichettatura neutrale
principio	Blocca l'accesso a tutti i siti selezionati	Consente l'accesso solo ai siti selezionati	Siti classificati in categorie: sta all'utente decidere se renderli consultabili al figlio o meno
conseguenza	Se non inserito nella black list, qualsiasi sito può venire consultato	Blocca tutto ciò che non viene messo in white list	Maggiore libertà dell'utente genitore
Più usati per	Pacchetti di filtraggio a funzionamento autonomo	L'ambito scolastico	Il monitoraggio dei figli dalle famiglie

Non è richiesto quindi, che gli adulti con responsabilità genitoriale siano esperti del Web ma sarebbe utile si interessassero ad esso, si avvicinassero e ne parlassero con i figli. È difficile rimanere costantemente aggiornati nonostante le incombenze che un genitore deve fronteggiare nella vita quotidiana ma il punto è proprio questo: il genitore non è solo, come lui ce ne sono tanti altri alle prese con web e competenze superiori, reali o presunte, dei figli.

[46] "Software": programmi informatici eseguibili dal computer, ne costituiscono la parte astratta ed immateriale a livello logico. Fonte: "enciclopedia Treccani" online.

Un altro strumento tanto utile quanto importante è la *peer education* tra gli stessi genitori: la condivisione di difficoltà, sensazioni, conoscenza di risorse che può avvenire attraverso *community online* come la Genitori Digital[47]: nata come amicizia, solidarietà e scambio di informazioni tra l'autrice[48] e altri genitori è sbarcata in rete, dando vita a *digital coffee* e incontri offline che si diffondono, rafforzano i legami tra chi ne fa parte e sono magnifiche occasioni formative con scambi di informazioni e opinioni tra educatori, genitori ed esperti in materia.

paragrafo 1.3 Il profilo psicologico del minore e i meccanismi utilizzati per ottenerne informazioni (riservate).

Data l'ingenuità del soggetto minorenne, si rende necessario che sia affiancato da figure con maggiore esperienza dei suoi coetanei nella propria attività online. I genitori o i tutori sono le figure più indicate dal momento che possiedono l'esperienza necessaria e vivono con i giovani da tutelare, costituendo quindi per loro dei punti di riferimento. Inoltre, tale funzione di affiancamento dei minorenni nonché di educazione alle regole da seguire per vivere delle esperienze costruttive online vengono prescritte anche dalla legge: la responsabilità genitoriale, viene auspicata solo dal punto di vista legale per la tutela del minore, vista la difficoltà del legislatore a garantire la sicurezza di un mondo virtuale che va a una velocità vertiginosamente diversa da quella della burocrazia.
Il problema della tutela del minore va affrontato considerando che quest'ultimo deve essere protetto sotto due profili: quale vittima di reato su Internet (e in primo luogo i reati concernenti l'abuso e lo sfruttamento sessuale) e quale fruitore dei servizi e delle informazioni. Come citato in precedenza, il minore nel corso delle sue attività online, talvolta manifesta l'esigenza di rapportarsi ad un adulto per capire le innumerevoli possibilità che gli si presentano; non solo, alle volte il minore si rifugia nel mondo virtuale perché solo lì non si sente trascurato, o reputa solo quello un posto sicuro che gli consenta di evadere comodamente dalla sua

[47] T. Maggi, "Giovani connessioni- orientarsi con i figli nel web", San paolo edizioni, 2020, pag. 138.
[48] Tamara Maggi, in riferimento all'opera della nota 41, è scrittrice, educatrice di giovani e collabora con psicologi, pedagogisti ed altri educatori nella realizzazione di progetti con lo scopo di costruire una rete tra genitori, meglio nota come la Rete dei Genitori Digital.

quotidianità. Quindi per naturale predisposizione dei ragazzi, continuamente bombardati da stimoli virtuali, si ha un loro avvicinamento alla realtà virtuale[49]. È questo che rende necessario che qualcuno garantisca l'equilibrio tra la loro genuina curiosità, voglia di esprimersi e la sicurezza con cui poter esprimere e vivere al meglio entrambe. La pandemia inoltre ha reso impossibile evitare l'avvicinamento dei più piccoli all'attività in rete a causa della didattica a distanza. Una volta quindi che i giovani vengo iniziati al mondo digitale è bene ricevano quell'educazione tale per cui comprendano che è solo un mezzo: per esprimersi, per fare il proprio dovere, per tenersi in contatto con amici e familiari lontani, per organizzare incontri con persone nella vita reale[50]. Proprio quest'ultimo scopo necessita una maggiore attenzione nell'analisi, perché le persone con cui il minore programma incontri nella vita reale, non sempre combaciano con chi ritengono di aver "conosciuto" nel mondo virtuale. Se già innumerevoli immigrati digitali cadono vittima di *catfish*, figurarsi i nativi; prede perfette per malintenzionati che scrivono loro mantenendo un'identità falsa, con cui illuderli di costruire un legame affettivo. I truffatori in questo caso scelgono attentamente la loro vittima, il più delle volte rispondente all'utente minorenne privo di controllo genitoriale nelle attività online e purtroppo anche privo di un dialogo soddisfacente con qualsivoglia adulto di riferimento che possa fargli capire che la persona che gli si sta avvicinando in chat pur senza conoscerlo, è tutt'altro che disinteressata. Giovani isolati quindi, privi di legami affettivi soddisfacenti, privi di una vita offline avvincente o quantomeno, ricca di attività, rispondono al profilo ideale della vittima per il *catfisher* di turno. Quest'ultimo, una volta scelto il potenziale bersaglio, cerca di entrare in confidenza con lui attraverso la tecnica del *grooming*, se ne prende cura, lo ascolta, intensifica l'attività online per non farlo sentire solo; desidera farlo sentire capito, per poter ottenere la sua fiducia e

[49] Realtà virtuale:" Ambiente virtuale che simula una realtà in cui l'operatore esterno si configura come interno a questo ambiente, come protagonista della realtà creata. Alcuni videogiochi aiutano i ragazzi a muoversi in una seconda realtà in cui sono sempre più coinvolti. Necessaria per gestire sistemi complessi, torna utile per prefigurare tutte le possibili soluzioni così da ridurre al minimo i rischi nella realtà effettiva" definizione riportata nel saggio di P. Bianchi, "4.0 La nuova rivoluzione industriale", ilMulino, 2018, pag. 14.

[50] Oltre a un'educazione che veicoli quel messaggio, è bene tenere presente che per molti giovani questa sia già una realtà quasi data per scontata, come dimostra la maggioranza dei minori intervistati negli Stati Uniti dalla Professoressa danah boyd.

fare breccia nelle sue debolezze. È così che molti utenti iniziano a far compiere azioni ai più piccoli contro la loro volontà pur non esercitando violenza fisica in maniera diretta: la coercizione viene dalla violenza mentale; il *groomer* sfrutta inizialmente i sensi di colpa del suo interlocutore per fargli fare ciò che vuole: "Io ero lì con te ad ascoltarti quando avevi bisogno, ricordi? Io ti voglio bene, non ti ho mai lasciato solo, vero?". Una volta ottenute confessioni, immagini, video o informazioni che gli possono tornare utili, le usa come materiale di ricatto per l'utente che ormai è caduto nella sua trappola. A questo punto si ha un'*escalation* di richieste, cui il piccolo non sa come sottrarsi, anzi, il più delle volte non pensa nemmeno lontanamente che sia possibile farlo, dal momento che il suo punto di riferimento si è trasformato nel suo aguzzino.[51] Quest'ultimo, assicurandosi che il minore non avesse un adulto con cui confidarsi, né tantomeno uno che ne supervisionasse l'attività in rete, si è trovato una vittima perfetta, inerme innanzi alle sue nefandezze; che possono assumere le sfumature più diverse: dalla pedopornografia al furto di dati del genitore per poi derubare la sua abitazione o addirittura il conto in banca. La vittima può sfuggire a tutto questo rivolgendosi alle forze dell'ordine, ai genitori o tutori responsabili della sua condotta online, all'azienda che gestisce il social che è stato reso teatro dell'illecito (nei prossimi capitoli spiegherò nel dettaglio le modalità e le leggi di riferimento). La tutela che consente all'utente minorenne di difendersi e farsi difendere da chi di dovere quindi discende dalla sua conoscenza delle possibilità di difesa di cui dispone, tanto che è visto come fondamentale il suo diritto all'educazione nonché partecipazione ai media. Tale diritto viene riconosciuto come inviolabile da parte della Convenzione ONU dei Diritti dell'Infanzia che ha disposto che gli Stati membri attuino programmi d'informazione volti alla promozione dell'uso sicuro di Internet. In Italia, tale volontà era già stata espressa nel luglio del 1995, con il decreto n. 385, del Ministero delle poste e delle comunicazioni, ha emesso un regolamento recante le norme circa le modalità di espletamento dei servizi *audiotex* e *videotex*, tenuto conto delle particolari esigenze dei più giovani che si avvicinavano a quei mezzi di diffusione, nonché prevedendo che le informazioni

[51] A. La Lumia, A. Dario, "Minori, internet e social network", Giuffrè, 2021, pag. 45.

o prestazioni *audiotex* e *videotex* fossero "*destinate ai maggiori di 18 anni*" [52]; disciplinando all'art.6 la materia per i servizi rivolti ai minori.

Un nativo digitale quindi, può cadere più facilmente vittima di un malintenzionato online rispetto ad un adulto, poiché si suppone che quest'ultimo conosca i suoi diritti, sappia difendersi da truffe online ed infine che conduca una vita dove ai social viene lasciato molto poco spazio tra lavoro, famiglia, relazioni, impegni e passatempi vari ed eventuali.[53] Sono proprio i più piccoli che non hanno una vita sociale (intesa in senso fisico) attiva, talvolta privi di interessi legati al mondo reale, nonché privi di attenzione ed affetto che cercano altrove tutto questo: online il ragazzo può disfarsi della propria identità, anzitutto. Può costruire un nuovo sé stesso, emulare modelli che più si confanno a ciò che ritiene piacevole per sé. Se nella sua famiglia si sente emarginato può costruire un'identità online che lo renda degno d'affetto, sfuggendo a ciò che secondo il suo parere non lo rende amabile da chi gli sta intorno.[54] Oppure può subire un vero e proprio sdoppiamento di personalità: è il caso dei cyberbulli, vittime nella vita reale, che si sfogano online sui loro carnefici o su altri ragazzi più indifesi, con profili creati appositamente.[55] In altri casi, invece, i ragazzi trovano online un mondo di conferme, di incoraggiamenti, che non provengono dagli ambienti in cui vive il ragazzo, in primis dalla famiglia; nel mondo virtuale ogni risultato viene registrato, ogni progresso viene festeggiato con gli altri utenti per mezzo di accattivanti effetti visivi e sonori che catturano l'attenzione e danno un senso di soddisfazione al giovane utente che vede riconosciuto un suo successo. Ma non solo, avendo la possibilità di condividerlo con altri, può acquisire maggiore consenso oltre che complimenti di coloro che sono stati messi al corrente dal risultato da esso conseguito.

---

[52] Decreto 13 luglio 1995, n. 385 "Regolamento recante norme sulle modalità di espletamento dei servizi audiotex e videotex" pubblicato in Gazzetta Ufficiale n. 218 del 18 settembre 1995, prodotto dal ministero delle poste e delle telecomunicazioni.

[53] R. Razzante, "Informazione: istruzioni per l'uso - notizie, rete, e tutela della persona ",Cedam, 2014, pag. 120 e ss.

[54] Generalmente tale meccanismo si innesca ad una potenza più elevata nel caso dei giochi di ruolo online, in particolare nei MMORPG (ovvero, Massive Multiplayer Online Role-Playing). A. La Lumia e A. Dario, "Minori, internet e social network", Giuffrè, 2021, pag. 55.

[55] G. Lavenia, "Mio figlio non riesce a stare senza smartphone", Giuntiedu, 2019, pag. 29 e ss.

Si può quindi dire che il bisogno di affermarsi che spinge il minore nel mondo virtuale, è psicologicamente spiegabile con il fatto che supporto e affermazione siano gli aspetti base per consentirgli una crescita sana. La mente del minore necessita di incoraggiamenti per consentirgli di crescere con un adeguato senso di autostima, che lo renda un adulto consapevole delle proprie capacità, dotato di un atteggiamento costruttivo costruito grazie alla sua abilità di adottare un'ottica *non defining*. In pratica, questo termine definisce l'approccio del ragazzo verso i suoi insuccessi da cui riesce a distaccarsi, evitando di identificarvisi ma anzi prendendovi spunto per far sì che non si ripetano con le stesse modalità: egli adotta quindi l'ottica costruttiva che vede sempre il margine di miglioramento anziché lasciarsi schiacciare dalla frustrazione dell'insuccesso. Ciò è possibile grazie ad un dialogo interiore propositivo che il ragazzo ha sviluppato grazie al fatto di aver ricevuto un'educazione attenta al modo con cui egli si pone innanzi alle sfide, e che si rifà al concetto di "*saying is believing*", ovvero "dire è credere". Sul medesimo principio si basa la profezia che si autoavvera di Thomas anche se in questo caso essa si lega ad una percezione negativa di sé: se il ragazzo ad esempio non si crede degno di affetto, si comporterà in modo tale da non riceverne, finendo così per dare ragione al pensiero che tanto temeva.[56] Ecco quindi l'importanza della figura adulta e della sua guida, delle sue rassicurazioni; tanto più il ragazzo viene lasciato a sé stesso, tanto più diventa fragile e cercherà un supporto finendo per trovarlo da chi non ha intenzione di darglielo davvero, per il suo bene, ma bensì illuderlo di farglielo avere per allontanarlo dai suoi già esigui legami che possiede per poi poterne approfittare. Questo diviene molto difficile, se non impossibile, quando il minore viene controllato, educato ed affiancato nelle sue attività, online e non, dal momento che viene inserito in un ambiente *caring* ovvero, che si occupa di lui. Egli stesso non farà fatica ad adottare un'ottica *self caring*. Quest'ultima diventerà molto importante non solo per il suo corretto sviluppo psicologico, che gli consentirà di costruirsi un'appagante vita da adulto; ma anche da piccolo lo aiuterà a riconoscere i campanelli d'allarme qualora una persona con intenzioni poco limpide provasse

[56] Fonti: C. Cornoldi, C. Meneghetti, A. Moè, C. Zamperlin, "Processi cognitivi, motivazione e apprendimento." Bologna: Il Mulino, 2018, pag. 125 e ss.; A. Moè, "L'ABC per motivare. Strumenti e metodi per favorire la voglia di imparare", Mondadori, 2021, pag. 23.

ad approcciarlo o a fargli strane richieste dopo aver colto qualche segnale di aiuto o ricerca di attenzione che il giovane utente ha affidato alla rete.

Purtroppo il web accoglie tutti i suoi utenti senza poter garantire loro una protezione perfetta: è vero che ci sono i moderatori e la polizia postale, ma mentre i primi sono costretti ad agire in tempi rapidissimi per processare una mole di dati impressionante, talvolta anche densa di contenuti psicologicamente pesanti, tanto che vengono seguiti da psicologi che li aiutano a gestire il carico emotivo che riversa loro addosso la propria mansione; la seconda deve fare i conti con la carenza di organico. In un interessante saggio di Aldo Cazzullo[57], giornalista del "Corriere della Sera" e scrittore, Zuckemberg individua i motivi per cui il web stia spopolando soprattutto tra giovani e giovanissimi, che essi stessi, di cui si fanno portavoce i figli dell'autore, riconoscono come validi: appartengono ad una generazione differente dalle precedenti, che provavano un senso di appartenenza ad una comunità, fosse stata anche religiosa o lavorativa. I giovani oggi si sentono disconnessi, avvertono un senso di vuoto che non sanno come colmare, temono di non essere accettati, cercano di rendersi appariscenti finendo per omologarsi pur di ricevere attenzione. Ma l'omologazione è un rischio che era presente da prima dei social, come testimonia una frase attribuita ad un autore

[57] A. Cazzullo; con R. e F. Maletto Cazzullo, "Metti via quel cellulare– un papà. due figli. una rivoluzione.", Mondadori, 2017, pag. da 105 a 107.

polacco del 1957 "*ci sono zebre che starebbero in gabbia pur di passare per cavalli bianchi*"[58].

Inoltre, i ragazzi minorenni si rendono conto che la tecnologia è uno strumento fantastico per aiutare la democrazia dando voce a chi non ne possiede, anche se questo non significa che tutti gli utenti siano educati e la sappiano usare nella maniera che più si conviene a delle persone mature che sanno che ogni azione ha una conseguenza. Così come che ogni post, assieme ai dati del suo creatore va a costituire dei *big data*[59] che rimangono in rete.

I genitori possono infatti presentare preoccupazioni circa quanto di indelebile ci sia in rete, ed i ragazzi, dal canto loro, non possono che prenderne atto, utilizzarla in maniera consapevole, apprezzando il fatto che l'espansione dei *big data* renderà più facile l'individuazione di utenti malevoli e disonesti, rivelandosi d'aiuto per le Forze dell'ordine.

Ai ragazzi piace la possibilità di avvicinarsi alla rete, di sentirsi grandi, importanti, di poter fare immediatamente ciò per cui nel mondo reale devono aspettare qualche anno, per esempio gli acquisti, esprimere la propria opinione ben sapendo che essa potrà venire accolta da alcuni membri del popolo della rete, così come messa in discussione, talvolta con toni provocatori, se non insolenti, da altri[60]. Un effetto di quell'apparenza di democrazia diretta[61] che vogliono dare i *social*, è quello della polarizzazione: innanzi ad un argomento, si formeranno e saranno prevalenti due posizioni, una opposta all'altra, estreme, e per l'effetto degli algoritmi su cui sono basati i social si formeranno delle *echo chambers*:

[58] Stanisław Jerzy Lec fu uno scrittore, aforista e poeta polacco che con la frase:" ci sono zebre che starebbero in gabbia pur di passare per cavalli bianchi" intendeva che le persone sono disposte anche a fare dei sacrifici pur di apparire diversamente da come sono, nel tentativo di dimostrarsi migliori di come si percepiscono o di come ritengono di essere percepite dagli altri. A. Cazzullo con R. e F. Maletto Cazzullo, "Metti via quel cellulare- un padre, due figli, una rivoluzione", Mondadori, 2017, pag. 68.

[59] Big data: Capacità di gestire ingenti volumi di dati generati da ogni tipo di connessione e device. È la quantità di dati disomogenei derivati da fonti diverse che per essere utilizzabile deve essere trattata attraverso la creazione di data analytics in grado di produrre info e conoscenze adeguate e rilevanti per prendere decisioni puntuali. Fonte: P. Bianchi, "4.0 La nuova rivoluzione industriale", ilMulino, 2018, pag. 113.

[60] W. Quattrociocchi, A. Vicini,"Misinformation", FrancoAngeli, 2016, pag. 83.

[61] La democrazia della rete viene definita come "apparente" e "diretta" da M. Castells nel saggio di A. Astone, "I dati personali del minore in rete- dall'internet delle persone all'internet delle cose", Giuffrè, 2019, pag. 4.

ovvero delle camere dove si verifica l'eco. Queste ultime altro non sono che dei gruppi in cui l'individuo entra in contatto con altri utenti che la pensano allo stesso modo sulla questione presa in esame, che portano ad un radicamento, un consolidamento delle opinioni già presenti, rafforzando nei loro membri la percezione di essere nel giusto. Non tutti i ragazzi credono a tutto ciò che leggono nel web, tantomeno ritengono che il fenomeno delle *echo chambers* sia pericoloso. D'altra parte, tuttavia, molti genitori condividono la preoccupazione della velocità con cui internet raggiunge i suoi bersagli se usato come mezzo di propaganda, ad esempio come ha fatto l'ISIS, ma i ragazzi[62] ritengono che mentre questa ideologia aveva tutto l'interesse a non far trovare le proprie tracce, altre realtà invece hanno utilizzato i media tecnologici alla luce del sole per fini assai più costruttivi. È il caso di Save the Children, come anche medici senza frontiere e tante altre, che hanno beneficiato degli algoritmi che ne hanno favorito la diffusione, collegandole ad altre realtà connesse da *link* che le rendevano visibili agli utenti che avevano manifestato interessi riguardo a tali tematiche.

[62] A. Cazzullo con R. e F. Maletto Cazzullo, "Metti via quel cellulare- un padre, due figli, una rivoluzione", Mondadori, 2017, pag. 90 e ss.

Capitolo 2: I contratti online

Introduzione al capitolo 2.

Nonostante il primo negozio online abbia aperto la propria attività nel 1994[63], l'attività di regolamentazione sul tema degli acquisti in rete annullabili perché compiuti da minorenni è tutt'ora in fase di sviluppo, anche se ha subìto una notevole accelerazione grazie al periodo pandemico. È stato proprio durante la pandemia che tutti erano collegati e gestivano i propri acquisti perlopiù in rete e tra coloro che avevano adottato questa abitudine figurano anche i giovanissimi internauti, talvolta col disappunto dei propri genitori. In tale occasione, nel 2020 infatti, il diritto al ripensamento è stato modificato e reso maggiormente accessibile circa le modalità di esercizio dai genitori dei clienti minorenni. Questi ultimi, già affascinati dalla tecnologia, le si sono avvicinati maggiormente scoprendone ulteriori funzionalità collegate al principio di ripensamento[64]. L'acquisto online è interdetto al minore in quanto tale, o meglio, egli può sottoscrivere un contratto di compravendita online anche se di fatto è annullabile dal giudice. Tuttavia ci sono alcuni casi in cui questa eventualità non è possibile e si verificano qualora l'acquirente minorenne abbia effettuato raggiri nei confronti del venditore.

Il pericolo di acquisto online quindi non lo corre solo la famiglia del minore nella misura del patrimonio cui può attingere quest'ultimo, ma anche il venditore qualora i genitori pretendano l'annullamento di un contratto che egli aveva inconsapevolmente stipulato con la prole. I genitori in questo caso possono avvalersi di molteplici strumenti quali il diritto di recesso, la dimostrazione di aver attuato i comportamenti previsti per non incorrere nella *culpa in educando* né *in*

[63] Nello specifico, Pizza Hut: una catena di ristorazione statunitense con sede a Dallas, in Texas, fondata nel 1958 dai fratelli Dan e Frank Carney. Ma tra i primi ad aprire online la possibilità di acquisti figura anche l'attuale colosso di Amazon, entrato in attività nel 1995.

[64] Questo tipo di diritto è differente dal classico diritto di recesso in quanto piò essere esercitato entro 6 ore dalla stipula del contratto online e non entro 14 giorni: in questo caso l'acquirente non fa in tempo a ricevere quanto ha appena comprato pertanto non è tenuto a rispedire indietro la merce mentre nel caso del diritto di recesso le spese di spedizione sarebbero a suo carico. Tale diritto, nato nel 2019 (delibera AGCOM n. 108/19/CONS del 12 Aprile 2019), prevedeva che potesse venire esercitato tramite la chiamata al numero 800442299, mentre dal 20 gennaio 2020 è sufficiente un messaggio al medesimo numero. A. La Lumia, A. Dario, " Minori, internet e social media" Giuffrè, 2019, pag 55 e ss.

vigilando, fino al più recente diritto al ripensamento, indicato non solo come sinonimo del diritto di recesso, ma dal 2019 con un significato differente in quanto è un'altra modalità di esercizio dello stesso in relazione a specifici servizi. [65] Quest'ultimo è uno strumento particolare che consente al genitore che non ha autorizzato l'acquisto di richiedere entro 6 ore da quando è stato concluso il contratto online dal figlio minorenne il riaccreditamento di quanto addebitato nonché la disattivazione della pratica commerciale posta in essere dal venditore online nei confronti del minore. Queste forme di tutela del patrimonio familiare da acquisti indesiderati dai genitori, compiuti dai minori, sono utilizzabili sia nel caso in cui la prole li abbia posti in essere consapevolmente, sia nel caso contrario. Data la facilità di concludere un contratto anche grazie alla nuova modalità "*point and click*"[66], è sempre più facile che un navigatore poco attento compia acquisti involontariamente, per non parlare degli abbonamenti che compaiono con delle finestre online mentre l'utente magari sta solamente visitando il sito e per una questione di tempismo sbagliato clicca per sottoscrivere l'acquisto di un abbonamento alla rivista del sito che stava consultando. Inoltre esiste anche la possibilità di poter comprare in app: da alimenti a *upgrades* nelle applicazioni di videogiochi, scaricando l'importo direttamente dalla ricarica del telefonino, senza necessità di informazioni sulla carta di credito virtuale.

Se è vero che la rete ha offerto infinite possibilità, è altrettanto vero che insieme a queste sono arrivati, inevitabilmente, anche dei rischi, come il non riuscire a verificare efficacemente l'identità di chi sta sottoscrivendo un contratto da dietro uno schermo. Le legislazioni italiana ed europea non lasciano soli né i consumatori né i venditori, fornendo ai primi mezzi e strategie di prevenzione nonché strumenti di tutela del proprio patrimonio anche una volta sottoscritto il contratto d'acquisto, mentre ai secondi sono state date delle indicazioni da seguire al fine di identificare momentaneamente chi sta per comprare il loro bene o servizio, stabilendo che qualora sia un soggetto inabilitato a farlo, come ad esempio un minore, il commerciante abbia diritto alla tutela.

[65] C. Baggio, articolo online dal sito Smartius "Acquisti online dei minorenni: come prevenirli e porvi rimedio", 4/05/2021.
[66] Medesima fonte della nota 65.

Nel presente capitolo quindi, oltre alle tutele in merito alla conclusione dei contratti online per i quali il minore viene considerato incapace di agire in quanto tale, viene volto lo sguardo anche a quei tipi di contratti negoziali che il minore può concludere, non solamente se emancipato. In virtù del principio del "*Best interest of child*", infatti, ai minori viene riconosciuta la possibilità di contrarre contratti dal valore economico scarso definiti come "atti minuti": questi sono normalissimi atti di compravendita conclusi dai minori al fine di rispondere alle loro necessità.

Tali concetti sono necessari all'introduzione dei molteplici temi: da quello dell'annullabilità del contratto normale (quindi non si parla più degli atti minuti di cui sopra) di compravendita stipulato dal soggetto minorenne, alla necessità di regolamentare e differenziare i due tipi di acquisto, in ragione delle capacità di cui dispongono i minori ultra-dodicenni, passando per la possibilità loro concessa di stipulare accordi in merito al trattamento dei propri dati personali nel rispetto di determinate condizioni dettate sia dall'Unione Europea sia dal legislatore italiano.

paragrafo 2.1 Il contratto del minore

La necessità di analizzare il tema del contratto stipulato da minori online è dovuta principalmente alla novità del fenomeno di un minore che contrae in via telematica ed alla necessità di tutela del patrimonio della famiglia del minore, del venditore e del minore stesso.

Quando si parla di minori è bene scindere le nozioni di bambino e adolescente. Il primo è il minore che non ha ancora compiuto 15 anni o che è ancora soggetto all'obbligo scolastico; mentre il secondo s'identifica con il minore di età compresa tra i 15 e i 18 anni che non è più soggetto all'obbligo scolastico[67].

La novità del tema sopra introdotto però, è direttamente proporzionale alla velocità di espansione della fattispecie citata, accelerata dall'avvicinamento dei ragazzi ai mezzi tecnologici dovuto alla diffusione del covid-19. Già in precedenza i più giovani manifestavano ampia curiosità nei confronti di tecnologia e mondo online, ma con l'avvento della pandemia sono stati in un certo senso costretti a sperimentarne le funzionalità, ad esempio imparando come connettersi per seguire le lezioni da casa, prestando attenzione all'audio del device in uso, all'attivazione della fotocamera e del microfono, per citare alcuni esempi. Anche gli insegnanti si è preteso si adattassero a questa inedita modalità di lavoro, e hanno sostenuto una sfida alquanto impegnativa, soprattutto per mantenere viva l'attenzione degli alunni pur facendo lezione con mezzi che sfruttano l'attenzione selettiva[68]. Ma mentre per gli immigrati digitali, che pur facendo un lavoro fantastico nell'adattarsi tanto in fretta ad un cambiamento così repentino, il mezzo tecnologico rimane un ostacolo e una pesantezza, per i cosiddetti nativi digitali rappresenta un'opportunità.

In particolare, l'opportunità di scoprire nuovi luoghi interessanti da visitare; di tenersi in contatto con amici lontani; conoscere nuove persone; di giocare, da soli o in compagnia; di seguire la lezione; di ascoltare la propria canzone preferita; di

[67]Definizioni all'art.1 della l. n. 977 1967 sulla tutela del lavoro dei bambini e adolescenti.

[68] L'attenzione selettiva consiste nell'operare una selezione tra gli stimoli che investono tutti gli organi di senso in un certo istante consentendo soltanto ad alcuni di accedere a successivi stadi di elaborazione. Essa è un processo dell'attenzione assieme all'attenzione mantenuta, a quella focalizzata, a quella divisa e a quella soggetta a spostamento (shifting). C. Cornoldi, C. Meneghetti, A. Moè, C. Zamperlin, "Processi cognitivi, motivazione, apprendimento", ilMulino, 2021, pag. 32 e ss.

riempire i momenti vuoti o di noia; di vedere film; di interagire con spettacoli e trasmissioni in tempo reale; di esprimere le proprie idee ed opinioni; oppure, nei casi estremi, di fare quello che nella vita reale non si avrebbe il coraggio di fare. Azioni percepite come pericolose o sbagliate, come comprare qualcosa senza dire la propria età o mentendo a riguardo, ben sapendo di non poterlo fare, ma sentendosi al sicuro dal fatto che tra sé stessi e il venditore ci sia un pc che non fa conoscere la propria identità.

Le tutele provenienti dall'esterno come i diversi tipi di *software*, così come quelle dovute a fattori interni al minore grazie alla cultura digitale che dovrebbe muoverne le azioni con la funzione di auto-controllo, non impediscono al soggetto in questione di porre in essere condotte che non avrebbe la facoltà giuridica di attuare, proprio in termini di consenso: il contratto concluso dal minore, è infatti invalido perché concluso da un incapace legale, e la sua eventuale capacità di intendere e volere al momento della conclusione del contratto non influisce sulla sua annullabilità (di cui verrà trattato in seguito). Sebbene sia stata superata la rappresentazione dell'infradiciottenne come quel soggetto "*totalmente incapace di agire*" assieme alla distinzione tra "stati naturali e arbitrari della persona"[69], e al soggetto minorenne venga quindi riconosciuto il diritto soggettivo della capacità di agire[70], è senz'altro da rilevare che quest'ultima tipologia di diritto talvolta venga mitigata dal legislatore[71].

Le condotte a cui si fa riferimento in questo capitolo, riguardano la conclusione di contratti online che principalmente possono avvenire per due ragioni ben distinte a cui però si applica la stessa disciplina. La prima motivazione è la volontà del minore di compiere l'acquisto; ciò che fa variare il trattamento legale del minore che ha posto in essere questa condotta, consiste nel fatto di aver attuato raggiri o meno per concludere il contratto. La seconda invece, si riferisce all'ipotesi di

[69] Tale superamento della legislazione relativa all'incapacità del minore è dovuta alla sua rivisitazione da parte di norme contenute nella Costituzione, nella Carta dei diritti fondamentali UE, nella Convenzione EDU, nella Convenzione di New York sui diritti del fanciullo (20/11/1989) e nella Convenzione di Strasburgo sull'esercizio dei minori del 25/01/1996.

[70] Art 2 Cod. Civ. : consiste nella possibilità per il soggetto di affermare e far valere i suoi interessi.

[71] R. Senigallia, "Minore età e contratto- contributo alla teoria della capacità", G. Giappichelli editore, 2020, pag. 3.

falle nel sistema di tutela del giovanissimo utente da trappole online che, sfruttando la sua inesperienza, potrebbero portarlo a fare acquisti indesiderati i cui contratti sono annullabili ma validi fino a che il giudice non li annulli con la propria sentenza.

Che rientrino o meno nella volontà di stipulazione dei minori, i contratti online sono molto frequenti secondo il rapporto Istat del 2019 relativo alla sezione “Cittadini e ICT”. In esso infatti, si può notare come il 40% di minori con un’età compresa tra i 14 ed i 17 anni, sul totale di ragazzi che hanno asserito di navigare online, abbiano dichiarato di aver compiuto acquisti in rete. Nello stesso report, tuttavia, emerge un dato preoccupante: la maggioranza dei ragazzi online possiede competenze basse o di base, pertanto più del 60% dei giovani internauti d’età compresa tra i 16 ed i 19 anni non risulta pronta a gestire al meglio le potenzialità che gli vengono offerte dagli strumenti di cui dispongono ma anzi rischiano di divenire vittime di truffe o altri pericoli nascosti nella rete da chi sta dall’altro lato dello schermo.

I ragazzi possono essere spinti a fare acquisti online per i motivi più diversi: dal compiere un’azione che normalmente gli viene interdetta, al progredire più velocemente con un videogioco. Ogni loro desiderio in questo senso diviene più agevole: non solo per la difficoltà del venditore di verificarne l’identità dal momento che la contrattazione non avviene alla presenza fisica degli interessati, ma anche per la semplicità dei metodi che consentono di compiere acquisti in

rete. La modalità "*point and clic*"[72], infatti, consente di acquistare in modo immediato, ed è perfettamente idonea a farlo: essa consiste semplicemente nel selezionare la casella dell'oggetto di interesse e con un clic il contratto è stato validamente concluso.

I minorenni, inoltre, possono essere più facilmente indotti rispetto ai giocatori di videogame meno giovani ad altri tipi di acquisto in rete. È il caso di quelli che si possono fare in app: è quanto accade nei videogiochi che consentono di comprare articoli consumabili che hanno le caratteristiche di essere acquistati una tantum e di non essere riutilizzabili, come valute elettroniche, armi, accessori, *upgrades* e tutto ciò che può far progredire il personaggio del giocatore per migliorarne l'esperienza di gioco. Quest'ultima conosce un ulteriore miglioramento qualora non vi fossero annunci e pubblicità a interromperla in determinate fasi del gioco, solitamente, quelle cruciali, ed ecco che il minore viene nuovamente tentato di pagare per assicurarsi la versione pro della propria applicazione, che ne rimuove gli annunci pubblicitari e gli consente di sbloccare non solo nuove funzioni ma anche nuovi livelli di gioco.[73] Ma se i giovani in questione non fossero tanto appassionati di videogiochi sicuramente lo sono in fatto di musica, qualsiasi sia il genere, e così diventano utilizzatori di app come Spotify[74] o, nel caso di film, Hulu[75].

Anche queste applicazioni sono scaricabili gratuitamente, ed è senza costi anche l'iscrizione alle stesse, pertanto vengono introdotte nei telefonini dei più senza problemi. Ciò a cui bisogna prestare attenzione è la loro proposta di

[72] Fonte: sito del Centro Europeo Consumatori (CEC) Italia (al link https://www.euroconsumatori.org/it/minorenni_in_internet).

[73] G. Lavenia, "Mio figlio non riesce a stare senza smartphone", Giuntiedu, 2019, pag.72; "Minori, Internet e social network" A. Dario, A. La Lumia, Giuffrè, 2021, pag. 54 e ss.

[74] App svedese nata nel 2008, tutt'oggi leader del mercato di settore per quanto concerne gli abbonamenti. Essa è una piattaforma web da cui poter ascoltare e scaricare musica in modo legale.

[75] Piattaforma che consente di vedere film e serie tv gratis negli USA. Nasce proprio lì infatti, insieme a Netflix e come lei propone un modello di televisione on demand, quindi non lineare ai propri utenti. In Italia non è ancora presente come piattaforma in sé, si può accedere ai suoi contenuti tramite la connessione criptata offerta da una VPN (Virtual Private Network) ovvero una rete privata, che si appoggia su una rete pubblica e che è in grado di mettere in comunicazione dispositivi e server. In questo caso anche Hulu come Netflix ha degli abbonamenti che gli aspiranti telespettatori devono quindi pagare. Lo stesso dicasi per servizi come Raiplay, presente in Italia: la logica di tv on demand è la medesima dei due casi precedenti ma in questo caso non occorre pagare per abbonarsi, o meglio, la quota è compresa nel canone Rai pagato con la bolletta dell'elettricità.

abbonamento: un *click* sbagliato potrebbe vincolare colui che lo ha compiuto a pagarlo senza limiti di tempo. Il più delle volte l'utente non si accorge della conclusione di tale contratto se non dopo un po' di tempo a seguito del prelievo di denaro periodico e continuativo che viene fatto a sue spese, o a quelle del genitore ignaro delle attività online del figlio minorenne. È stato per fare fronte a casistiche simili che dall'1 /11/2019 esiste un nuovo strumento a disposizione dei genitori di minorenni che si venissero a trovare in tale situazione grazie alla delibera n. 108/19/CONS del 12 Aprile 2019, per mezzo della quale l'AGCOM ha sancito l'approvazione del nuovo Codice di Condotta[76] per l'offerta dei Servizi Premium, giunto alla quarta versione, denominata CASP 4.0. Lo strumento in questione consiste in una richiesta di disattivazione e riaccredito di quanto addebitato (a seguito della stipulazione di un contratto di questo tipo da parte dei figli minorenni) entro 6 ore che iniziano a decorrere dalla ricezione del messaggio di attivazione del servizio oggetto del contratto appena concluso. Tale azione è quindi necessaria nello specifico per disattivare i servizi aggiuntivi a pagamento (ovvero servizi premium VAS[77]) non desiderati attivati inconsapevolmente o senza consenso esplicito. Per farlo, basta contattare il call center unico col numero gratuito 800442299 attivo 24 ore al giorno per 7 giorni /7 per accedere al "Centro Unico di Disattivazione", dove, dopo aver avvisato dell'eventuale registrazione della telefonata e rassicurato il consumatore sul trattamento dei dati personali (che avviene sempre nel pieno rispetto della *privacy*), la voce guida effettua una verifica dei servizi premium attivi sul numero chiamante con la possibilità di disattivarli in tempo reale.

[76] Il Codice di Condotta per i servizi originariamente definiti a sovrapprezzo (CASP) è nato, inizialmente, con la prima versione sottoscritta il 29 Maggio 2008, per disciplinare servizi offerti tramite SMS/MMS su numerazioni in decade 4 e, successivamente, quelli forniti anche tramite connessione dati su reti mobili. In seguito all'introduzione di nuovi canali di accesso e fruizione (smartphone e tablet), nel Luglio 2013 è stata trasmessa all'Autorità una versione rinnovata del Codice di Condotta (CASP 3.0), approvata con delibera n. 47/13/CIR.

[77] I servizi Premium, conosciuti anche con il nome di servizi a sovrapprezzo, a valore aggiunto o "VAS", sono l'insieme delle prestazioni fornite soprattutto da provider esterni al proprio operatore di telefonia mobile, mediante SMS, MMS o connessione dati, che possono essere attivati, ricevuti o fruiti su Telefonino, Tablet o PC. Questi comportano il pagamento quotidiano, settimanale, mensile o a singolo messaggio-contenuto (a seconda della tipologia di servizio attivato), di somme aggiuntive rispetto al canone mensile dell'offerta principale sottoscritta.

Non è sempre detto che gli acquisti online determinino un prelievo dal conto corrente del genitore se vengono compiuti dai figli: questa fattispecie si verifica solo nel caso in cui il primo abbia memorizzato i dati di accesso e pagamento nel *browser* utilizzato sui dispositivi multimediali utilizzati per effettuare i pagamenti. A rendere più veloce ed immediato l'acquisto in questo caso è la memorizzazione dei dati d'accesso dell'utente: l'*account* utilizzato nelle app è quasi sempre collegato ad una carta di credito della quale non serve ogni volta inserire i dati grazie ai sistemi di compilazione automatica. In questo modo, una volta che il minore entra in possesso del telefono del genitore, gli bastano un paio di *click* per poter effettuare l'acquisto di suo interesse. Tale fattispecie ha comportato per Amazon una condanna al risarcimento dei propri clienti[78]. Nello specifico, l'azienda non aveva informato chiaramente i propri clienti in merito al fatto che le applicazioni gratuite potevano indurre a compiere degli acquisti, determinando un meccanismo incontrollato che consisteva negli acquisti fatti dai minorenni all'insaputa dei genitori proprio tramite tali app. E' stato proprio a seguito delle denunce di questi ultimi che la Federal Trade Commission[79] ha iniziato ad indagare su segnalazioni di pagamenti non autorizzati, effettuati inconsapevolmente dai figli attraverso un *click* nelle suddette app. Amazon è stata dunque condannata a rimborsare i propri clienti, ed in seguito l'azienda ha inserito nelle sue app degli strumenti informativi e di protezione allo scopo di impedire che tali vicende si verificassero nuovamente. Infatti, in Europa, Amazon non vende prodotti ai minori di 18 anni e qualora questi vogliano effettuare degli acquisti necessitano del coinvolgimento di un proprio genitore o tutore, in modo tale da arginare il fenomeno degli acquisti online involontari da parte dei minori. [80]

[78] Il giudice americano ha condannato, nel 2016, il colosso della tecnologia Amazon a rimborsare 70 milioni di acquisti senza autorizzazione, pertanto addebitate in modo illecito ad alcuni utenti in seguito agli acquisti in app compiuti involontariamente dai figli, rinunciando ad un eventuale ricorso in appello.

[79] La Federal Trade Commission è un'agenzia governativa statunitense che dal 1914 (anno in cui è stata istituita dal Federal Trade Commission Act) promuove la tutela dei consumatori e l'eliminazione e la prevenzione di pratiche commerciali anticoncorrenziali.

[80] A. Astone, "I dati personali dei minori in rete- dall'internet delle persone all'internet delle cose", Giuffrè, 2019, pag. 41.

Un'altra tipologia di pagamento effettuabile via web, ancora più temibile della precedente, è quella che avviene tramite il credito dello *smartphone*. Una volta che il minorenne ha sottoscritto tale modalità di pagamento infatti, è molto probabile che il credito sul dispositivo termini molto velocemente, ancor che egli si renda conto di come sia potuto succedere. Il soggetto non ancora maggiorenne infatti, molto spesso non sa controllare il credito del proprio telefonino e ancora più frequentemente non si preoccupa di doverlo fare, dal momento che è il genitore che si occupa di pagare l'importo. Ed è proprio questo insieme di elementi che rende ancora più difficoltosa la scoperta di eventuali contratti stipulati con tale modalità di pagamento.

Parlando di prevenzione di tali modalità di acquisto e pagamento, non si può non fare riferimento alle possibilità offerte dalle grandi multinazionali che rendono possibili anche gli acquisti online come ad esempio Apple e Google Play. Mentre la prima fornisce ai suoi utenti la possibilità di creare un accesso collettivo e controllabile ai servizi, la seconda offre la possibilità di impostare la richiesta di una password ogni volta che si intenda effettuare un acquisto in app. il funzionamento di entrambe è molto semplice: qualora un minorenne richieda di poter effettuare acquisti in app, l'utente "organizzatore" della famiglia riceve una notifica e può autorizzare o meno l'operazione direttamente dal proprio dispositivo. [81]

La disciplina contrattuale contenuta nel codice del consumo non fa riferimento solamente ai contratti conclusi in presenza del professionista e dell'acquirente; ma contempla anche le possibilità di contratto concluso fuori dai locali commerciali e del contratto a distanza. Il primo è da intendersi come concluso alla presenza fisica dei contraenti all'esterno dei locali commerciali, oppure, a distanza se successivo all'avvicinamento dell'acquirente all'esterno dei locali commerciali o durante un viaggio promozionale. Il secondo, ovvero il contratto a distanza sopra citato, è di particolare interesse; viene definito all'articolo 45[82],

[81] C. Baggio, articolo online dal sito Smartius "Acquisti online dei minorenni: come prevenirli e porvi rimedio", 4/05/2021.

[82] Articoli presenti nel cod. civ. poiché in essi avviene la traduzione del recepimento di direttiva europea n. 11/1983.

lettera “g” come la modalità con cui viene concluso qualsiasi tipo di contratto in un regime di vendita organizzato, senza la presenza fisica simultanea del professionista e consumatore, mediante l’uso esclusivo di uno o più mezzi di comunicazione a distanza. Il contratto a distanza è stato disciplinato dalla direttiva europea numero 11 del 1983, recepita ora negli articoli 45 e seguenti del codice di consumo. La ratio della direttiva è la tutela del consumatore per i contratti telematici o conclusi all’esterno dei locali commerciali. Il consumatore infatti deve, da un lato, essere tutelato in quanto tale, da eventuali pratiche ingannevoli poste in essere dal commerciante riguardo a beni o servizi oggetto di contrattazione a mezzo della legge; dall’altro, deve essere in grado di tutelarsi da sé grazie alle sue conoscenze utilizzando ordinaria diligenza. Uno degli obiettivi principali del codice del consumo è infatti quello di responsabilizzare il consumatore per renderlo libero di scegliere e conoscere i propri diritti, oltre a tutelarlo. Ricapitolando quindi:

Contratto concluso fuori dai locali commerciali	Contratto a distanza
-concluso alla presenza fisica dei contraenti all’esterno dei locali commerciali; -nei locali del professionista o attraverso qualsiasi mezzo di comunicazione a distanza subito dopo che il consumatore è stato avvicinato personalmente in un luogo diverso dai locali del professionista; -durante un viaggio promozionale	-qualsiasi tipo di contratto concluso in un regime di vendita organizzato, senza la presenza fisica simultanea del professionista e consumatore, mediante l’uso esclusivo di uno o più mezzi di comunicazione
Art. 45 Cod. Cons. lett. h	Art 45 Cod. Cons. lett. g

Queste modalità di conclusione del contratto, prevedono come tutele il diritto di recesso, l’obbligo di informazione; l’onere della prova a carico del

professionista[83]; la tutela amministrativa posta in essere dall'AGCM; l'azione condotta dall'associazione dei consumatori.

La prima forma di tutela è prevista all'art 49 Cod. Cons. ed indicata a carico del professionista, che deve adempiere quest'obbligo anche in sede di *e-commerce*[84], considerato che ha delle ricadute sul periodo di recesso, che la direttiva europea 11/83 ha unificato ad un periodo di 14 giorni. Il diritto di recesso viene riconosciuto come irrinunciabile all'articolo 66 ter del codice di consumo, ed è definito all'articolo 52 del medesimo; la sua ratio è quella di tutelare l'utente dall'acquisto che, se compiuto all'esterno dei locali commerciali potrebbe essere stato preso alla sprovvista dal venditore. Invece, qualora fosse stato persuaso ad acquistare online, potrebbe rimanere sorpreso una volta ricevuto il prodotto che risulta differente dalle aspettative che avevano dato luogo all'acquisto. Ecco perché il diritto in questione ha per effetto lo scioglimento del contratto che cessa così di produrre i suoi effetti. Tuttavia, la finestra temporale che ne consente l'esercizio è limitata, come già detto, a 14 giorni; il *dies a quo* parte in momenti differenti a seconda che l'oggetto dell'acquisto sia un bene o un servizio.
Nel primo caso, i 14 giorni iniziano a decorrere dal momento della consegna del bene; nel secondo caso, invece, partono dalla data che segna l'inizio di erogazione del servizio.

La stessa direttiva europea n. 11/1983 tratta del recesso sia per quanto concerne il contratto che ha per oggetto l'acquisto online di beni e servizi, indipendentemente dal fatto che possa venire stipulato dal ragazzo per errore (es. mentre gioca e clicca su una pubblicità *pop up*) o volontariamente (falsificando i suoi documenti d'identità e usando la carta di credito online dei genitori), sia in merito all'autorizzazione che ha per oggetto la cessione dei dati personali (caso di iscrizione ai *social network*). Come indicato dal Codice Civile,

[83] In caso di un contratto di compravendita concluso online da un minorenne, quando si parla di onere della prova a carico del professionista, si fa riferimento al fatto che in sede giudiziaria stia al venditore dimostrare di avere informato correttamente l'acquirente circa il proprio diritto di recesso. Inoltre il professionista, in sede di giudizio, qualora vi si arrivasse, deve anche dimostrare di avere seguito le procedure normative atte ad individuare l'altro contraente e che questo sia riuscito (eventualmente) ad eluderle.

[84] E-commerce: commercio elettronico che può avere ad oggetto beni o servizi.

all'art. 1373: "*1. Se a una delle parti è attribuita la facoltà di recedere dal contratto, tale facoltà può essere esercitata finché il contratto non abbia avuto un principio di esecuzione. 2. Nei contratti a esecuzione continuata o periodica, tale facoltà può essere esercitata anche successivamente, ma il recesso non ha effetto per le prestazioni già eseguite o in corso di esecuzione. 3. Qualora sia stata stipulata la prestazione di un corrispettivo per il recesso, questo ha effetto quando la prestazione è eseguita. 4. È salvo in ogni caso il patto contrario*". Dunque alle parti è consentito sottrarsi a tale disciplina generale, in quanto le stesse potranno concordare ed inserire nel contratto un più ampio termine a garanzia dell'esercizio del diritto di recesso. Il venditore a distanza deve informare il consumatore circa l'esistenza di tale diritto, consentendogli di esercitarlo; l'art. 49 cod. cons. infatti, alla lettera h), prevede l'obbligo per il soggetto di cui sopra, di consegnare all'acquirente il modulo preimpostato per il recesso che potrà utilizzare o meno.

Se il venditore prima della stipulazione del contratto non informasse in modo completo il consumatore, sull'esercizio del recesso, i termini per recedere aumenterebbero ad 1 anno e 14 giorni. Nel momento in cui invece il venditore adempisse ai propri obblighi d'informazione dei suoi clienti circa il loro diritto di recesso, l'art. 53 cod. cons. stabilisce che se il consumatore-acquirente esercita il diritto di recesso, il venditore dovrà rimborsare al consumatore i pagamenti ricevuti in occasione della vendita, senza alcuna penalità. Il diritto di recesso regolato dal Codice del Consumo è rivolto esclusivamente al consumatore, al quale viene garantita una tutela completa in quanto considerato la parte debole del contratto. Per esercitarlo il consumatore dovrà comunicare tale intenzione al venditore (adottando una delle modalità previste dall'articolo 54 del codice del consumo[85]). A sua volta il venditore, ricevuta tale comunicazione, dovrà provvedere al rimborso del prezzo, che avverrà mediante lo stesso metodo di pagamento adottato per l'acquisto. Per quanto riguarda le spese di spedizione nel caso in cui il diritto di recesso venga esercitato successivamente alla

[85] Le modalità sono prevalentemente due: la prima consiste nel compilare ed inviare un modulo online nel caso di acquisti tramite e-commerce, la seconda invece prevede la possibilità di comunicare con una qualsiasi altra dichiarazione esplicita, la decisione di recedere dal contratto presa dall'acquirente. In entrambi i casi, tale comunicazione dovrà essere inviata prima della scadenza del periodo di recesso.

spedizione del prodotto, il consumatore dovrà comunque sostenere le spese per rispedire il bene al venditore.
In alcuni casi, il venditore potrà offrire in alternativa la possibilità di sostituire la merce con altri prodotti dello stesso importo.
Qualora l'acquirente desideri comunque esercitare il proprio diritto di recedere dal contratto, il venditore può offrire al consumatore l'opzione di compilare e inviare elettronicamente il modulo di recesso, o una qualsiasi altra dichiarazione esplicita sul sito web del professionista, per poi comunicargli la conferma di ricevimento su supporto durevole. Tale conferma su supporto durevole è necessaria al consumatore poiché qualora si andasse in giudizio, egli avrà l'onere di dimostrare di aver correttamente esercitato il diritto di recesso. Tale diritto tuttavia, è escluso nei casi elencati nell'art. 59 del D.lgs. 205/2006.

Una seconda fonte di tutela a favore del consumatore è quella che onera il professionista di dimostrare di aver fatto il possibile per rendere il consumatore consapevole che stava sottoscrivendo una procedura d'acquisto, nonché di avere verificato la sua identità. Per il venditore risulta tuttavia molto complicato verificare l'età ed i requisiti dei suoi contraenti online, e la difficoltà è resa ancora maggiore dal comportamento di questi ultimi, qualora utilizzino dei siti che ne cancellino le tracce elettroniche consentendogli di navigare così in incognito, ricorrendo quindi agli *anonymous remailings*[86]. Solitamente, ad utilizzare questi stratagemmi, sono i contraenti che non vogliono farsi riconoscere, dal momento che sanno benissimo di non poter effettuare legalmente l'acquisto, oppure, più semplicemente, ben sapendo di effettuarlo contro la volontà dei propri rappresentanti, dai quali hanno tutto l'interesse a non farsi riconoscere, né tantomeno a far loro sapere le proprie attività online.

La tutela amministrativa viene posta in essere dall'Autorità Garante della Concorrenza e del Mercato; quest'ultima, in poche parole, si occupa di tutelare i cittadini verso gli altri cittadini e verso la Pubblica Amministrazione, che deve

[86] "Anonymous remailer" è un server che riceve messaggi di posta elettronica e li rinvia seguendo apposite istruzioni incluse nei messaggi stessi, senza rivelare la loro provenienza originaria.

svolgere le proprie funzioni nel rispetto dei principi di legalità, imparzialità, ed efficienza.

Esiste anche la tutela posta in essere dall'associazione dei consumatori, disciplinata all'articolo 137 del Codice del Consumo. Queste associazioni, per essere considerate tali, devono possedere determinati requisiti che le facciano rientrare in un elenco istituito presso il Ministero delle attività produttive, rappresentative a livello nazionale. L'associazione di per sé è un ente senza scopo di lucro, il cui atto costitutivo è nato da un contratto tra soci; essa può esercitare un'attività economica che va a vantaggio dell'ente e non dei soci.

Altro modo di difendere il genitore dagli acquisti indesiderati del figlio, previsto nel codice CASP[87] 4.0, consiste in un tipo di diritto di ripensamento differente dal diritto al recesso. A partire dall'1/ 11/ 2019, infatti, al genitore viene concesso di richiedere la disattivazione e il riaccredito di quanto addebitato entro un termine di 6 ore che iniziano a decorrere dalla ricezione del messaggio di attivazione del servizio oggetto del contratto appena concluso. La possibilità del genitore quindi offerta dall'esercizio di questo diritto gli rende agevole porre nel nulla l'acquisto effettuato dal minore. L'elemento di agevolazione è stato rafforzato nel gennaio 2020, mese in cui è stato stabilito che l'adulto di riferimento possa farlo anche solo con un sms al numero 800442299, invece di dover effettuare una chiamata al medesimo numero, come stabilito precedentemente.[88]

Infine, qualora un contratto a distanza non soddisfi l'acquirente per la merce acquistata, diversa da quella che si aspettava di ricevere, oppure se il contraente ha cambiato idea circa l'acquisto effettuato, in casi meno frequenti, si può vedere applicata la nullità di protezione. Quest'ultima consiste in una specifica ipotesi di nullità che può essere fatta valere solo dal consumatore se il fornitore ostacola il diritto di recesso, non rimborsa le spese o viola gli obblighi di informazione precontrattuale, alterando significativamente la rappresentazione delle caratteristiche dell'oggetto della compravendita. Inoltre, la nullità può essere

[87] La condotta per i servizi originariamente definiti a sovrapprezzo: si occupa di disciplinare servizi offerti tramite SMS/MMS e quelli forniti anche tramite connessione dati su reti di telecomunicazione mobili.
[88] C. Baggio, articolo online dal sito Smartius "Acquisti online dei minorenni: come prevenirli e porvi rimedio", 4/0572021.

rilevata d'ufficio dal giudice sempre e solo per tutelare il contraente debole, come riportato all'articolo 36 del Codice di Consumo. Avendo lo scopo di tutelare la parte debole del rapporto contrattuale questa nullità si dice "protettiva". Il diritto di recesso di cui sopra, è un'ulteriore tutela che la Direttiva 2011/83 UE garantisce a tutti i consumatori europei, ed in particolare può essere strumento per i genitori i cui figli minorenni hanno compiuto acquisti online di importi troppo elevati, per ottenere un risarcimento. In questo caso però il tutore del minore deve agire tempestivamente rispettando i termini che partono dal *dies a quo*, che si può estendere ad un anno se il venditore non ha informato correttamente l'acquirente circa l'esistenza e le modalità di esercizio di tale diritto, tenendo presente che le spese di spedizione saranno quasi sicuramente a suo carico.

Ricapitolando, quindi: il contraente che costituisce parte "debole" contrattuale (cioè l'acquirente), dispone del diritto di recesso; della tutela amministrativa; e se il venditore ostacola il diritto di recesso può richiedere la nullità del contratto. Questa disciplina si applica anche nell'ambito dell'*e-commerce*, composto da contratti online, che tuttavia è caratterizzato dalla distanza fisica tra i contraenti, rendendo la loro identificazione assai difficoltosa. Questa identificazione sarebbe importante per garantire diritti al venditore nonché agli acquirenti. Il primo, infatti, ha il diritto a concludere un contratto con un contraente che abbia la facoltà di essere tale, dopo aver fatto il possibile per accertarne i requisiti nel rispetto di quanto stabilito dalla legge. Il secondo ha diritto ad essere pienamente consapevole dell'azione che sta per compiere o ha compiuto, nonché del prodotto o servizio che si accinge ad acquistare, il quale deve corrispondere alle caratteristiche descritte dal fornitore, in modo da fare sottoscrivere il contratto. In particolare, diventa rilevante per il professionista se il contraente, in quanto minorenne, conclude illegalmente un contratto con lui.

Secondo quanto riportato all'art. 322 cod. civ., il contratto è annullabile se compiuto espressamente dal minore non emancipato. Più in generale è corretto affermare che tutti gli atti unilaterali aventi contenuto patrimoniale e i contratti del minore che esulano dagli atti della vita quotidiana e presuppongono la maggiore età possono essere conclusi dal rappresentante legale, in nome e nell'interesse del minore (art. 1387 c.c.). A protezione del minore, essi sono altrimenti

annullabili in virtù dell'art. 1425 cod. civ. L'annullabilità si estende agli atti compiuti dal minore senza l'assistenza richiesta (curatore) o la dovuta autorizzazione (del tribunale o del giudice tutelare). Ne consegue che il contratto sia annullabile entro 5 anni dalla sua stipulazione, trascorsi i quali l'azione di annullamento cade in prescrizione; tuttavia, finché non viene annullato, continua a produrre effetti giuridici. Entro questi 5 anni dalla stipulazione, i soggetti che possono richiedere l'annullamento del contratto sono: il minore una volta raggiunta la maggiore età, oppure il suo rappresentante legale che di solito è un genitore a patto che questi ultimi dimostrino, dal momento che è su di loro a gravare l'onere della prova, che l'acquisto è stato fatto dal minore. Questa dimostrazione diviene complessa nel caso di contratto telematico: nel caso in cui il figlio avesse usato il proprio nome, l'onere della prova si considera assolto ai sensi dell'art 13 d.lgs. n. 70/ 2003; qualora invece avesse utilizzato i dati dei genitori, le difficoltà circa l'assoluzione dell'onere della prova aumenterebbero, come stabilito all'articolo 1426 del Codice Civile. La disciplina prevede due casistiche a riguardo con due differenti tipi di onere della prova da parte del genitore o di chi ne fa le veci. In particolare: se il minore era capace di intendere e volere al momento della conclusione del contratto, il genitore deve dimostrare di averlo educato e aver vigilato su di lui in modo conforme alle condizioni sociali, età, carattere, indole del minore, tenendo conto di quanto riportato nell'articolo 2048 Codice Civile. Se, invece il minore non è imputabile, il genitore deve solamente dimostrare di non aver potuto impedire il fatto. Quindi, non è tenuto a dimostrare anche di avergli impartito una buona educazione.[89]

L'annullabilità del contratto incontra un'eccezione quando il minore abbia con raggiri occultato la sua età. Con il termine "raggiri" si intende un fenomeno che non è ancora stato ben definito, se non indicando esplicitamente cosa non sia: per "raggiro" infatti, non si può intendere il fatto che il minore si dichiari maggiorenne, così come quello in cui ometta l'informazione relativa alla sua età.

[89] A. Astone, "I dati personali del minore in rete- dall'internet delle persone all'internet delle cose", Giuffrè, 2019, pag. 50; Codice Civile; sito del Centro Europeo Consumatori, Italia, ufficio di Bolzano; report dal sito Perlegal, "acquisti online dei minorenni: come prevenirli e porvi rimedio", C. Baggio, 4/05/2021; articolo online "contratto: a quale età si può firmare?", A. Concas, 23/05/2018.

L' articolo 1426 del Codice Civile non trova applicazione qualora siano assenti gli strumenti tecnici idonei ad impedire gli acquisti online da parte dei minori[90].

Le forme di tutela in merito ai contratti sottoscritti da clienti minorenni sono necessarie a disciplinare le eventualità in cui i contratti siano stipulati da utenti non maggiorenni né tantomeno autonomi, e necessitano di essere distinti dai contratti normalmente posti in essere da tali tipologie di contraenti. I ragazzi infatti sono nell'età in cui passano dal compiere gli atti minuti della vita quotidiana a porre in essere quelli che hanno il fine di soddisfare gli interessi specifici anche di una certa rilevanza patrimoniale che variano in base a condizione sociale culturale e economica della persona. Gli atti minuti, riferiti alle esigenze esistenziali del minore, sono[91] contratti (oggettivamente) di modesta entità, la cui minutezza rappresenta la garanzia di assenza di rischio di un rilevante pregiudizio per il patrimonio del minore[92]. Non sono però ben definiti dalla nostra dottrina, tanto che esistono più scuole di pensiero circa cosa si debba intendere ricorrendo a questo concetto[93]. A questi tipi di contratto sono collegate alcune categorie di beni di consumo e di servizi del mercato i cui operatori professionali sono soliti concludere contratti direttamente con gli adolescenti.

In caso di compravendite di beni di valore economico trascurabile , o meglio, di scarso valore economico, il minore agirebbe in rappresentanza dei propri rappresentanti legali, quindi normalmente, dei propri genitori. Formalmente questo è corretto perché trova fondamento nell'art. 1389 cod. civ. il quale sottolinea che il rappresentato (ovvero il genitore in questo caso) il quale disponga della capacità legale d'agire può conferire tacitamente la procura al rappresentante (il figlio minorenne) qualora abbia una capacità di fatto adeguata alla natura nonché al contenuto del contratto. Pertanto si potrebbe concludere che il minore rappresenti i suoi genitori e che in virtù di questo stipuli contratti direttamente produttivi di effetti della propria sfera giuridica. Tuttavia la correttezza formale in questo caso costituisce solamente una finzione che

[90] Fonte:" I dati personali del minore in rete- dall'internet delle persone all'internet delle cose" A. Astone, Giuffrè, 2019, pag 47.
[91] M. Cinque, "Il minore contraente- contesti e limiti della capacità", CEDAM, 2007, pag. 10.
[92] Cit. nota 91, pag. 99.
[93] Cit. nota 91, CEDAM, 2007, pag. 104 e ss.

giustifica il fenomeno preso in considerazione ma non consente né il progresso della disciplina, né tantomeno il riconoscimento di qualsivoglia capacità giuridica del minore in merito alla fattispecie trattata.[94]

I beni necessari acquisiti dal minore sono quelli che determinano la validità del contratto che ha stipulato il soggetto in questione con le caratteristiche relative all'età fino ad ora esaminate. Le caratteristiche di questi beni sono indicate ad esempio nel Sale of Goods Act[95] nell'ordinamento inglese, e si basano sul fatto che un bene sia considerato necessario a seconda del minorenne che lo ha concluso. Anche nell'ordinamento italiano è prevista la possibilità che il soggetto minore d'età compia validamente atti della vita quotidiana: tra questi sono compresi gli atti negoziali (acquisto di beni per esigenze quotidiane), non negoziali (testimponianza, impossessamento, e contratti.[96] I criteri in merito a quali contratti stipulati dai minorenni possano definirsi validi in quanto rientranti tra gli atti minuti si basano sulla situazione economica e sociale del minore nonché sulle sue attuali esigenze, ulteriormente specificate da un insieme di sottocriteri.

La questione è sorta a seguito dei casi giudiziari italiani. In particolare, l'interrogativo più urgente è sempre quello relativo a come stabilire che un bene venduto al minorenne sia per egli necessario[97]. Si procede quindi considerando quali siano i beni necessari considerati come tali dal linguaggio comune, includendo anche la specificazione che i beni necessari non sono confinati alle sole necessità. Essi infatti sono direttamente proporzionali alle disponibilità economiche del minorenne. Pertanto, la crescita di queste ultime determinerà un aumento proporzionale delle esigenze che il minore potrà legittimamente soddisfare da solo. Nonostante questo, il legislatore inglese ha specificato per

[94] R. Senigaglia, "Minore età e contratto- contributo alla teoria della capacità", G. Giappichelli editore, 2020, pag. 108.

[95] Il Sale of Goods Act: atto (suddiviso in 8 parti) del Parlamento del Regno Unito risalente al 1979 relativo ai rapporti di commercio con gli Stati Uniti.

[96] Art. 1389 cod. civ.

[97] La necessità di un bene oggetto di contratto per il minore ne determina la validità dell'azione di compravendita e l'abilitazione quindi del minore a stipulare quel contratto secondo l'art. 409 c. 2 cod. civ. nel rispetto del concetto di atti minuti di vita quotidiana, con riferimento a quegli atti che pur essendo considerati negozi giuridici non richiedono la generale capacità di agire, ma in considerazione della loro quotidianità presuppongono in chi li compie la capacità di comprendere e valutarne il significato.

esempio che i beni di lusso non possono venire mai considerati necessari, semmai possono rientrare nella categoria di beni di una certa utilità per il minore, lo stesso non si può dire per i beni acquistati dal minore per poi essere donati a terzi: in questo caso avranno molta difficoltà a rientrare persino nella categoria di beni necessari.[98]

Il fatto che il minore capace di discernimento venga necessariamente coinvolto nelle scelte che lo interessano, porta razionalmente a riconoscergli una capacità contrattuale, non solo rispetto ad atti della vita quotidiana, ma anche con riguardo a tutti gli atti a lui utili, vantaggiosi, non pregiudizievoli e posti in essere con mezzi propri o messi a sua disposizione. Il mutamento di paradigma è visibile quando l'ordine giuridico elegge a criterio definitorio della capacità contrattuale la "capacità di discernimento" come strumento che, istituendo il diritto all'ascolto, all'affermazione delle proprie scelte, esige la valorizzazione della personalità, consentendo così di accostarsi alla ricerca della identità del minore e di misurarne la graduale e progressiva affermazione[99]. Nel contesto delle attività negoziali la capacità di discernimento è una tecnica di specificazione della capacità di agire, e ne indica una maggiore flessibilità.

La capacità di agire, in tali contesti, consiste nella capacità di volere, di diversa intensità in base agli specifici assetti negoziali; essa è protagonista del cambiamento di paradigma che porta alla considerazione della capacità di discernimento come categoria espressiva della capacità di agire e criterio di definizione della capacità contrattuale. Se l'ascolto portasse a ritenere l'atto compiuto dal minore conforme alla "necessità o evidente utilità del figlio" esso dovrebbe neutralizzare l'azione di annullamento dell'esercente la responsabilità genitoriale, anche nell'ipotesi in cui l'atto posto in essere dal minorenne si qualifichi come eccedente l'ordinaria amministrazione. Tanto che il giudice, in sede di giudizio di annullamento, deve esperire l'ascolto (sussistendo i presupposti) in base all'art ex 320, comma 3 c.c. e se all'esito dovesse emergere che è interesse del minore mantenere in vita quell'atto, perché a lui non

[98] R. Senigaglia, "Minore età e contratto- contributo alla teoria della capacità", G. Giappichelli editore, 2020, pag. 146.

[99] M. Cinque, "Il minore contraente- contesti e limiti della capacità", CEDAM, 2007, pag. 55.

pregiudizievole, ma anzi necessario e utile, il giudice dovrebbe non autorizzare l'azione e dichiarare anche d'ufficio, la carenza d'interesse ad agire.

Se si desiderasse fare una sintesi degli espedienti normativi utilizzati per concedere spazi di capacità contrattuale ai minori si giungerebbe a due orientamenti differenti. In uno si potrebbe considerare il minore capace di concludere determinati tipi di contratti al raggiungimento di un'età precisa[100], mentre nell'altro il soggetto minorenne verrebbe considerato in grado di stipulare contratti sulla base delle conseguenze che tali contratti genererebbero nella sua sfera giuridica[101]. Il primo orientamento, necessita tuttavia di una individuazione circa le *rationes* giustificative[102] dei tipi di contratto che potrebbero venire stipulati dal minore.

Dal punto di vista europeo, al minorenne vengono riconosciute diverse capacità a seconda degli Stati Membri che si prendono in considerazione.

Nel codice civile tedesco viene tracciata l'autonomia patrimoniale del soggetto infradiciottenne a partire da due elementi fondamentali quali utilità e assenza di pregiudizio per il minore capace di discernimento. In questo codice infatti l'attenzione viene posta sulla differenza della capacità d'agire del minore più che su una sola categoria astratta di ragazzo di età inferiore ai 18 anni: il legislatore tedesco infatti al minore ultrasettenne riconosce una limitata capacità di agire (relativa alle azioni alle quali per il minore segue solamente un vantaggio giuridico). Per gli altri atti è necessario acquisisca il consenso del rappresentante legale[103].

Nel codice spagnolo, al sedicenne è riconosciuta la possibilità di porre in essere atti di ordinaria amministrazione che hanno ad oggetto beni acquisiti con il proprio

[100] È quanto accade nel caso di sottoscrizione di un contratto di lavoro che può avvenire in autonomia del ragazzo che abbia compiuto 16 anni. L. n. 977/1967.

[101] In questo caso può essere esemplificativo il contratto matrimoniale per effetto del quale il minore è emancipato di diritto (art. 390 cod. civ.), cui consegue la capacità di agire anticipata limitatamente agli atti che non eccedono l'ordinaria amministrazione.

[102] Rationes giustificative: ragioni che consentono al minore di stipulare uno dei determinati tipi di contratto citati nel testo: ad esempio una ragione potrebbe essere l'assenza di rilevanti rischi economici per il minore, un'altra potrebbe essere costituita dal fatto che ad una data età viene considerato consequenziale il raggiungimento di una certa maturità del minore che gli consente di soddisfare un particolare presupposto.

[103] R. Senigaglia, "Minore età e contratto- contributo alla teoria della capacità", G. Giappichelli, 2020, pag. 44.

lavoro esigendo il consenso dei genitori solo per gli atti di straordinaria amministrazione.

In Italia il minore che non abbia raggiunto una adeguata maturità non potrebbe prendere autonomamente decisioni di natura personale e dovrebbe essere rappresentato dai genitori che esercitano al potestà (salvo gli atti cosiddetti personalissimi).[104] Inoltre, il legislatore italiano ha previsto che il minorenne anche qualora fosse dotato della capacità di discernimento necessaria per un determinato atto personale non potrebbe porlo in essere se questo fosse per lui potenzialmente cagione di grave pregiudizio. Invece il minore capace di discernere potrebbe compiere l'atto conforme alla propria scelta personale- anche in disaccordo con i genitori- se questo non lo esponesse al rischio di gravi pregiudizi.

L'art. 2 cod. civ. fa riferimento alla capacità che acquisisce il maggiorenne al compimento della maggiore età in merito agli atti di natura patrimoniale che non potrebbe compiere ad un'età inferiore a quella dei 18 anni. L'articolo tuttavia specifica che "*Con la maggiore età si acquista la capacità di compiere tutti gli atti per i quali non sia stabilita una età diversa*" in modo tale da fornire al legislatore lo spazio per regolamentare in merito agli atti di natura personale del minore nonché alle capacità del minorenne emancipato.[105] Il minore, pur essendo incapace di agire, infatti, può compiere atti di natura personale[106] come contrarre matrimonio, previa autorizzazione del Tribunale e purché ultra sedicenne; stipulare contratti di lavoro autonomamente e anche agire autonomamente in giudizio per far valere i diritti nascenti dal contratto.

Nel caso in cui il soggetto minorenne sia emancipato, inoltre, come riconosciutogli dall'art 394 cod. civ., può compiere da solo gli atti che non

[104] Cit. nota 102, pag. 33. Gli atti personalissimi sono atti riguardanti le scelte fondamentali di vita dell'incapace d'agire, sono legati quindi alla sfera più intima della persona, perciò non si può ammettere che vengano compiuti da un soggetto diverso dalla stessa. Tra essi sono compresi il matrimonio, il riconoscimento del figlio naturale, il testamento, la donazione, e altresì, la prestazione del consenso informato ai trattamenti sanitari, il consenso in ordine all'inseminazione artificiale.

[105] M. Cinque, "Il minore contraente- contesti e limiti della capacità", CEDAM, 2007, pag. 56.

[106] Gli atti di natura personale sono atti che coinvolgono la sfera esistenziale e la fisicità del soggetto che ne è titolare.

eccedono l'ordinaria amministrazione e può, con l'assistenza del curatore, riscuotere i capitali sotto la condizione di idoneo impiego e stare in giudizio sia come attore, sia come convenuto. L'art 108 della l. n. 633/1941 aveva lo scopo di consegnare nel minor tempo possibile al soggetto non ancora maggiorenne, la capacità in merito agli atti che coinvolgevano la sua sfera più personale e un giudizio riguardo all'assenza di consistenti rischi nella concessione dello spazio di autonomia dei "*grand mineurs*"[107].

paragrafo 2.2 Il trattamento dei dati personali del minorenne.

Quando si parla di contratti online, è bene tenere presente che non esistono solamente quelli che prevedono il pagamento di un corrispettivo in denaro in cambio di un bene od un servizio; esistono, e sono anche molto diffusi, gli accordi che per l'erogazione di un servizio richiedono dei dati appartenenti all'utente. In questi casi viene prevista, in qualità di corrispettivo, la cessione dei dati personali. È il caso che si verifica quando ci si iscrive ai *social network*: è vero che sono gratuiti in quanto l'iscrizione in sé non comporta il pagamento di una quota, tuttavia sarebbe errato ritenere che non abbiano scopo di lucro o che forniscano servizi di messaggistica e intrattenimento senza ricavarne dei vantaggi.

Secondo un ricercatore della Cambridge Analytica[108], Michal Kosinski, sono sufficienti informazioni su 70 "Mi piace" messi su Facebook per sapere più cose sulla personalità di un soggetto rispetto ai suoi amici, 150 per saperne di più dei genitori del soggetto e 300 per superare le conoscenze del suo partner; inoltre con una ulteriore quantità di "Mi piace" è possibile conoscere più cose sulla personalità rispetto a quante ne conosca il soggetto[109]. Il fatto che al minorenne

[107] Il "grande minore" (traduzione di "grand mineurs") è l'adolescente che ha conseguito un livello di maturità che lo rende capace di discernere, saper distinguere le scelte conformi al proprio interesse da quelle a esso contrarie. Tale concetto ricorre nel saggio M. Cinque, "Il minore contraente- contesti e limiti della capacità", CEDAM, 2007, pag. 82.

[108] La Cambridge Analytica è un'azienda britannica di consulenza e marketing online fondata nel 2013 e successivamente chiusa con la dichiarazione di bancarotta il 2/05/2018 a seguito dello scandalo legato all'utilizzo dei dati volto ad influenzare le campagne elettorali che l'ha coinvolta insieme alla nota piattaforma social network Facebook.

[109] Articolo del quotidiano online "il Post" intitolato "Il caso Cambridge Analytica, spiegato bene-

sia concesso di manifestare il consenso al trattamento ma contemporaneamente gli venga negata la possibilità di accordare il consenso contrattuale, si traduce nella privazione di effettività del potere di concedere il consenso al trattamento stesso dei dati, che determina il pregiudizio di un diritto della personalità. Ecco perché si rende necessario riconoscere la capacità contrattuale del minore in una serie di casi.[110]

A livello europeo nel caso in cui venga richiesto il consenso per il trattamento dei dati personali, il Regolamento Generale sulla Protezione dei Dati ha stabilito all'art.8 che l'offerta diretta di servizi digitali è vietata ai minori di 16 anni. Ne consegue che viene introdotto il "consenso digitale" valido a partire dai suddetti 16 anni, mentre in caso di età inferiore[111] il trattamento viene considerato lecito solamente in caso di autorizzazione da parte del titolare della responsabilità genitoriale.[112] Agli Stati membri dell'UE viene tuttavia riconosciuto dall'art.8.1 del medesimo Regolamento la possibilità di derogare al limite minimo d'età per poter presentare validamente il consenso a patto che tale età non sia inferiore ai 13 anni. L'Italia ha pertanto fissato, nel rispetto di tale indicazione, un limite di 14 anni con il Codice Privacy[113] entrato in vigore il 20 settembre 2018.

Gli spazi di autodeterminazione e di autonomia del minore (sintetizzati dal diritto all'ascolto[114] e alla capacità di discernimento) contribuiscono a legare validità e effettività, reclamando l'adeguamento delle regole e l'attivazione dei congegni autocorrettivi nonché delle tecniche di differenziazione del sistema giuridico. L'inferenza è che la capacità di discernimento ha dimensionato la semantica della capacità di agire, assurgendo a categoria conformativa della capacità

Perché Facebook è di nuovo oggetto di accuse e critiche su come gestisce i nostri dati, e cosa c'entrano Donald Trump e la Russia", scritto da E. Menietti, 19/03/2018.

[110] R. Senigaglia, "Minore età e contratto- contributo alla teoria della capacità", G. Giappichelli, 2020, pag. 71.

[111] L. n. 633/1941, art 97.

[112] A. La Lumia, A. Dario, "Minori, internet e social network", Giuffrè, 2021, pag.24.

[113] Codice Privacy, d.lgs. n. 101/2018, art 2-quinquies.

[114] Art. 336 bis cod. civ.: "Il minore che abbia compiuto gli anni dodici e anche di età inferiore ove capace di discernimento è ascoltato dal presidente del tribunale o dal giudice delegato nell'ambito dei procedimenti nei quali devono essere adottati provvedimenti che lo riguardano.".

contrattuale e di qui incidendo, a diversi livelli, sulle regole, i concetti, i ruoli e le procedure che articolano il diritto civile minorile.

Piattaforme come Instagram[115] e affini, per citare le più usate in Italia, raccolgono dati personali degli utenti che vi si registrano e costituiscono preziosissime risorse per le aziende che vogliono avviare online delle campagne di *marketing* alla ricerca di acquirenti. In un articolo del Sole 24 Ore del 2018, Instagram, godeva già non solo di un'ottima visibilità, ma anche di un valore tutt'altro che trascurabile: se fosse stata un'azienda autonoma, secondo Bloomberg, sarebbe valsa già all'epoca 100 miliardi di dollari, e le stime di allora prevedevano che nei successivi 5 anni, gli utenti attivi sarebbero passati da un miliardo a due.[116]
Il valore sempre crescente dei social dipende dal numero di utenti attivi che questi possono vantare: il numero degli utenti è particolarmente rilevante per chi voglia avviare delle campagne elettorali[117], o per motivi di *marketing*; solo acquisendo le informazioni dei social infatti, le aziende interessate a pubblicizzare i propri

[115] Instagram: considerato come il social della bellezza e dell'estetica, nonché del racconto tramite video o immagini è molto diffuso soprattutto tra i giovani. Tale applicazione permette di scattare delle foto e di utilizzare dei filtri per modificarle rendendole più gradevoli, inoltre possono anche essere accompagnate da una didascalia costituita da testi lunghi o brevi a seconda delle preferenze di chi la pubblica. Prevede che i minori di 13 anni non possano iscriversi e che i minori di 16 possano solo con il consenso del genitore, le stesse previsioni valgono per WhatsApp.

[116] Articolo online del Sole 24 ore "Così Instagram ha centuplicato il suo valore e oggi può salvare Facebook", S. Biagio, 29 giugno 2018.

[117] È il caso che ha fatto scandalo nel 2018 che ha visto come protagonisti Facebook e la società di consulenza britannica Cambridge Analytica. Sostanzialmente, grazie alla collaborazione di un ex dipendente di quest'ultima, si era scoperto che la società di consulenza avesse usato per la propaganda politica i dati Facebook di 87 milioni di utenti Facebook senza il loro consenso. I dati in questione consistevano nel numero di "mi piace" messi da ogni utente e a quali post, così sotto a quali lasciassero il maggior numero di commenti, i luoghi da cui condividevano i contenuti e altre informazioni di questo genere che venivano poi elaborate da algoritmi in modo tale da creare un profilo psicologico per ogni utente così da presentargli gli aspetti del candidato politico che volevano promuovere. Quanto alla modalità con cui tali informazioni private fossero venute a conoscenza della Cambridge Analytica, si fa riferimento all'iscrizione degli utenti Facebook tramite il proprio profilo del social in questione all'applicazione "this is your digital life" che assicurava di produrre profili psicologici e di previsione del comportamento di chi vi si iscriveva, basandosi sulle loro attività online svolte e dei loro contatti su Facebook (successivamente la stessa piattaforma social ha fatto in modo che le reti di amici non fossero più accessibili alle app che utilizzassero Facebook Login. Già nel 2015 sulla nota rivista del The Guardian era stata segnalata una condotta illecita simile attuata all'epoca anche se lo scandalo è scoppiato solo il 17/03/2018, data in cui sono stati rilasciati articoli a riguardo da eminenti testate giornalistiche americane quali "The Observer" e "The New York Times". V. Gheno e B. Mastroianni, "Tienilo acceso- posta, commenta, condividi senza spegnere il cervello", Longanesi, 2018, pag 63.

prodotti riescono a creare delle pubblicità targhetizzate che gli consentano di raggiungere e persuadere il maggior numero possibile di ipotetici futuri acquirenti.

Sono proprio questi ultimi a fornire tutte le informazioni possibili, e anche di più, ai social media. In un primo momento cedendo i loro dati personali al momento dell'iscrizione, successivamente con le tracce che lasciano online: ogni *like* lasciato, ogni post condiviso o ricondiviso, ogni commento reso pubblico, per non parlare delle domande che pone il social all'utente allo scopo dichiarato di presentargli contenuti maggiormente in linea con i suoi interessi. La richiesta dell'età, oltre a questo, potrebbe essere anche un metodo di identificazione degli utenti per verificare che abbiano i requisiti per poter essere tali, ovvero che abbiano l'età che gli consenta di avere una propria pagina social gestita in autonomia. Si può vedere la ricerca di queste informazioni da parte dei gestori dei social che la pongono in essere come una delle azioni di tutela dei più piccoli auspicate dal Codice di autoregolamentazione per i servizi Internet, che insieme all'articolo 4 lettera "c" enuncia i principi di tutela della dignità umana e dei minori: "*La protezione dei minori impone il rifiuto di tutte le forme di sfruttamento, in particolare quelle di carattere sessuale, e di tutte le comunicazione ed informazioni che possono sfruttare la loro credulità; il rispetto della sensibilità dei minori impone inoltre cautela particolare nella diffusione al pubblico di contenuti potenzialmente nocivi*".

I dati personali in questione, vista la loro importanza, sono tutelati dal testo unico in materia ovvero il decreto legislativo numero 196 del 2003. Questo conferma la previsione di appositi codici deontologici cui devono attenersi i fornitori di servizi di informazione e comunicazione in rete per garantire la sicurezza dei dati personali dei propri utenti. Lo scopo di tale strumento è quello di informare questi ultimi riguardo all'uniformità di trattamento dei loro dati personali; e per garantire la sicurezza circa trasparenza, riservatezza, ed uso corretto dei dati che "viaggiano" in rete, il medesimo testo unico dispone la pubblicazione dei codici di autodisciplina sulla Gazzetta Ufficiale. Riassumendo, quindi, la prescrizione dei codici insieme al controllo delle autorità pubbliche sono considerate necessarie alla salvaguardia degli interessi comuni nonché alla garanzia di un quadro normativo che sia omogeneo in merito alle regole di autodisciplina.

La pubblicazione dei codici però, non è detto basti per conferire loro una specifica forza prescrittiva: si rende infatti necessario un controllo da parte delle autorità pubbliche sia per salvaguardare la tutela degli interessi comuni, sia per garantire un quadro normativo omogeneo sulle regole di autodisciplina.

Al medesimo fine, è stato emanato il Regolamento europeo meglio noto come GDPR, ovvero General Project Data Regulation[118] il quale, agli artt. 7 e 40, disciplina, in merito al trattamento dei dati personali, che la prestazione di servizi è condizionata dal fatto di acconsentire il trattamento stesso, mentre all'articolo 40, sancisce che il titolare di tale trattamento, debba obbligatoriamente adottare il codice di condotta che ne garantisca la trasparenza.

Per tutti gli utenti che sottoscrivano un accordo in merito al trattamento dei propri dati personali inoltre è prevista la possibilità di esercitare il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò[119].

Nonostante la previsione di tali tutele, nell'ambito dell'e-commerce si registra una grave lacuna in merito al tema della protezione dei minori, in particolare nel Codice di comportamento europeo in materia di rapporti commerciali online. Tale Codice Euro- Label è stato promosso in Italia da Confcommercio allo scopo di assicurare la correttezza dello scambio di informazioni precontrattuali riguardo a prodotti e sicurezza della garanzia pre e post-vendita dei siti commerciali che vi aderiscono.

---

[118] GDPR, ovvero il regolamento generale sulla protezione dei dati elaborato dal Comitato europeo per la protezione dei dati. Nato dall'intenzione di proteggere i diritti e le libertà delle persone fisiche, è stato pubblicato sulla Gazzetta Europea il 4/05/2016 è stato applicato a decorrere dal 25/05/2018 con l'obbligo per le realtà aziendali europee, pubbliche o private, di adeguarvisi entro un limite massimo di tempo che consisteva in 2 anni.

[119] L'art. 7 EU RGPD, "Condizioni per il consenso" al comma 3 enuncia che" L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato." Parlando di RGPD si fa riferimento alla l. 119/1 che è il regolamento europeo 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 e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

Tuttavia la *privacy* degli utenti è da difendere anche da altri utenti, non solamente dai gestori dei social di cui fanno uso: nel momento in cui si è in rete bisogna decidere cosa si vuole condividere e con chi. Anche qualora sul social siano state impostate tutte le restrizioni sulla *privacy*, è necessario ricordare che comunque quanto pubblicato in rete esce dal controllo di chi ha condiviso ed è potenzialmente visibile a tutti se qualcuno che lo osserva fa lo *screenshot* e lo ricondivide[120]. Lo stesso concetto di privacy assume una connotazione differente per i ragazzi che si iscrivono ad uno o più social: sembra quasi che alcuni lo facciano ma preferiscano poi mantenere l'anonimato oppure ancora che vogliano eludere le richieste dei coetanei circa le proprie abitudini, sia perché non hanno voglia di condividere situazioni familiari pesanti, sia perché non ritengono di voler dire alcunché. Eppure, secondo questa loro nuova concezione di *privacy*, per averla sono disposti a sacrificarne una parte pubblicando un po' di quanto accade loro nella propria quotidianità, per mantenere riservati altri aspetti della loro vita che non pubblicano per evitare gli vengano fatte domande. Lo stesso motivo è riferito anche ai genitori dei ragazzi affezionati alla propria *privacy* anche se suscita non poca apprensione nei primi, convinti che i loro figli abbiano quindi qualcosa da nascondere, anche se non è necessariamente vero. Così facendo, la curiosità degli altri utenti viene saziata, si sentono come se conoscessero la persona in questione che pubblica contenuti relativi ad una piccola parte della sua vita che in realtà sta solo mostrando agli altri utenti ciò che vuole vedano.

Non è sempre detto però, che i giovanissimi internauti siano consapevoli di questa possibilità, a volte infatti arrivano a fare un uso improprio dei social pubblicando contenuti che non sembra prendano in considerazione l'eventualità che vengano visti da possibili futuri datori di lavoro[121]. Anche se i *social* vengono utilizzati per farsi notare e per affermare il proprio status e per pubblicizzare la propria appartenenza a questo o quel gruppo, non è affatto detto che gli unici

[120] T. Maggi, "Giovani connessioni- orientarsi con i figli nel web", San paolo edizioni, 2020, pag. 97.

[121] È indicativo il caso verificatosi negli Stati Uniti che aveva per protagonista un ragazzo che non è stato ammesso all'accademia a cui aveva fatto domanda. Nonostante la domanda fosse stata fatta in maniera ineccepibile, gli esaminatori della sua ammissione controllarono il suo profilo Facebook personale, scoprendo che fosse pubblico e che contenesse immagini relative alla gang responsabile dei disordini del quartiere cui apparteneva. Vista tale attività online, il comitato di ammissione ha deciso di non ammetterlo all'istituto cui tanto teneva.

spettatori dei contenuti messi online siano gli amici, i membri del gruppo di appartenenza (oppure di cui vuole entrare a farne parte) di cui si cerca l'approvazione, i *follower* nel momento in cui il materiale viene pubblicato, e chi commenta quanto gli viene offerto: vi sono anche molti spettatori silenziosi che non commentano alcunché, ma, per il fatto di avere una connessione ed essere *follower*, vengono a contatto con informazioni preziose che possono decidere il futuro di chi le ha messe in rete. Per esempio, il futuro può essere deciso dai datori di lavoro che osservano le attività in rete dei possibili collaboratori che stanno selezionando, anche sulla base di ciò che osservano collegato alle loro attività online ed ai contenuti pubblicati sui loro profili *social* (se pubblici).

La *privacy* del giovane navigatore della rete è quindi necessario venga tutelata dalla legge sia verso i gestori dei social a cui si iscrive, sia dagli altri individui che hanno accesso ai suoi contenuti pubblicati, e il primo modo per garantire tale protezione è dato dall'educazione civica digitale ricevuta dal minore che si affaccia al mondo online, in modo da avventurarvisi in modo consapevole e da sfruttarlo con saggezza[122].

paragrafo 2.3 La responsabilità extracontrattuale dell'acquirente d'età inferiore ai 18 anni.

Nonostante le tutele per i minori online e per il patrimonio delle loro famiglie da acquisti indesiderati fatti in rete dai figli, alle volte, a necessitare di tutela dai minorenni stessi, sono i venditori che danno la possibilità di stipulare contratti online.

In questa sede trattiamo del pericolo relativo alla conclusione del contratto da parte del minore che, mentendo circa la propria età, truffa il venditore al fine di concludere il contratto online. Il professionista infatti, per ampliare i profitti e suscitare l'interesse di quanti più possibili clienti, dà l'opportunità di concludere contratti di compravendita in modalità telematica, nonché di effettuare acquisti in-

[122] T. Maggi, "Giovani connessioni- orientarsi con i figli nel web", San paolo edizioni, 2020, pag. 66.

app, ovvero, prevede la possibilità per l'acquirente di effettuare compere anche dalle applicazioni di dispositivi mobili.

La particolarità di queste possibilità offerte dal professionista, risiede in azioni precostituite e dirette alla conclusione del contratto, che ne semplificano sensibilmente la procedura, rendendo più accessibile l'esperienza dell'acquisto, che è più semplice e veloce, ed in una società che sperimenta una costante corsa contro il tempo, questi aspetti rendono l'intero processo ancora più allettante. Tuttavia, non sempre è un bene, perché proprio l'aspetto dell'immediatezza e della semplicità, rendono tale procedura d'acquisto invitante anche per chi invece non potrebbe attuarla: è questo il caso degli utenti minorenni. Questi ultimi, infatti, grazie alle procedure di conclusione del contratto rese più semplici dal limitato numero d'informazioni richieste all'acquirente, riescono ad eludere facilmente i controlli riguardo alla propria effettiva identificazione.

D'altra parte, però, c'è l'obbligo del venditore di riconoscere l'altro contraente, accertandosi che sia maggiorenne e quindi abilitato alla conclusione del contratto. Come per il contratto in presenza, infatti, anche per quello telematico sussiste l'obbligo di identificare correttamente l'altro contraente. Qualora ciò non avvenga, la piattaforma di e-commerce non potrà che essere ritenuta responsabile per aver colposamente ignorato l'incapacità dell'altra parte. Questo è quanto previsto dal regolamento emesso dal Ministero delle poste e delle comunicazioni riguardo alle norme sulle modalità di espletamento dei servizi *audiotex* e *videotex*[123], numero 385 del luglio 1995. In esso vengono disciplinate le procedure d'esercizio dei servizi sopra citati, specificando che gli operatori devono fare il possibile per evitare l'accesso ai servizi agli utenti minorenni, inoltre

[123] I servizi audiotex e videotex sono definiti all'interno della Gazzetta Ufficiale.
In particolare, i servizi audiotex sono indicati come <<tutti i servizi che consentono, tramite l'uso di specifiche numerazioni della rete telefonica commutata, l'accesso, a pagamento, da parte degli utenti telefonici, a informazioni o prestazioni, di tipo vocale, testuale o grafico, rese disponibili da fornitori, direttamente ovvero tramite centri servizi, e contraddistinte da "modalità di espletamento", "caratteristiche e contenuti", "procedure di esercizio">>. I servizi videotex invece, i sono identificati come <<servizi che consentono, tramite l'uso di specifiche numerazioni della rete di telecomunicazioni nonché di codici alfanumerici di indirizzamento, l'accesso, a pagamento, da parte degli utenti della rete, a informazioni o prestazioni, di tipo testuale o grafico e strutturate secondo gli standard videotex internazionali, rese disponibili da fornitori, direttamente ovvero tramite centri servizi, e contraddistinte da "modalità di espletamento", "caratteristiche e contenuti", "procedure di esercizio">>.

prevedono un protocollo che l'operatore deve seguire qualora abbia il sospetto di interfacciarsi con un utente di questa fascia d'età. Anzitutto, l'operatore deve chiedere all'utente sospetto l'età e la data di nascita; successivamente, rivolgergli tre domande che possono fornire indicazioni utili sulla sua vera età se non proprio rivelarla; infine, qualora le risposte facciano sospettare l'operatore di trovarsi davanti un minore, o diano conferma di questo, l'utente deve venire considerato un minore e di conseguenza deve essere escluso dai servizi, salvo che non si tratti di uno dei servizi previsti dall'articolo 6 della direttiva europea recepita dal nostro ordinamento con il decreto legislativo numero 185 del 22 maggio 1999, in merito alla protezione dei consumatori in materia di contratti a distanza.

Il legislatore europeo si è occupato di fornire tutele specifiche ai minori attraverso un mezzo che fosse adeguato alle tecniche di comunicazione a distanza con l'articolo 4 della direttiva appena citata, che richiama i criteri di chiarezza e comprensibilità, indispensabili per fornire le informazioni commerciali al fine di proteggere i soggetti che secondo le disposizioni di legge degli Stati Membri non sono capaci di manifestare il proprio consenso, tra i quali, rientrano i minorenni.

Il venditore quindi ha responsabilità e obblighi che se rispettati dovrebbero essere sufficienti a permettergli di tutelarsi autonomamente. Qualora egli abbia rispettato tutte le norme circa le azioni da adottare ma venisse truffato, viene protetto dalla legge. Se il venditore ha adottato tutte le pratiche idonee al riconoscimento dell'altro contraente online ma quest'ultimo lo ha truffato, scatta la tutela degli interessi del venditore.

Il minore che raggiri il venditore infatti, non vede la possibilità di dichiarazione di contratto annullato dal momento che la sua condotta non viene reputata legittima e pertanto meritevole di tutela. Data la novità del fenomeno del contratto online e ancora di più, del fatto che venga utilizzato in modo improprio da soggetti minorenni, non vi sono specificazioni circa cosa si intenda con il termine "raggiri" evocato dall'articolo 1426 del codice civile; è dato sapere solamente che non costituisce "raggiro" l'età dichiarata superiore ai 18 anni da parte del minore che vuole sottoscrivere un contratto online. Lo stesso si può dire qualora egli ometta

l'informazione relativa all'età (Cassazione civile n. 2616 del 21 luglio 1954[124]). Nelle fattispecie appena riportate, ad ogni modo, si tratta di illecito extracontrattuale compiuto dal minore la cui responsabilità ricade o sui genitori o su chi doveva vigilare sui ragazzi. Si tratta quindi di responsabilità extracontrattuale che nasce a seguito dell'illecito compiuto nell'ambito di rapporti tra due o più soggetti non precedentemente legati da un vincolo contrattuale. Tale espressione inoltre viene spesso usata come sinonimo di responsabilità civile, in contrapposizione alla responsabilità contrattuale.

Vengono pertanto definite dalla legge tre differenti tipologie di responsabilità: quella relativa alla *culpa in vigilando*, il cui riferimento legale è all'art. 2048 C.C., relativo alla colpa sottostante alla responsabilità per il fatto illecito altrui, che viene attribuita a coloro che sono tenuti alla sorveglianza di determinate persone reputate non in grado di rendersi pienamente conto delle proprie azioni. Viene riconosciuta, sempre nel codice Civile anche la *culpa in educando*, al medesimo articolo, che riguarda in questo caso invece il criterio di imputazione della responsabilità dei genitori e del tutore per i danni cagionati dal fatto illecito commesso dai figli minori non emancipati o dalle persone soggette a tutela (in caso di coabitazione). Infine, nel medesimo codice, ma ad un articolo differente, per la precisione, il 2049, viene riportata la definizione di *culpa in eligendo*, che si occupa di indicare il criterio di imputazione della responsabilità di padroni e committenti, per i danni arrecati a terzi dai loro dipendenti nell'esercizio delle incombenze cui questi ultimi sono adibiti. In particolare quindi, in caso di contratto telematico, la dimostrazione che sia stato compiuto da un minorenne diviene più ardua, se tuttavia il soggetto abbia compiuto l'acquisto inserendo il proprio nome, l'onere della prova è assolto ai sensi dell'art. 13 d. lgs. n. 70/2003. Qualora il ragazzino invece utilizzasse i dati dei genitori (nome, data di nascita, carta di credito), le difficoltà circa l'assoluzione dell'onere della prova aumentano, come stabilito all'articolo 1426 del Codice Civile. La disciplina prevede due casistiche a riguardo, con due differenti tipi di onere della prova da parte del genitore o di chi ne fa le veci, in particolare: se il minore non era capace di intendere e volere

[124]A. Astone, "I dati personali del minore in rete- dall'internet delle persone all'internet delle cose", Giuffrè, 2019, pag. 48 e ss; Codice Civile.

al momento della conclusione del contratto, al genitore spetta la dimostrazione di averlo educato nonché di aver vigilato su di lui in modo conforme alle condizioni sociali, all'età, al carattere e all'indole dello stesso. Nel momento in cui invece il minore sia imputabile, il genitore deve solamente dimostrare di non aver potuto impedire il fatto, quindi, non è tenuto a dimostrare anche di avergli impartito una buona educazione, tenendo conto di quanto riportato nell'art. 2048 Codice Civile.

Capitolo 3: Il mondo online: rischi e tutele per i minorenni

Introduzione al capitolo 3

Quello degli acquisti online non è l'unico pericolo in cui possono incorrere i giovani e giovanissimi internauti.

Le fattispecie più preoccupanti per quanto concerne le dimensioni della loro diffusione nonché quella (perlopiù recente) delle norme volte a contrastarle sono infatti quelle relative al fenomeno del cyberbullismo, della pedopornografia, e quella della diffusione (la maggiore parte delle volte inconsapevole) dei dati personali. Sebbene tutti e tre i fenomeni citati siano di per sé spiacevoli, quanto veramente ha preoccupato il legislatore e le istituzioni italiane ed europee sono soprattutto le conseguenze che possono avere [125]. Le conseguenze che derivano per il soggetto dal fatto di aver esperito casi di cyberbullismo, così come quelle di essere stati sottoposti alla pratica del *revenge porn* o di essere stati esposti video pedopornografici, possono essere particolarmente gravi sia a livello psicologico sia fisico, talvolta rischiando di sfociare in gesti estremi come quelli portati alla conoscenza comune dai fatti di cronaca. Tra le soluzioni proposte dal GPDP e le Forze Armate italiane nonché il legislatore nazionale, figurano progetti di educazione civica digitale che insegnino ai ragazzi come comportarsi sul web e come riconoscere delle richieste quantomeno bizzarre (per non dire decisamente inusuali e inopportune da parte di estranei) in modo da segnalare gli account da cui sono partite e prenderne le distanze. Tali progetti educativi hanno lo scopo di prevenire che i giovani utenti siano vittime di tali problematiche veicolate dalla rete internet (suo malgrado) e coinvolgono attivamente gli istituti scolastici di ogni ordine e grado di cui i ragazzi fanno parte, in modo tale da aiutare i genitori a creare una rete di protezione dei propri figli minorenni che gli consenta di poter esercitare il proprio diritto esplicitato dalla legge 285/97[126] in sicurezza. Oltre alle iniziative di prevenzione ci sono anche da evidenziare le

[125] A. La Lumia, A. Dario, "Minori, internet e social network, Giuffrè, 2021, pag. 32 e ss. Il cyberbullismo non è di per sé un reato ma lo sono le condotte ad esso collegate come il revenge porn, sostituzione di persona, istigazione al suicidio, per citare degli esempi.

[126] La legge 285/97 reca disposizioni riguardo la promozione di diritti e di opportunità per l'infanzia e l'adolescenza.

misure sanzionatorie qualora le condotte illecite siano state poste in essere ed abbiano cagionato danno. Tra queste vale la pena citare per il cyberbullismo la legge 71/2017, il protocollo d'intesa tra il GPDP e la Polizia Postale, fino alla più recente applicazione Youpol[127]. Riguardo alla pratica del *revenge porn* e tutti i reati ad essa correlati, le sanzioni sono riportate nel Codice Penale per le varie fattispecie che sono state riassunte in una tabella nel secondo paragrafo; mentre in relazione ai dati personali e alla loro diffusione inconsapevole da parte degli utenti minorenni rivestono particolare importanza il diritto all'oblio, codici di autoregolamentazione sottoscritti dall'Associazione per la Convergenza dei Servizi di Comunicazione e da alcune associazioni di provider, senza scordare la Carta di Treviso, documento fondamentale volto a garantire, come indicato nella sua premessa, "*l'armonico sviluppo dell'identità del minorenne senza distinzione di genere, status sociale, origine etnica, nazionalità, lingua, religione e credo politico*.".[128]

[127] App creata dai tecnici informatici della Polizia di Stato italiana, divenuta operativa in tutta la nazione nel 2018. Inizialmente elaborata per denunciare episodi di bullismo e spaccio, con il tempo ha compreso al proprio interno anche fattispecie quali la violenza domestica ed il cyberbullismo (soprattutto per quanto concerne le condotte ad esso correlate che costituiscono reato). La stessa applicazione è servita ad una ragazza per sfuggire alle violenze del padre: essa infatti ha mandato il messaggio tramite quella che è stata definita dai giornali come l'app che funge da whatsapp tra il cittadino e la polizia di Stato denunciando i soprusi del padre venendo finalmente liberata dallo stesso grazie alla polizia che ha fatto irruzione nell'abitazione. T. Maggi, "Giovani connessioni- orientarsi con i figli nel web", San paolo edizioni, 2020, pag. 24.

[128] Il documento, approvato per la prima volta nel 1990 dall'Ordine dei giornalisti e dalla Federazione nazionale stampa italiana (Fnsi) con il Telefono Azzurro e gli Enti e Istituzioni della Città di Treviso, fissa le regole deontologiche riguardanti i minorenni. Esso, creato nel 1990, all'inizio della rivoluzione tecnologica della rete, ha subìto delle innovazioni già nel 2006, ma alla luce dei cambiamenti avvenuti nel mondo dei media, sono state rese necessarie ulteriori modifiche e aggiornamenti dall'Ordine dei giornalisti e Fnsi, arrivando ad assumere l'attuale versione approvata il 6 luglio 2021. La Carta trae ispirazione dai principî e dai valori della Costituzione, della Convenzione Onu sui diritti dell'infanzia e dell'adolescenza, recepita in Italia dalla legge n. 176/1991, delle normative internazionali ed europee e della legge istitutiva dell'Ordine dei giornalisti (n. 69/1963) per estensione dell'art. 2.

paragrafo 3.1 Il problema del cyberbullismo

Tra i rischi che i minori corrono online, vi sono senz'altro quelli di incorrere in condotte che hanno come unico obiettivo quello di provocare danni a un coetaneo incapace di difendersi, meglio note con il termine di cyberbullismo. Spesso viene confuso dai giovani e giovanissimi con il bullismo dal momento che l'obiettivo è lo stesso, ma il cyberbullismo, oltre ad avere delle caratteristiche differenti nei modi in cui si manifesta è un fenomeno più recente. Viene definito *border-line*[129] tra devianza giovanile e psicologia dei gruppi e si manifesta quando i minori usano i media per veicolare o mettere in atto azioni vessatorie, persecutorie, lesive della dignità dei coetanei. Il cyberbullo infatti, grazie ai dispositivi multimediali è in grado di inserirsi nella vita privata della vittima sempre e senza limiti con messaggi video audio immagini offensivi verso la vittima mandati a lei o pubblicati in rete. La gravità del fenomeno sta nell'impatto che ha sulla vita dei bersagli, in particolare sulla loro identità in formazione. Il minorenne si sente "grande", perché sta facendo qualcosa che di solito nella vita reale non fa; si sente al sicuro grazie all'anonimato che percepisce come garantito dal fatto di stare dietro ad uno schermo. Inoltre, sperimentare questa percezione di sicurezza può portarlo a sfogarsi nel mondo che, secondo le sue convinzioni infondate, non lo riconoscerà mai, sfogando le emozioni negative che accumula nel mondo reale, nella realtà virtuale talvolta con un *account* appositamente creato all'uopo.[130] Tuttavia i giovani utenti troppo spesso hanno poca consapevolezza circa il fatto che ciò che avviene online ha ripercussioni sulla vita reale e sulle relazioni e forse è proprio questa assenza di consapevolezza che ha determinato un aumento della diffusione di tale fenomeno come dimostrato dai numeri di denunce fatti nel 2017[131].

---

[129] A. La Lumia, A. Dario, "Minori, internet e social network", Giuffrè, 2021, pag. 32 e ss.

[130] Il riferimento allo "sdoppio di personalità" del giovane utente che si sfoga in internet è riportato nel libro di G. Lavenia, "Mio figlio non riesce a stare senza smartphone", Giuntiedu, 2019, pag. 29 e ss.

[131] Nel 2017, a conferma che il fenomeno di cyberbullismo stia conoscendo un periodo di proliferazione, la Polizia Postale ha raccolto 325 denunce e 37 minori sono stati denunciati all'Autorità Giudiziaria; una crescita indesiderata, tanto da portare, nel 27/03/2018, alla firma di un accordo tra il Capo della Polizia Franco Gabrielli e il Capo del Dipartimento per la Giustizia Minorile e di Comunità Gemma Tuccillo che sancisce collaborazione tra il Dipartimento e la Polizia di Stato al fine di rinforzare il sistema di tutele dei minori in riferimento ai pericoli del web, in continuità con gli adempimenti introdotti dalla l. n. 71/2017.

Il cyberbullismo è la manifestazione online del bullismo dal quale però si allontana per via di alcune caratteristiche che non coincidono, a partire dal profilo psicologico dell'aguzzino che li mette in atto. Mentre il bullo è un soggetto dotato di forte personalità, spesso con accanto dei complici; il cyberbullo invece è debole, il più delle volte è vittima di episodi di bullismo nella vita reale che lo caricano di un risentimento tale da crearsi un profilo social apposito, sotto falsa identità, con il quale dare libero sfogo alla sua rabbia non assumendosi alcuna responsabilità, dal momento che si sente protetto dall'anonimato virtuale[132]. Il bullo invece si prende la responsabilità delle sue azioni, o per meglio dire, se ne vanta con la sua cerchia ristretta, rivendicando la propria identità in quanto autore della condotta posta in essere; sa di avere delle responsabilità, ma nel momento del confronto con un adulto cerca di porre il fatto su un piano scherzoso. Altro aspetto rilevante riguarda la condotta stessa: il bullo può metterla in pratica per un arco di tempo ristretto, così come gli spazi in cui essa può verificarsi; il cyberbullo invece la può praticare sempre, in qualsiasi momento della giornata, e da qualsiasi luogo, a condizione di avere una connessione alla rete: non vede la reazione della vittima, come invece accade al suo "collega" del mondo reale, in questo modo non viene in alcun modo disincentivato a reiterare la condotta. Non si può rendere conto dei danni che sta infliggendo alla sua vittima, non avendola innanzi a sé. Il più delle volte ad essere sconosciuta, non è solo la reazione della vittima, ma anche l'identità del cyberbullo al bersaglio, che non sa come difendersi da un nemico che neppure conosce e che potrebbe essere chiunque e operare da qualunque luogo; in caso di bullismo invece, la vittima conosce bene i suoi aggressori, dal momento che il più delle volte sono suoi compagni di scuola o di attività extra scolastiche. È infatti stato rilevato che il fenomeno trattato in questa sede sia in crescita soprattutto tra gli adolescenti, come denotano i dati del report dell'Osservatorio Nazionale Adolescenza del

Fonte:" Cyberbullismo: Giustizia Minorile e Polizia di Stato insieme per la tutela dei minori", Diritto e Giustizia, 28/03/2018.

[132] Da notare come in tutta la bibliografia consultata, la rabbia di chi attua la condotta offensiva è sempre supportata da motivazioni inerenti alla sua vita quotidiana nel mondo offline, composte da fattispecie complesse. Nel libro di d. boyd, "It's complicated", Castelvecchi edizioni, 2014, pag. 162 e ss., l'autrice tiene a specificare che il bullo agisce e reagisce con aggressività per affrontare i propri problemi, ed è ben diverso dal sociopatico che arreca danno agli altri per il puro piacere di farlo.

2017: il 10% di adolescenti tra 11 e 13 anni, dichiara di essere stato vittima di prepotenza e soprusi in rete, medesima dichiarazione viene fatta dall'8,5% di ragazzi tra 14 e 19 anni[133].

Tra i fattori che motivano i cyberbulli a perpetrare le proprie condotte vi è la percezione di anonimato che si sentono conferire dalla rete: non sono faccia a faccia con il bersaglio delle proprie azioni ma vi è un mezzo tecnologico tra l'uno e l'altro, uno schermo, una connessione e a volte, nel tentativo infantile di non farsi rintracciare, un profilo falso, per poter agire sentendosi abili nel mantenere l'anonimato. Sperimentare questa percezione di sicurezza data dal fatto di operare da dietro un media device celando, seppure in modo maldestro, la propria identità, può portare il minore a sfogarsi nel mondo che secondo le sue convinzioni infondate, non lo riconoscerà mai, riversando così le emozioni negative che accumula nel mondo reale, nella realtà virtuale che consente di fare ciò che con la sua identità reale riconoscerebbe essere contrario al buon senso.

La possibilità data dai media di creare un nuovo sé stesso, quindi, può generare uno sdoppiamento di personalità nel ragazzo, che a furia di subire soprusi nella sua realtà quotidiana, può trasformarsi in un cyberbullo per farsi giustizia da solo.[134]

È necessario tenere in considerazione, tuttavia, che talvolta il cyberbullo può non essere una vittima del bullismo, ma semplicemente un ragazzino con molta rabbia repressa o desiderio di attenzione che sfoga online su vittime più o meno casuali, sentendosi protetto dal proprio *nickname* non riconducibile a sé nel mondo reale. Le conseguenze del cyber bullismo però, sono tutt'altro che assenti nel mondo reale della vittima, che si ritrova accerchiata sia online che offline.
Nel primo, viene costantemente derisa o minacciata, con un livello di invadenza della propria vita privata potenzialmente massimo, il più delle volte senza nemmeno riuscire a capire chi sia il proprio carnefice.

[133] G. Lavenia, "Mio figlio non riesce a stare senza smartphone", Giuntiedu, 2019, pag. 30.
[134] A. Cazzullo con R. e F. Maletto Cazzullo, "Metti via quel cellulare– un papà. due figli. una rivoluzione.", Mondadori, 2017, pag. 51 e ss.

Nel secondo, la vittima non sa di chi fidarsi, non sa di chi sospettare, inizia a vivere una condizione d'ansia generalizzata che la porta a non voler più uscire di casa, incapace di spiegare il motivo a causa della vergogna che prova per gli atti che compie nei suoi confronti il cyberbullo, non sa come fare finire questa spirale di soprusi e minacce.

È stato trattato il profilo psicologico del bullo cibernetico, ma non quello della vittima online con conseguenze offline. Questo perché quest'ultima figura potrebbe essere chiunque: non occorre sia un ragazzo emarginato o diverso in qualche modo dai suoi coetanei, potrebbe essere chiunque, anche il più popolare che come unica colpa ha quella di aver suscitato l'invidia del cyberbullo che desidera ad ogni costo sentirsi alla sua altezza, se non migliore. La vittima di solito diviene oggetto di scherno generale, magari con un video o un'immagine che la ritrae mentre fa qualcosa di insolito o di cui normalmente si vergognerebbe, ripresa in una particolare situazione, magari destinata a non ripetersi, ma una volta che viene decontestualizzata mettendola online dal cyberbullo, l'impressione può essere assai diversa, e peggiore. La vittima inizia a sentirsi giudicata da tutti, magari senza che nemmeno abbiano visto il contenuto comunque diventato virale, e non sa nemmeno a chi rivolgersi per chiedere aiuto, dal momento che prova vergogna per l'impressione che potrebbero avere i suoi genitori, oppure anche di tradire la loro fiducia, per non parlare del timore di una punizione.

La persona oggetto di scherno online, non si riconosce nel comportamento adottato nella situazione divenuta virale e fraintendibile dal momento che è stata decontestualizzata, teme di perdere le proprie amicizie, non sa come verrà considerata dalle stesse, teme anche che rispondendo a chi ha diffuso l'immagine o il video incriminato possa peggiorare la situazione, che spera sia solo transitoria e termini in fretta.

Purtroppo, pensare che la gogna mediatica sia una condizione transitoria, è un errore frequente nei ragazzi, che si ritrovano a parlarne con i genitori dopo molto tempo quando la situazione è ormai divenuta insostenibile. È importante che i genitori creino un clima disteso che favorisca il dialogo coi figli, e si accorgano dei segnali che questi danno: la carente voglia di uscire di casa, il calo del

rendimento scolastico, la mancanza di appetito, l'umore differente dal solito sono dei validi indizi. Prestare attenzione a comportamenti insoliti può aiutare a cercare un dialogo col minorenne, cercando di ascoltare quanto ha da dire, senza sminuire ciò che prova, né interromperlo, tantomeno contraddirlo.

Nei casi meno gravi, può essere sufficiente che il minore venga accompagnato dalle sue figure adulte di riferimento in un percorso di "*detox* tecnologico": dedicando mezz'ora a fare attività all'aria aperta col telefono spento, creando spazi d'ascolto di sé e delle proprie emozioni, creando luoghi off-limits per la tecnologia. Se ciò non dovesse bastare e la fattispecie concreta fosse più grave, si può fare ricorso ad uno psicoterapeuta che attraverso un percorso studiato sulla base della problematica e delle esigenze della famiglia che chiede il suo aiuto, riporti alla socialità il ragazzo.[135] Il tutto naturalmente dopo aver avvisato le Autorità e proceduto al rintracciamento delle persone che hanno portato il cyberbullismo alla sua degenerazione in azioni penalmente rilevanti quali molestie, violenza privata, interferenza abusiva nelle vite delle persone, stalking, lesioni personali, istigazione al suicidio nonché omicidio. Non esiste infatti una legge che definisca il cyberbullismo come un reato. Pertanto, in sé non può venire considerato né tantomeno sanzionato come tale.[136] Lo stesso non può dirsi per le condotte ad esso integrabili come la diffusione di immagini sessuali di coetanei[137] di cui si tratterà nel prossimo paragrafo o il furto d'identità che verrà approfondito in tale sede. Quest'ultimo rientra nella fattispecie della creazione di un falso profilo su un social network che può essere di due tipologie differenti: quella in cui il creatore del profilo fasullo utilizzi una foto vera procuratasi da qualche chat oppure scaricata dalla rete; o la tipologia in cui colui che crea il profilo lo fa verosimile a quello che potrebbe essere fatto dalla persona reale associando alla foto il vero nome dell'individuo in essa ritratta senza però essere

[135] G. Lavenia, "Mio figlio non riesce a stare senza smartphone", Giuntiedu, 2019, pag. 100.
[136] M. P. Fontana (assistente sociale specialista, sociologa e formatrice),"Cyberbullismo: famiglia, scuola e servizi dopo la legge 71 del 2017", Questione giustizia, 20/12/2017 (Questione giustizia è una rivista di Magistratura Democratica con analisi e riflessioni su giustizia, magistratura e società; nata nel 1982 come rivista cartacea trimestrale, dal 2013, le si affianca Questione giustizia online, rivista ad accesso libero e quotidianamente aggiornata.); A. Astone, "I dati personali del minore in rete", Giuffrè, 2019, pag. 65 e ss.; A. La Lumia, A. Dario, "Minori, internet e social network", Giuffrè, 2021, pag. 32 e ss.
[137] A. Thiene, "Ragazzi perduti <<online>>: illeciti dei minori e responsabilità dei genitori", Dogi, 2018.

lei. In entrambi i casi l'autore o autrice del "*fake*", incorre nel reato di sostituzione di persona di cui all'articolo 494 del Codice Penale come stabilito dalla Cassazione con sentenza 25774/2014[138].

Spesso, nell'occhio del mirino dell'opinione pubblica, finiscono i mezzi che hanno reso possibile tale fattispecie spiacevole: i social, imputati del processo contro il cyberbullismo. Questi ultimi in realtà sono solamente mezzi con l'unica caratteristica di essere straordinari strumenti di amplificazione acritici. I loro gestori tuttavia, volendo difendere i propri utenti assieme ai propri profitti, si sono dati da fare per impedire l'uso distorto dei *social network,* di cui sono responsabili o addirittura proprietari, da un numero sempre maggiore di utenti. Facebook Italia, ad esempio, ha creato la piattaforma anti bullismo: chi segnala episodi di bullismo sul sito viene direttamente indirizzato in questa specifica piattaforma dove può trovare: informazioni utili in caso di necessità, ma anche consigli validi per affrontare questo tipo di problema oltre a suggerimenti su come comportarsi a seconda delle circostanze.

Un altro strumento messo a disposizione degli utenti e delle famiglie dalla medesima piattaforma è il Facebook *safety*: una pagina per la sicurezza delle famiglie.[139]

Nel 2017, il Parlamento italiano ha fornito ai suoi giovani utenti di un ulteriore strumento di tutela: la legge numero 71 entrata in vigore nel giugno del medesimo anno, allo scopo di prevenire i danni delle manifestazioni di abusi, vessazioni e denigrazioni che imperversano nella rete ed hanno per protagonisti i minori. È stata proprio la vicenda di una di questi, alunna della prima senatrice firmataria della proposta di legge poi denominata "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo"*,* a determinare la sua ideazione e approvazione. La vicenda tristemente nota ha per protagonista una vittima delle conseguenze del cyberbullismo che quella stessa legge si impegna a contrastare: la ragazza, a seguito della diffusione di un video che la ritraeva

[138] R. Razzante, "Informazione: istruzioni per l'uso - notizie, rete, e tutela della persona ",Cedam, 2014.
[139] M. Faccioli, "Minori nella rete -pedofilia, pedopornografia, deepweb, social network, sexting, gambling, grooming, e cyberbullismo nell'era digitale. Analisi e riflessioni su giovani e giovanissimi navigatori nei lati oscuri del web" Key editore, 2015, pag. 37 e ss.

ubriaca mentre dei coetanei simulavano con lei un rapporto sessuale, ha deciso di suicidarsi a Novara nel 2013[140].

Alla legge del 2017[141] non si può non riconoscere il merito di aver reso la materia di cui tratta una priorità delle politiche educative, tanto da rendere indispensabile il dialogo tra istituzioni in modo tale da costituire una rete protettiva capace di responsabilizzare circa il corretto uso e prevenire o correggere le degenerazioni dell'uso scorretto di Internet.

Allo stesso tempo, tuttavia, la scelta del legislatore di considerare solamente il cyberbullismo e non anche il bullismo che potremmo definire off-line, analogico, ha suscitato non poche perplessità. Nelle situazioni che coinvolgono fenomeni come il bullismo e il suo simile cibernetico, infatti, spesso sono presenti entrambi e generano una spirale nella quale è difficile riconoscere se l'inizio è scaturito nella vita reale o da una condotta virtuale. La difficoltà di distinzione non coinvolge invece la definizione di cosa la suddetta legge identifichi con il termine "cyberbullismo", ovvero: «*qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on-line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso o la loro messa in ridicolo*».

Con la nuova legge quindi, non vengono introdotte nuove fattispecie di reato dal momento che il cyberbullismo ospita al proprio interno varie tipologie di illeciti che già trovano una previsione penalistica all'interno dell'ordinamento italiano. L'intento del legislatore infatti, è quello di fornire solide basi alle iniziative di prevenzione ed educazione dei minori, dando particolare importanza all'istituzione scolastica ed i suoi interventi formativi ed informativi, volti a

[140] M. P. Fontana, " Cyberbullismo: famiglia, scuola e servizi dopo la legge 71 del 2017", Questione giustizia, articolo scritto il 20/12/2017.

[141] Il riferimento è alla legge 71/2017 che in materia di cyberbullismo è una delle prime in Europa, e dà notevole importanza all'Autorità Garante per la Protezione dei Dati Personali: infatti gli ultra quattordicenni e i genitori dei ragazzi possono rivolgersi ad essa per chiedere la rimozione dei contenuti lesivi presenti su internet.

fronteggiare la complessità del fenomeno della prevaricazione on-line, riconosciuta come forma di devianza minorile.

L'art. 3 della legge numero 71/ 2017, conferisce al Miur il coordinamento di un Tavolo tecnico per la prevenzione e il contrasto del cyberbullismo, istituito con decreto del Presidente del Consiglio dei ministri presso la Presidenza del Consiglio. Quest'organo, entro 60 giorni dalla sua istituzione, è tenuto ad elaborare un *piano di azione integrato* per il contrasto e per la prevenzione del cyberbullismo costituendo un sistema di raccolta dati anche in collaborazione con le forze di polizia (specialmente la Polizia postale e delle comunicazioni[142]). Il medesimo piano deve venire integrato da un codice di co-regolamentazione che vincoli tutti gli operatori del web in modo tale da tutelare i giovani utenti. Per la stessa motivazione è stata conferita al Miur[143] la guida del suddetto tavolo: l'istituzione scolastica viene infatti vista come agenzia educativa privilegiata per la possibilità di intercettare almeno potenzialmente l'universo dei minori. La sua azione si rivela propedeutica a realizzare l'educazione alla cittadinanza digitale nonché al corretto esercizio di diritti e doveri nello spazio di azione e di espressione garantito dal web. Infatti non è sempre vero che gli episodi di bullismo cibernetico si verifichino tra conoscenti, o che sfocino a seguito di relazioni nate in contesti di istruzione e formazione. Talvolta possono coinvolgere soggetti di Stati differenti: ecco perché è importante costruire una rete, non solo interna allo Stato italiano, ma sarebbe auspicabile fosse anche internazionale, per formare le nuove generazioni. L'internazionalità però, al momento, è un obiettivo tanto desiderabile quanto utopistico a causa delle diverse legislazioni che prevedono maggiori età raggiunte in anni differenti (da 14 a 23, a seconda della Nazione cui si fa riferimento), così come le condotte sanzionabili o la definizione del fenomeno qui considerato.

L'investimento che il legislatore italiano ha compiuto nei confronti della Scuola, è lungi dal conferire alla stessa tutte le responsabilità in merito alla formazione dei giovani internauti: i genitori, o comunque i tutori, hanno l'obbligo nonché il diritto

[142] M. Alovisio (avvocato), articolo "Protocollo di Intesa contro il cyberbullismo fra il Garante Privacy e la Polizia Postale", Diritto e Giustizia, 16/01/2018.
[143] Miur: Ministero dell'Istruzione, Università e Ricerca.

costituzionalmente sancito in capo a loro dall' articolo 30, di mantenere, istruire ed educare i figli. Disposizione che, con il mutamento sociale in atto, si è arricchita di ulteriori nuove accezioni, tali da rendere l'evoluzione delle competenze educative genitoriali la cartina di tornasole dei cambiamenti sociali, sebbene quest'ultima non sia stata indicata come agenzia di educazione primaria. In sociologia si parla di agenzie di socializzazione ed educazione, riferendosi a delle istituzioni o autorità che fanno parte della vita del bambino e lo conducono verso un corretto processo d'integrazione sociale all'interno della propria comunità di riferimento. Esse si distinguono in agenzie di socializzazione primaria e secondaria: la prima viene definita dai sociologi come la famiglia. Solitamente, la seconda invece, viene convenzionalmente riconosciuta in più istituzioni come ad esempio la scuola e tutti i gruppi cui il minore prende parte nel suo tempo libero, come quelli composti da chi svolge le sue stesse attività extrascolastiche[144].

Nella composizione del Tavolo tecnico di cui sopra, vengono previste rappresentanze di associazioni di genitori, i quali sono espressamente menzionati al fine di poter richiedere «*l'oscuramento, la rimozione o il blocco di qualsiasi dato personale diffuso attraverso la rete internet*». Azione che può compiere anche la medesima vittima ultraquattordicenne.

Le figure genitoriali inoltre, vengono riconosciute come soggetti titolari di un diritto di informazione nel momento in cui il dirigente scolastico venga a conoscenza di atti di cyberbullismo, in quanto lo stesso dirigente deve avvisare tempestivamente i genitori ovvero i tutori dei minori coinvolti, come previsto dall'art. 5 della legge 71/2017. Infine, la presenza degli esercenti la potestà genitoriale è richiesta dall'art. 7, con l'obiettivo finale che consiste nell'accompagnamento del minore cyberbullo davanti al questore per la procedura di ammonimento. Quest'ultimo istituto è un provvedimento amministrativo che può essere richiesto presso qualsiasi ufficio di polizia ed è ipotizzabile possa comprendere specifiche prescrizioni per il minore; i cui effetti

[144] M. P. Fontana, "Cyberbullismo: famiglia, scuola e servizi dopo la legge 71 del 2017", Questione giustizia, 20/12/2017.

cesseranno al compimento dei diciotto anni del ragazzo. È stata proprio la mancata evidenziazione dell'importanza del ruolo familiare nell'educazione al corretto uso dei mass media a far temere la deriva alla sua deresponsabilizzazione che parallelamente al protagonismo scolastico potrebbe portare ad una temuta delega genitoriale mentre invece sarebbe fondamentale la collaborazione di queste due agenzie di socializzazione. Tale pericolo, potrebbe essere ipoteticamente fugato nel caso in cui le iniziative di informazione e prevenzione previste dal suddetto *piano di azione* siano veramente nelle condizioni di incrementare tanto la coscienza critica e il senso di responsabilità dei ragazzi, quanto le competenze di *media education* dei loro genitori, nei limiti delle risorse economiche messe a disposizione. Il piano integrato dovrebbe essere in grado di perseguire gli ambiziosi obiettivi proposti, coadiuvato dall'integrazione, appunto, delle periodiche campagne informative di prevenzione e di sensibilizzazione predisposte dalla Presidenza del Consiglio dei Ministri, dai progetti elaborati dalle reti di scuole in collaborazione con i servizi e le istituzioni locali; nonché dalle istituzioni scolastiche di ogni ordine e grado.

Quando ancora non era presente nel 2017 un piano integrato operativo, la governance del Miur si era attrezzata con l'attività di *peer education*[145], tale attività è ora prevista dall'art. 4, comma 2 della legge n. 71/2017 "*la formazione del personale, la partecipazione di un proprio referente per ogni autonomia scolastica, la promozione di un ruolo attivo degli studenti, nonché di ex studenti che abbiano già operato all'interno dell'Istituto scolastico in attività di* peer education*, la previsione di misure di sostegno e di rieducazione dei minori coinvolti*".

L'importanza dello strumento della *peer education* non ha come unici protagonisti gli studenti, come erroneamente si potrebbe pensare: questa modalità di apprendimento, in effetti, si basa sul mutuo aiuto tra ragazzi, ed è ottima per avvicinarli nonché portarli a scoprire ognuno le potenzialità dell'altro. In particolare, gli studenti che si trovano nella condizione di ricevere aiuto,

[145] La peer education è una delle tecniche "personalizzate" di apprendimento cooperativo basate sulla responsabilizzazione dei partecipanti che concentrano la propria attenzione sulle caratteristiche dei ragazzi nella condizione di richiedere aiuto. C. Cornoldi, C. Meneghetti, A. Moè, C. Zamperlin, "Processi cognitivi, motivazione e apprendimento", il Mulino, 2018, pag. 138 e ss.

ottenendo consigli dai loro pari, non solo sentono meno pressione e si esprimono più liberamente, ma fanno anche meno fatica a capire concetti che vengono loro spiegati da dei coetanei con i quali condividono senz'altro dei punti di riferimento: siano essi dati dalla serie tv del momento o da cartoni animati che seguivano da bambini. Affinché tale progetto possa definirsi un successo, è necessaria la figura di qualcuno che lo introduca, ne spieghi il funzionamento, intervenga in casi di necessità: queste sono solo alcune delle funzioni del docente referente. Quest'ultimo infatti ha anche il compito di interfacciarsi con le forze di Polizia, con i Servizi minorili dell'Amministrazione della Giustizia, le associazioni e i centri di aggregazione giovanile sul territorio, allo scopo di coordinare efficacemente le iniziative di prevenzione e di contrasto del cyberbullismo. Questo ambizioso progetto vede concretizzarsi la possibilità della propria realizzazione grazie alle Linee guida, che offrono indicazioni pratiche per la segnalazione dei casi di abuso, e ribadiscono l'importanza di un articolato sistema di prevenzione del cyberbullismo, tanto a livello centrale quanto regionale e periferico. Il tutto ponendosi in continuità con la scia di iniziative come la Generazioni connesse.[146]

Qualora la scuola non disponesse di personale qualificato nonché di strumenti adeguati allo scopo di garantire la formazione in merito all'uso scorretto dei mass media, e le Linee specificano sia compito del Preside prendere accordi con le autorità locali istituendo una fitta rete in grado di fornire supporto specializzato e continuativo ai minori coinvolti. Questo obiettivo sarebbe quindi realizzabile grazie alla collaborazione degli uffici locali di servizi della salute, servizi sociali, forze dell'ordine, servizi minorili dell'amministrazione della Giustizia.

La normativa del 2017 apre quindi le porte ad un'intensa collaborazione interistituzionale che in qualche territorio è stata anticipata e preparata dall'istituzione di specifici Tavoli locali. È auspicabile inoltre che tale organizzazione e tali reti che si stanno costituendo al fine di tutelare i minori, possano dare vita a nuove progettualità integrate, le quali, per quanto concerne la prevaricazione e l'abuso che i giovani manifestano attraverso il *web*,

[146] M. P. Fontana, "Cyberbullismo: famiglia, scuola e servizi dopo la legge 71 del 2017", Questione giustizia, 20/12/2017.

potrebbero ricordare il metodo della concertazione e della co-costruzione delle politiche minorili territoriali proprio della legge n. 285/97, recante disposizioni per la promozione di diritti e di opportunità per l'infanzia e l'adolescenza. Tuttavia, il livello di creatività e di efficacia delle progettualità elaborate dalle varie realtà locali verrà influenzato dalla capacità delle istituzioni di collaborare.

Nello stesso 2017 in cui, grazie alla legge 71, nasceva la rete composta da scuole e genitori per consentire ai minori una navigazione in rete più sicura dai rischi del cyberbullismo e delle condotte ad esso assimilabili, veniva presentata[147] l'innovativa applicazione Youpol. Tale app gratuita è entrata in funzione con copertura totale della penisola l'anno successivo segnando l'inizio di una proficua collaborazione tra cittadini e forze armate nel periodo compreso tra gennaio e giugno 2022 la commissaria capo Arianna Donati, ha dichiarato in un'intervista che grazie a tale strumento hanno raccolto una media di due segnalazioni al giorno gran parte delle quali attendibili.[148] La stessa, nel corso della medesima intervista ha anche spiegato brevemente il funzionamento[149] piuttosto intuitivo dell'app, pensata per i ragazzi dato che sono i principali fruitori dei prodotti online e che è più probabile entrino in contatto con realtà quali bullismo, reati legati al cyberbullismo, spaccio e che non riescano a parlarne con gli adulti per denunciare tali condotte: con l'applicazione sono loro stessi a potere denunciare, in tempo reale, alla polizia quanto accade sotto i propri occhi inviando immagini, audio, video, segnalazioni scritte, link, siti web. L'applicazione in questo modo consente a chiunque, soprattutto al minore, di mettersi in contatto diretto con le sale operative della polizia di Stato, senza doversi sentire in imbarazzo a doverne parlare con un familiare e gestire un carico emotivo troppo pesante per lui in

[147] Il funzionamento dell'applicazione della Polizia di Stato è stato illustrato dal Ministro dell'Interno Minniti e dal capo della Polizia Gabrielli presso l'istituto Lombardo Radice di Roma nel novembre 2017.
[148] A. Scarcella (giornalista e videomaker),"Bolognatoday.it", l'11 agosto 2022.
[149] La applicazione Youpol consente di compiere segnalazioni che arrivano direttamente alla questura grazie ad un semplice messaggio che può contenere un massimo di 500 caratteri in cui vengano indicati: l'illecito che sta avvenendo, il luogo (anche se le segnalazioni sono automaticamente georeferenziate cosicché le forze dell'ordine trovino immediatamente il luogo da cui è partita la segnalazione), ed i dati di chi sta inviando il messaggio. Certo, è anche presente la funzione della segnalazione in anonimato ma la commissaria capo, ci tiene a precisare che le segnalazioni compiute con questa modalità hanno meno probabilità di venire verificate. Le forze armate legate a tale risorsa infatti sono esigue, pertanto viene considerata maggiormente attendibile una segnalazione fornita da un utente identificabile.

quella determinata circostanza, in modo tale da poter ricevere la necessaria tutela e il supporto utile a potersi sentire libero di parlare con la propria famiglia e le figure adulte di riferimento che lo aiutino a ritrovare la serenità.

paragrafo 3.2 I danni all'integrità psico-fisica: *challenges* e possibili effetti del *revenge porn* sul comportamento dei minori

Il 33% degli episodi di cyberbullismo riguarda reati di tipo sessuale. Il *revenge porn*[150] consiste nella diffusione in rete e condivisione di immagini intime a scopo vendicativo da parte di amici o ex partner della vittima[151]. Nella maggior parte dei casi è quest'ultima a fornire il materiale al suo ricattatore facendo sexting, ovvero, inviando immagini o testi sessualmente espliciti via *web*. Molto spesso quindi le molestie non nascono online ma sono frutto di interazioni avvenute con persone conosciute a scuola, nelle attività sportive, tramite reti di amici che fanno parte della vita offline delle vittime, che hanno delle basi nella vita reale e che continuano online[152].

[150] Il revenge porn è indicato come reato all'art. 612-ter del Codice Penale che punisce la diffusione illecita di immagini o video sessualmente espliciti. Conosciuta anche come "revenge pornography", associa la parola "vendetta" (revenge) a quella di pornografia. È stata riconosciuta come reato anche in Italia solo nel 2019, grazie alla legge 19 luglio 2019 n. 69 (la Codice Rosso), volta a tutelare le vittime di violenza domestica e di genere; la legge ha introdotto nel codice penale, grazie al proprio articolo 10 comma 1, l'articolo 612-ter.

[151] Fino al 2019 non esisteva alcuna legge specifica per tutelare tali vittime che solo con il primo comma dell'articolo 10 della Legge numero 69 del 19/07/2019 hanno ottenuto uno strumento utile nella lotta alla violenza domestica e di genere, grazie al fatto che lo stesso articolo abbia introdotto nel c.p. l'art.612-ter rubricato "Diffusione illecita di immagini o video sessualmente espliciti". Tale legge prevede la reclusione da 1 a 6 anni e una multa da 5.000 a 15.000 euro per chi ceda, consegni, diffonda, invii, pubblichi immagini o video a contenuto sessualmente esplicito dopo averli realizzati o sottratti. A questi effetti si aggiungono quelli di rimozione dei contenuti di cui sopra ad opera della legge 205 di conversione del Decreto Capienze: viene introdotto infatti il nuovo articolo in materia nel Codice relativo alla protezione dei dati personali, il numero 144-bis che stabilisce: " Chiunque, compresi i minori ultraquattordicenni, abbia fondato motivo di ritenere che registrazioni audio, immagini o video o altri documenti informatici a contenuto sessualmente esplicito che lo riguardano, destinati a rimanere privati, possano essere oggetto di invio, consegna, cessione, pubblicazione o diffusione attraverso piattaforme digitali senza il suo consenso ha facoltà di segnalare il pericolo al Garante, il quale, nelle quarantotto ore dal ricevimento della segnalazione, decide ai sensi degli articoli 143 e 144 del Codice della Privacy". M. Alovisio, "L'impatto della legge di conversione del D.L. 8 ottobre 2021 n. 139 "Decreto Capienze" sulle misure di prevenzione e contrasto del revenge porn", Diritto e Giustizia, 20/12/2021.

[152] d. boyd, "It's complicated", Castelvecchi, 2014, pag. 162 e ss.

Che sia per gioco, per noia, per avere qualche spicciolo in più in tasca o per altre motivazioni, queste azioni hanno delle conseguenze che non sono affatto piacevoli[153] come documentato da molti casi di cronaca.

Sebbene per l'opinione pubblica la rete venga messa nel novero degli imputati, in realtà è solamente un mezzo acritico dotato di straordinaria rapidità di diffusione. Ai suoi gestori non interessa come venga usata fintanto che continuano ad aumentare i loro utenti e gli utili che provengono dagli inserzionisti. Le aziende produttrici di qualsivoglia prodotto da mettere in commercio, mai come recentemente, riconoscono la necessità di far passare dai social la propria pubblicità per raggiungere un numero sempre maggiore di possibili futuri acquirenti.

Già sui motori di ricerca qualunque bambino o utente con media dimestichezza con computer, *smartphone* e simili, può cercare qualsiasi parola e venire a conoscenza di realtà poco appropriate alla sua età nonché al livello di maturazione e sviluppo mentale che la caratterizzano. Nel 2013, ad esempio, tra le cinque parole più cercate dai minori sul *web*, figuravano "sesso" e "porno", con la particolarità, per quest'ultima parola, di essere stata la quarta parola maggiormente ricercata dai minori di 7 anni secondo quanto riportato dallo studio Symantec.[154] Il maggiore problema che mettono in luce questi dati non è tanto la profonda curiosità dei minori sul tema della sessualità quanto il fatto che l'educazione ricevuta a scuola non viene considerata sufficientemente esaustiva, tanto da portarli a cercare ulteriori informazioni in rete, navigando in solitaria. Non solo: il fatto che alla parola "sesso" venga associato il vocabolo "porno", denota una carenza di educazione affettiva collegata ai temi della sessualità anche da parte delle famiglie che troppo spesso delegano alla scuola il trattamento di argomenti tanto delicati in modo da non dover gestire lo stress di affrontarli da soli con i propri figli. Questi ultimi, un po' per vergogna, un po' per timore, nonostante siano avidi di conoscenza, pongono le domande all'unico

[153] G. Lavenia, "Mio figlio non riesce a stare senza smartphone", Giuntiedu, 2019, pag. 35 e ss.

[154] Symantec: meglio nota con il nome di NortonLifeLock, è un'azienda statunitense specializzata nella produzione di software relativi alla sicurezza informatica. M. Faccioli, "Minori nella rete -pedofilia, pedopornografia, deepweb, social network, sexting, gambling, grooming, e cyberbullismo nell'era digitale. Analisi e riflessioni su giovani e giovanissimi navigatori nei lati oscuri del web", Key editore, 2015, pag. 36.

interlocutore con cui hanno moltissima confidenza e di cui non temono un giudizio negativo: Internet.

Le conseguenze, tuttavia, sono tutt'altro che confortanti; proprio perché come precedentemente detto, Internet, motori di ricerca e social media ad esso associati sono acritici, e non impediscono all'utente non meglio identificato, quando non dichiaratamente minorenne, di accedere ad immagini, video e contenuti multimediali che rispondano alle richieste digitate dai giovani internauti in maniere imprevedibili persino per loro.[155] L'imprevedibilità dei contenuti, se così si può definire, in maniera assai edulcorata, consiste in quello che per i ragazzi diventa il primo impatto con la pornografia e quanto la circonda quindi pedopornografia, pornografia minorile, pedofili e malviventi di ogni sorta. Quando un minore viene in contatto con la pornografia ed i contenuti ad essi associati, tra i primi rischi che corre vi sono quelli psicologici di non svilupparsi correttamente dal punto di vista psicologico. Ma i danni si ripercuotono anche sul piano fisico: il 25% di adolescenti tra 14 e 16 anni che visionava spesso siti porno vietati ai maggiorenni, ha sviluppato vere e proprie disfunzioni sessuali come l'eiaculazione precoce o la diminuzione del desiderio.

Il minore può avvicinarsi alla pedopornografia a seguito delle proprie ricerche spinto da curiosità personale e vergogna di parlarne con un adulto, oppure può essere spinto ad informarsi riguardo a simili temi in seguito di discorsi fatti con un soggetto parafiliaco che gli si è avvicinato. L'individuazione del minore a cui approcciarsi, per un soggetto molestatore o pedofilo, può avvenire perché già lo conosce nella sua vita off- line (come è la maggioranza dei casi), oppure tramite gruppi di cantanti famosi tra i più giovani, o ancora più semplicemente perché ha notato l'intensa attività online del ragazzino di turno nel *deep web*. In seguito, grazie all'opera di *grooming* della futura vittima, può arrivare a chiedergli di fare delle videochiamate (registrate all'insaputa del minore) dove gli chiede di attuare comportamenti insoliti e di compiere azioni sessualmente più o meno esplicite, che in seguito userà per ricattarlo. Talvolta basta anche solo una foto, ed è

[155] A. Cazzullo con R. e F. Maletto Cazzullo, "Metti via quel cellulare. Un padre, due figli, una rivoluzione", Mondadori, 2017, pag. 123 e ss.

preoccupante come, tra i giovani che utilizzano Internet, il 13% abbia ammesso di aver inviato proprie foto o immagini di sé nudi ad adulti, chi per essersi lasciato trasportare dal *groomer*, chi per soddisfare la propria curiosità di vedere le foto con cui avrebbe ricambiato l'autore (la maggior parte delle volte sono uomini) della richiesta, chi a seguito di minacce congiunte alla promessa di ricariche telefoniche o di regali dal basso importo economico, attirato quindi nella trappola un po' dalla necessità che non si divulghi la sua precedente attività online, un po' attratto dalla prospettiva di un guadagno "facile".

Per quanto concerne invece il caso in cui un minore sia protagonista di condotte lesive che lo hanno come bersaglio a mezzo di materiale pornografico di cui è esso stesso protagonista, i danni sopra citati si aggiungono a tutti quelli che possono derivare dalla fattispecie in cui si verrebbe a trovare la vittima e le tappe che l'anno portata alla stessa. Troppo spesso i soggetti parafiliaci sono coloro che dovrebbero avere cura dei più piccoli a loro affidati, e quelli di loro che riescono a realizzare i propri desideri danno vita agli abusi compiuti in ambito domestico che, secondo i dati del CENSIS, riportati dal famoso criminologo Marco Strano, costituiscono i 2/3 delle modalità con cui si compiono questi crimini. Le conseguenze psicologiche per il minore saranno comunque nefaste, in quanto gli adulti di cui si fidava hanno tradito la sua fiducia, e si lascerà plagiare credendo di essere il vero colpevole, provando un senso di vergogna che, assieme al timore che ogni adulto possa sottoporli a simili torture, gli impedirà di parlare con chi invece lo potrebbe aiutare. Poco importa, quindi se gli abusi sessuali sono intrafamiliari[156] o extrafamiliari[157]: le conseguenze per il minore saranno le medesime[158]. A volte è il carnefice online a trovare la sua vittima, che magari non chiede altro che attenzione e un po' di affetto, quando non addirittura una conferma di essere degno d'amore, in poche parole aiuto, anche se con post che crede siano anonimi (se lo fossero davvero infatti, sarebbero comunque a

[156] Si definisce abuso sessuale intrafamiliare quello operato dai parenti del minore. Statisticamente è la forma di abuso minorile più diffusa.
[157] L'abuso sessuale extrafamiliare può essere compiuto da tutte quelle figure che per i motivi più diversi entrano in contatto von il minore per un periodo più o meno lungo di tempo. Alcune volte i genitori sono complici di tali individui.
[158] F. Caccetta, "Abbandonati nella rete- Internet e gli adolescenti", MGC edizioni, 2016, pag. 58 e ss.

danno dei minori che li hanno scritti e pubblicati dal momento che chi potrebbe aiutarli non li riterrebbe attendibili[159]). L'unica colpa della vittima è di essersi avventurata da sola nel *deep web*, ad esempio, ma è proprio qui che fioriscono i gruppi online di pedofili, che vengono considerati dalla rete alla stregua di gruppi online degli alcolisti anonimi[160]; tali individui, infatti, sono definiti dai propri desideri e si distinguono dai molestatori (prontamente bannati dai social e oggetto di pene e sanzioni) che invece sono caratterizzati non dai desideri bensì dalle loro stesse azioni. Va precisato però, che mentre il *network* di pedofili è considerato perfettamente lecito, non lo è il tentativo, che però deve essere dimostrato in sede di giudizio, di adescamento dei minorenni: quest'ultimo è un reato imputabile ai sensi dell'articolo 609 undecies Codice Penale. Anche l'Unione Europea si è impegnata nella lotta contro l'abuso[161] e lo sfruttamento sessuale di minori e pornografia minorile con la direttiva 93/2011[162] attuata in Italia col d. lgs. 39 del 6/04/2014[163]. A livello europeo però, così come nella direttiva italiana appena nominata, non si attua la distinzione tra pedopornografia e pornografia minorile: questi due concetti invece presentano delle specifiche che hanno rilevanza a livello legale per quanto riguarda soprattutto le disposizioni di legge riguardo tale materia. Con il termine "pedopornografia" si intende tutto il materiale pornografico che ha tra i suoi protagonisti bambini dagli 0 ai 14 anni, definiti tali perché non sessualmente sviluppati, pertanto non in grado di riprodursi; convenzionalmente infatti, l'inizio della pubertà viene fatto coincidere con i 14 anni anche se nella realtà varia da 11 a 14. La "pornografia minorile", invece, è un concetto che indica tutto il materiale pornografico che abbia tra i

[159] d. boyd,"It's complicated", Castelvecchi, 2014, pag. 98 e ss.
[160] M. Faccioli, "Minori nella rete -pedofilia, pedopornografia, deepweb, social network, sexting, gambling, grooming, e cyberbullismo nell'era digitale. Analisi e riflessioni su giovani e giovanissimi navigatori nei lati oscuri del web", Key editore, 2015, pag. 26.
[161] Il concetto di "abuso" è stato definito, durante il IV Colloquio Criminologico del Consiglio d'Europa (tenutosi a Strasburgo nel 1978), come "l'insieme di atti e carenze che turbano gravemente il minore, attentano alla sua integrità corporea, al suo sviluppo fisico, affettivo, intellettivo e morale, le cui manifestazioni sono la trascuratezza e/o le lesioni di ordine fisico e/o psichico e/o sessuale da parte di un familiare o altri che hanno cura del bambino. F. Caccetta, "Abbandonati nella rete- Internet e gli adolescenti", MGC edizioni, 2016, pag. 57 e ss.
[162] Direttiva emanata il 13/12/2011 relativa a alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio.
[163] Il decreto citato è entrato in vigore il 6/04/2014 anche se era stata pubblicata nella GU il 22 marzo del medesimo anno.

soggetti rappresentati dei ragazzini con un'età che varia dai 14 ai 17 anni. Pertanto dei preadolescenti che attraversano la fase della pubertà e presentano una sessualità in fase di sviluppo.

Questo stesso tipo di pornografia viene descritto anche all'articolo 609 ter del Codice Penale come "*ogni rappresentazione, con qualunque mezzo, di un minore di anni 18 coinvolto in attività sessuali esplicite, reali, simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni 18 per scopi sessuali*"[164].

L'articolo prevede inoltre differenti tipi di sanzioni e pene, che variano in base alle condotte poste in essere:

Reato	Sanzione penale	Sanzione amm.va
- Reclutare/indurre minori a partecipare a esibizioni o spettacoli pornografici o ne trae profitto - Usare minori per esibizione o spettacoli pornografici - Commerciare materiale pedopornografico	Reclusione da 6 a 12 anni	Multa da 24000 a 240000 euro
- Divulgare materiale pedopornografico con qualsiasi mezzo - Dare informazioni su come adescare o sfruttare sessualmente i minori	Reclusione da 1 a 5 anni	Multa da 2582 a 51645 euro
Cedere materiale pedopornografico anche gratis	Reclusione fino a 3 anni	Multa da 1549 a 5164 euro
Assistere a spettacoli pornografici con minori come soggetti coinvolti	Reclusione fino a 3 anni	Multa da 1500 a 6000 euro

[164] M. Faccioli, "Minori nella rete -pedofilia, pedopornografia, deepweb, social network, sexting, gambling, grooming, e cyberbullismo nell'era digitale. Analisi e riflessioni su giovani e giovanissimi navigatori nei lati oscuri del web", Key editore, 2015, pag. 38 e ss.

Tali pene sono state espressamente previste e ben descritte a causa dell'assiduità e della varietà di fattispecie con cui il legislatore italiano ha avuto a che vedere, dal momento che l'Italia è al quarto posto in fatto di quantità di cultori di materiale pedopornografico, dietro a Russia, Germania e Stati Uniti che invece occupano rispettivamente: terzo, secondo e primo posto. I dati dell'osservatorio internazionale dell'associazione Telefono Arcobaleno riportano inoltre che il 92% dei bambini sfruttati è di etnia europea, il 61% dei clienti e dei consumatori della pedofilia online è europeo, l'86% dei materiali pedofili rilevati in rete è allocato in territorio europeo, il 52% dei siti internet legati al *pedobuisness* è allocato in territorio europeo[165]. La sede di Siracusa della medesima associazione ha evidenziato inoltre come il target delle vittime sia ulteriormente ringiovanito nel 2007, arrivando a coinvolgere maggiormente non più bambini di 10 anni come accadeva nel 2003 ma minorenni di addirittura 7 anni.

Ma il nostro Stato non è lasciato solo nel contrasto a tale fenomeno: esistono anche nell'Unione Europea associazioni di contrasto alle derive della pedofilia. Quest'ultima è stata presente in ogni epoca e società prima dell'avvento di Internet, la cui unica colpa è di essere uno strumento di amplificazione delle società di pedofili che hanno cerato *network* legali in sé e per sé. Il fatto di detenere filmati pornografici e farne uso personale non è di per sé reato, altrimenti anche qualsiasi utente che scarichi un filmato dalla rete convinto che sia un film della Disney e si ritrova nel pc un filmato di tutt'altro genere sarebbe imputabile. L'illegalità sta nelle condotte tenute durante il video, da chi lo crea, da chi lo mette in rete nonché dai protagonisti coinvolti nella realizzazione dello stesso. Nel caso dei filmati di questa tipologia che hanno per protagonisti dei minorenni, il 40% delle bimbe dai tratti indo-europei e più del 50% dei bimbi hanno un'età tra i 9 e i 12 anni, il 10% dei soggetti dei video porno coinvolgono minori di età ancora inferiore. È infatti a queste caratteristiche che corrispondono le due ragazzine minorenni coinvolte nel caso trattato dalla Corte di cassazione nel 2021[166]. La fattispecie riguardava due bambine con meno di 14 anni e la loro

[165] F. Caccetta, "Abbandonati nella rete- Internet e gli adolescenti", MGC edizioni, 2016, pag. 15 e ss.
[166] L. Picotti e L. Lupária C. Crescioli, C. Greco, B. Panattoni, M. Pittiruti e R.M. Vadalà in collaborazione con l'Osservatorio Cybercrime dell'Università degli Studi di Verona, "Corte di Cassazione, sez. III penale,

condotta online che ha determinato, per l'uomo cui inviavano i loro *selfies* "intimi", la responsabilità penale relativa ai reati di pornografia minorile e produzione di materiale pedopornografico[167]. Egli ha infatti indotto le minori a ritrarre le proprie nudità con foto e video che poi queste ultime gli inviavano, assicurandogli di essere maggiorenni e di aver già pubblicato simili contenuti in siti per adulti. L'imputato ha ritenuto veritiere le dichiarazioni di entrambe dal momento che nelle loro immagini ha riconosciuto i tratti di sviluppo tipici delle maggiorenni, tuttavia questo non basta per venire considerato come causa di non punibilità: l'ignoranza da parte dell'imputato circa l'età delle persone offese opera solamente qualora sia indotto a ritenere che i minorenni siano maggiorenni sulla base di elementi univoci che non possono fermarsi alle rassicurazioni verbali di queste ultime.

Sempre nell'ottica di fornire maggiori tutele agli utenti, in Italia la legge prevede oneri per le piattaforme ed i fornitori di servizi online tra i quali quello di comunicare al Garante o pubblicare nel proprio sito internet i provvedimenti adottati dal Garante. Qualora tali obblighi restino inadempiuti, il Garante diffida il fornitore del servizio ad adempiere entro trenta giorni; mentre in caso di inottemperanza alla diffida si applica la sanzione amministrativa pecuniaria di cui all'articolo 83, paragrafo 4, del Regolamento europeo per la protezione dei dati personali.

paragrafo 3.3 La diffusione inconsapevole di dati personali

Il tema della diffusione inconsapevole dei dati personali ha sempre destato apprensione ma è stato portato al centro dell'attenzione nel 2018, in riferimento

sentenza 26 marzo 2021 n. 11623/2021; "Due ragazzine inviano selfie nude ad un uomo: esclusa la violenza sessuale", Diritto e Giustizia, 29/03/2021.

[167] Il reato di violenza sessuale il cui riferimento legale è l'art. 609-bis c.p. si verifica qualora vi sia un coinvolgimento della corporeità sessuale da parte del soggetto passivo. Questo può verificarsi anche tramite strumenti tecnologici come ad esempio quando, attraverso comunicazioni telematiche, la vittima venga indotta a compiere atti che ne coinvolgono la corporeità sessuale e siano pertanto idonei a violarne la libertà personale.

allo scandalo che vedeva coinvolti Facebook e Cambridge Analytica[168] nell'utilizzo di dati personali degli utenti del primo senza la loro consapevolezza, ai fini di propaganda politica[169].

Infatti, tra i possibili pericoli che riguardano i giovani utenti che si affacciano al *web* vi sono anche quelli legati ai loro dati personali. Con l'espressione "dati personali" si intendono le informazioni sugli utenti online che costituiscono una risorsa strategica per molte imprese che sviluppano il loro *buisness* sulla raccolta, aggregazione e analisi dei dati dei propri clienti, attuali e potenziali. Le informazioni in rete su di noi, infatti, rappresentano la valuta dell'attuale mercato digitale, perciò hanno un valore immenso e possono essere utilizzati per scopi commerciali in maniera più o meno lecita.[170] La liceità dei fini commerciali dipende dall'utilizzo che le aziende fanno dei dati con cui vengono a contatto e come se li procurano: l'uso del *driver* di internet deve avvenire nel rispetto dei diritti degli utenti. Dal momento che anche solo la nostra permanenza online su un determinato sito fornisce informazioni che ci riguardano è in gioco il nostro spazio di libertà, la tutela della nostra identità digitale e autodeterminazione informatica. Affinché tale consapevolezza venga raggiunta dai giovani internauti, l'impegno delle istituzioni ha portato a delle forme di autodisciplina come il Codice di autoregolamentazione internet e minori, siglato il 19 /11 /2003 da quella che oggi si chiama Associazione per la Convergenza dei Servizi di Comunicazione e da alcune associazioni di *provider*, al fine di favorire un corretto e consapevole uso della rete telematica da parte dei minori e di promuovere un accesso sicuro per il soggetto non ancora maggiorenne alle risorse di Rete, preservando la sua riservatezza e il corretto trattamento dei suoi dati personali.

[168] La Cambridge Analytica è una società di consulenza britannica specializzata nel raccogliere dai social network dati relativi agli utenti.

[169] V. Gheno e B. Mastroianni, "Tienilo acceso- posta, commenta, condividi senza spegnere il cervello", Longanesi, 2018, pag. 101 e ss.

[170] A. La Lumia, A. Dario, "Minori, internet e social network", Giuffrè, 2021, pag. 12 e ss. ; A. Astone, " I dati personali del minore in rete", Giuffrè, 2019, pag. 30 e ss. ; articolo 4 comma 1 GDPR relativo al "dato personale" mentre al primo paragrafo del nono articolo si occupa di "dati personali particolari" altrimenti detti "sensibili" quali ad esempio l'origine razziale, l'etnia, le opinioni politiche, le convinzioni religiose, l'appartenenza sindacale, le informazioni relative a vita e orientamento sessuale nonché i dati genetici, biometrici e concernenti la salute (sia mentale che fisica). (Vi è anche R. Razzante, "Informazione: istruzioni per l'uso - notizie, rete, e tutela della persona ",Cedam, 2014, pag. 123 e ss.) .

La necessità di diffondere la cultura dell'infanzia e dell'adolescenza anche nel mondo dei media porta alla nascita della Carta di Treviso del 30/ 03/ 2006 pubblicata in GU dopo essere stata approvata dal Garante della privacy. In essa l'Ordine e il Sindacato s'impegnano a richiamare particolare attenzione sui diritti del minore anche in merito a trasmissioni d'intrattenimento, pubblicità e contenuti dei siti internet a cui sono soggetti anche i responsabili delle reti radiotelevisive; i provider, nonché gli operatori di ogni forma di multimedialità. Ma i diritti riconosciuti dalle Carte di Treviso non riguardano solamente i contenuti con cui i minori possono entrare in contatto: si concentrano anche sulla tutela dei diritti che detengono i ragazzi minori d'età sui propri dati personali. Con particolare riferimento agli utenti minorenni ed alla loro sicurezza, quindi, la carta di Treviso 85 /10 /1990 istituisce l'obbligo inderogabile dell'anonimato e di pubblicazione dei dati personali nonché la divulgazione di immagini riguardanti i minori.

Il divieto si estende a tutti i particolari che possono rendere identificabile il minore e si trova anche nell'articolo numero 13 del dpr relativo al processo minorile; all'articolo 40 del Testo Unico sulla Privacy; all'interno del suo sesto comma dell'articolo 114 del Codice di Procedura Penale.

Ciò non significa che il minore debba sempre essere censurato; la censura non avviene infatti nei casi in cui i genitori e il giudice competente diano l'autorizzazione di mostrare il minore in quanto oggetto di ricerca perché rapito o scomparso e si tenta di ritrovarlo utilizzando i mass media per diffonderne l'immagine. Altro caso in cui non viene censurato il minore è dato dalla fattispecie in cui egli sia ritratto in scene di manifestazioni pubbliche o private ma di rilevanza sociale o altre iniziative collettive non pregiudizievoli e che comunque non appaiano idonee a creare un pregiudizio a personalità, sviluppo, dignità e privacy del minore.[171] Qualora si verifichino simili fattispecie tuttavia, il minore gode del "diritto all'oblio", che è indicato come il diritto a non restare indeterminatamente esposti a danni ulteriori che la reiterata pubblicazione di una notizia può arrecare all'onore e alla reputazione del soggetto coinvolto.

[171] R. Razzante, "Informazione: istruzioni per l'uso - notizie, rete, e tutela della persona" , Cedam, 2014, pag. 124 e ss.

Simile al diritto all'oblio per ciò che concerne l'impedimento all'esterno delle informazioni personali che non hanno un apprezzabile interesse sociale per la collettività, è il diritto alla riservatezza. Mentre nel diritto all'oblio però si tratta di un diritto a far tornare riservate informazioni che non sono più d'interesse pubblico, nel caso del diritto alla riservatezza si stanno trattando dei dati che non sono mai stati di interesse per la collettività e che non devono essere condivisi con la stessa in quanto strettamente personali. Entrambi questi diritti sono comunque necessari alle persone per tutelare sé stesse ed i propri dati personali che vanno a creare ed influenzare il diritto all'immagine strettamente legato ai concetti di identità[172] e reputazione digitale[173]. Questi diritti sono estremamente importanti dal momento che qualora vengano lesi determinano delle ricadute in svariati aspetti della persona che ne era titolare: dalle relazioni interpersonali agli aspetti lavorativi e professionali.

La necessità di proteggere l'identità personale e digitale delle persone è resa ancora più pressante dalla rapidità con cui si diffondono le informazioni grazie ad internet portando a delle conseguenze più gravi e pesanti. Si pensi all'esempio dello stress da "*web reputation*": generato dalla comunità della rete nei confronti di una persona che magari neppure conosce, a seguito di una lesione della reputazione di cui la stessa gode; essa arriva a sperimentare questo tipo di stress a causa dell'importanza che viene data ad un gruppo di individui che molte volte le sono sconosciuti. Questi ultimi possono essere datori di lavoro futuri o possibili che nella scelta dei propri dipendenti potrebbero digitarne il nome sul noto motore di ricerca Google[174] per avere ulteriori informazioni del candidato rispetto al curriculum che questi ha fornito, decisi a scoprirne l'essenza. Con l'accesso ad Internet, nell'era dei *social media*, ognuno, per quanto tenti di prendere le distanze dal mondo digitale, vi si ritrova a partecipare suo malgrado, ecco perché è importante che le persone siano consapevoli che la propria vita privata e

[172] Per "identità digitale", M. Iaselli, in "Investigazioni digitali" intende il rapporto di conoscenza" tra un soggetto e la sua comunità.

[173]La "Reputazione digitale" viene intesa da M. Iaselli come un giudizio di valore associato all'identità digitale di un individuo in un momento successivo alla conoscenza della stessa.

[174] Google è il motore di ricerca più usato al mondo e allo stesso tempo anche il sito con più alto traffico al mondo. V. Gheno e B. Mastroianni, "Tienilo acceso- posta, commenta, condividi senza spegnere il cervello", Longanesi, 2018, pag. 161.

pubblica si sono fuse e restano in perenne collegamento ed è fondamentale che ognuno sia a conoscenza di quanto gli viene collegato in rete dagli algoritmi di quest'ultima e da altri utenti. Solo così la persona riuscirà a veicolare il messaggio su di sé che vuole trasmettere, senza che qualcun altro decida per lei dando luogo a spiacevoli equivoci e fraintendimenti che potrebbero avere conseguenze molto pesanti[175].

Ecco quindi perché i dati personali necessitano di tanta protezione e sono considerati il "nuovo petrolio": che siano consapevoli, o meno, involontari o non. I dati forniti in maniera consapevole sono quelli che le persone sanno di rendere pubblici così come sanno che possono essere visti da altre persone oltre a quelle che li commentano. L'inverso dicasi per le informazioni pubblicate in maniera inconsapevole. Quelle involontarie possono non essere state pubblicate direttamente dalla persona o essere messe in circolazione senza che essa ne sia a conoscenza, mentre le informazioni diffuse in modo volontario sono quelle che la persona pubblica, anche se non tenendo conto di tutti i possibili spettatori, soprattutto futuri (si veda l'esempio relativo ai datori di lavoro di cui sopra).

Di sicurezza e diritti del minore in rete si è occupato anche il garante per la protezione dei dati personali (GPDP)[176]. Tra le materie su cui è intervenuto, nonostante lo scenario fosse reso complicato dalla pandemia, figura quanto concerne le grandi piattaforme e la tutela dei minori, il cyberbullismo ed il *revenge porn*. La relazione annuale del GPDP 2021 non solo è di facile accesso al sito istituzionale, ma è ordinata all'interno di una tabella che raccoglie anche tutte quelle che l'hanno preceduta, agevolandone la consultazione. In tale sede, è di particolare interesse trattare il contenuto del nono capitolo della relazione relativa all'annata del 2021 in merito al tema dei dati dei minori ed in particolare le innovazioni introdotte sulle loro garanzie dalle regole ontologiche codificate nel documento in esame nonché dalla Carta di Treviso. In aggiunta, il 6 luglio 2021 il Consiglio dell'Ordine dei giornalisti ha deliberato un nuovo testo della Carta, di

[175] Cit. fonte nota 173, pag. 127 e ss.

[176] Il Garante per la Protezione dei Dati Personali, altrimenti conosciuto come Garante della privacy, è un'autorità amministrativa indipendente italiana istituita dalla legge 31 dicembre 1996, n. 675, al fine di garantire la tutela dei diritti e delle libertà fondamentali e il rispetto della dignità nel trattamento dei dati personali.

cui l'Autorità, peraltro non coinvolta nella stesura, ha preso atto anche se rilevando delle criticità. La materia dei dati personali dei minori è riconosciuta dal Garante come estremamente importante, tanto da meritare il più rigoroso rispetto nelle disposizioni di protezione ad essa relative. Proseguendo tra le pagine del GDPR si trovano anche i dati relativi ai fenomeni di cyberbullismo: i casi segnalati, quelli risolti e quelli contro i quali non si è potuto procedere. I primi sono perlopiù resoconti su pubblicazioni di post diffamatori e denigratori aventi ad oggetto foto anche a carattere intimo sfuggite al controllo del minore che le aveva inserite in chat private. I secondi invece vengono descritti nelle modalità che hanno permesso d'intervenire in tempi celeri ovvero: formulando richiesta d'intervento al gestore del sito resosi teatro della condotta denigratoria, prendendo contatti via mail oppure telefono con il segnalante al duplice scopo di richiedere ulteriori informazioni sul singolo caso e di fornire eventuali altre indicazioni utili relative allo stesso. I terzi, invece, non sono stati oggetto di alcun procedimento dal momento che in essi non sono stati ravvisati i requisiti minimi per qualificare le condotte in esame come atti di cyberbullismo.

Ma le azioni del Garante della protezione dei dati non terminano qui. Per la tutela dei diritti dei minori nel contesto dei social network, dei servizi e dei prodotti digitali in rete, il Garante ha infatti partecipato al tavolo tecnico istituito con decreto del Ministro della giustizia del 21 giugno 2021, cui hanno preso parte anche l'Agcom e il Garante. Le principali aree d'intervento di tale tavolo tecnico sono tre e comprendono la protezione dei minori nella navigazione in internet; la sensibilizzazione dei genitori; nonché lo sfruttamento commerciale dell'immagine dei minori. Al fine di operare in un contesto sufficientemente aggiornato e rappresentativo a riguardo, sono state effettuate numerose audizioni di esperti nonché di rappresentanti operanti nel settore della tutela dei minori, oltre alla predisposizione di un questionario riguardante le misure adottate a tutela dei minori.

Quest'ultimo si è rivelato uno strumento particolarmente efficace grazie alla collaborazione delle piattaforme social che lo hanno trasmesso ai propri utenti chiedendo loro confidenzialità nonché la sua restituzione una volta compilato.[177]

In materia di diffusione dei dati personali quindi, non si può non fare riferimento al decreto legislativo 196 del 2003 meglio noto, anche se informalmente, come Codice della Privacy. Entrato in vigore all'inizio del 2004, contiene tutte le norme nazionali in merito alla tutela dei dati personali, a cominciare dal limite d'età al di sopra dal quale il cittadino si può prendere la responsabilità circa l'autorizzazione al trattamento dei propri dati; mentre al di sotto dello stesso limite per conseguire la medesima finalità, c'è bisogno dell'intervento di un genitore o di chi ne faccia le veci. Il legislatore italiano ha riconosciuto, nel primo paragrafo dell'art. 8 del d.lgs. 196/ 2003, l'età di 14 anni come idonea a consentire al soggetto di esprimere il consenso al trattamento dei suoi dati personali relativamente all'offerta diretta dei servizi della società dell'informazione.
La decisione di stabilire il limite di età a 14 anni è stata presa dal nostro legislatore osservando quanto stabilito dalla regolamentazione europea espressa dal GDPR. Infatti il Regolamento all'art. 8 stabilisce una regolamentazione specifica sul minore e sui dati che lo riguardano senza però entrare nel merito della capacità d'agire del minore, che rimane quindi fissata dall'ordinamento civile nazionale. Questa parte del regolamento generale sulla protezione dati indica che per poter applicare quanto necessario alla tutela degli interessi dei minori sono necessari due requisiti. Il primo è che vi sia un'offerta diretta di servizi della società dell'informazione a soggetti minori di 16 anni (oppure, nel caso in cui l'età sia differente, è necessario che venga fissata dal legislatore nazionale) mentre il secondo consiste nel fatto che il trattamento dei dati relativi ai minori sia basato sul consenso. Con l'approvazione del GDPR avvenuta il 25/ 05/ 2018, viene introdotta una deroga alla regola generale stabilita dall'ordinamento, abbassando il limite d'età dei 18 anni creando quindi una sorta di maggiore età digitale con il conseguimento della quale viene ammesso, in riferimento alla profilazione, il consenso al trattamento dei dati personali di chi l'ha raggiunta. Tale limite d'età

[177] M. P. Fontana, "Cyberbullismo: famiglia, scuola e servizi dopo la legge 71 del 2017", Questione giustizia, 20/12/2017.

può essere ulteriormente abbassato dagli Stati nazionali con l'unico vincolo di non scendere al di sotto dei 13 anni. Nel rispetto di tale disposizione quindi, il legislatore italiano, con decreto di adeguamento del Codice della Privacy ha fissato il limite da applicare in Italia all'età di 14 anni.[178]

[178] A. Astone, "I dati personali del minore in rete- dall'internet delle persone all'internet delle cose", Giuffrè, 2019, pag. 21 e ss. ; M. Faccioli, "Minori nella rete -pedofilia, pedopornografia, deepweb, social network, sexting, gambling, grooming, e cyberbullismo nell'era digitale. Analisi e riflessioni su giovani e giovanissimi navigatori nei lati oscuri del web", Key editore, 2015, pag. 44 e ss.

Capitolo 4: I soggetti garanti delle tutele.

Introduzione al capitolo 4

Le istituzioni nazionali ed europee si sono occupate a più riprese, soprattutto nell'ultimo trentennio, di fornire agli utenti minorenni e alle loro famiglie indicazioni e strumenti adeguati nonché la formazione necessaria per utilizzarli al meglio.

Data la natura globale della rete, è necessario stabilire delle regole che tutelino i suoi utenti più giovani dal momento che le legislazioni dei vari paesi non sono sempre conosciute e un atto considerato illecito in uno Stato potrebbe non esserlo in un altro, anche se ha arrecato danno ad un minore magari residente nel primo. La grandezza e la inclusività della Rete determina una enorme ricchezza di informazioni ma allo stesso tempo anche pericoli non indifferenti. Pertanto, il bisogno di utilizzare la rete, condiviso anche dai soggetti minorenni determina da un lato la necessità di sicurezza per questi ultimi, garantita grazie a modalità stabilite da diverse istituzioni, mentre dall'altro rende imprescindibile una regolamentazione.
Le modalità d'azione che garantiscono la sicurezza degli utenti minorenni in rete sono definite a livello europeo su molteplici piani: da quello riguardante la disciplina del cyberbullismo e delle condotte ad esso collegate a quello della protezione dei dati personali.

A livello nazionale italiano, non solo ci sono i decreti attuativi di quanto disposto dalle norme europee, ma anche istituzioni che operano nel rispetto di quanto sopra citato al fine di garantire la sicurezza e la salvaguardia degli utenti minorenni (e non). In particolare, nella cornice legislativa stabilita a livello europeo, si collocano il Garante per la protezione dei dati personali, l'Unità di analisi sul crimine informatico che costituisce parte della Polizia postale, così come il Ministero delle Comunicazioni e l'Autorità garante per le comunicazioni, oltre all'operato dell'Arma dei Carabinieri.
Nonostante il fine sia il medesimo, le modalità con cui perseguirlo variano notevolmente da un'istituzione all'altra. Basti pensare che alcune sono impegnate maggiormente nella prevenzione di fatti che potrebbero cagionare danno agli utenti più piccoli ed altre invece si occupano dell'aspetto legato

all'indagine nonché alla sanzione da comminare. Con riferimento alla frase precedente va anche ricordato che la prevenzione si suddivide in educazione civica di genitori e ragazzi ad un uso sano e corretto della rete e contemporaneamente in strumenti dati dalle varie piattaforme per consentire ai genitori di monitorare le attività online dei figli minorenni.
La tutela dei ragazzi passa anche attraverso i progetti fatti a scuola con esperti che parlano dei rischi della rete. È particolarmente interessante considerare inoltre come in tali progetti, i ragazzi vengano solo redarguiti in merito ai comportamenti da non attuare, ma non viene fornito alle eventuali o potenziali vittime un vero e proprio iter da seguire per fare valere i propri diritti. Vengono spiegati loro solo gli aspetti appena citati e le regole della navigazione online che li rendono degli utenti rispettosi delle norme educative relative all'attività in rete. Questo perché il più delle volte, a svolgere la formazione sono esperti o giornalisti che hanno seguito alcuni casi, ma sarebbe preferibile che la sensibilizzazione nelle scuole e la formazione dei ragazzi venisse anche fatta da membri delle Forze dell'Ordine, ed in particolare dall'Arma dei Carabinieri, vista la sua capillare diffusione sul territorio italiano[179]. Essi infatti, seguono da vicino i casi e dispongono di tutte le conoscenze pratiche in merito a strumenti di tutela, procedure e sanzioni, pertanto potrebbero fornire risposte più precise alle domande dei ragazzi. Negli Stati Uniti l'FBI manda i propri agenti regolarmente negli istituti scolastici al fine di garantire la preparazione dei ragazzi sui comportamenti da adottare durante la navigazione in rete e su quelli da evitare, dando luogo così a progetti educativi che consentano di diffondere conoscenze concrete nonché utili fornite da professionisti in materia.

Quanto ai genitori invece, l'educazione volta a prevenire eventuali situazioni rischiose in cui possono incorrere i propri figli minorenni a seguito dell'attività in rete, prevede anche la presentazione di strumenti ai quali possono ricorrere una volta che gliene venga spiegato l'uso oppure che gli venga fatta conoscere una comunità di altri genitori più esperti dove ognuno mette il proprio sapere a disposizione degli altri (è quello che accade nella *community Genitori digital*). I

[179] F. Caccetta, "Abbandonati nella Rete- Internet e gli adolescenti", MGC Edizioni, 2016, pag 129 e ss.

genitori necessiterebbero di un progetto volto a spiegare solamente la vastità dei mezzi a loro disposizione: dai *software* che bloccano gli indirizzi web che i genitori non vogliono vengano digitati dai figli, a quelli che consentono ai minori di visitare solamente quelli selezionati dai genitori, passando per le varie funzionalità del "controllo parentale" delle varie app tra cui Google store, Facebook, Apple store. Se da un lato tuttavia è sicuramente importante informare i genitori che, tra strumenti e istituzioni cui potersi rivolgere all'occorrenza, non sono soli nella tutela degli interessi dei loro figli minorenni, dall'altro è fondamentale renderli consapevoli che solo chi conosce bene la propria prole e vi ha instaurato un buon dialogo riesce a cogliere. In questo caso non c'è un corso o un progetto da seguire, ma solamente la sensibilità di chi ha a cuore la salute e gli interessi dei propri figli.

Quanto alle procedure da attivare in caso di necessità, queste sono consultabili presso i siti delle istituzioni competenti (ma come già detto, è essenziale che i danneggiati e le loro famiglie sappiano a chi rivolgersi). Non tutte le fattispecie devono seguire il medesimo iter per garantire la protezione degli interessi dei minorenni che hanno subito dei danni: nel caso in cui si tratti di dati personali è necessario contattare il Garante della loro protezione con le modalità previste dal suo stesso sito istituzionale, in caso invece di atti di cyberbullismo o di condotte ad esso relative, rilevanti a livello penale, sta alla sensibilità del genitore capire cosa sia effettivamente successo al minorenne e decidere di contattare le forze dell'Ordine in una delle modalità previste dall'ordinamento.

paragrafo 4.1 A livello europeo

La tutela dei minori in relazione alla loro attività online viene garantita a livello europeo per quanto concerne i dati personali degli stessi. La normativa originariamente era stata immaginata in forma di bozza di decreto elaborata da un'apposita Commissione che voleva abrogare il d.lgs. n. 196/2003 riscrivendo tutto e non prevedendo alcuna sanzione penale per le violazioni della privacy. Tale idea tuttavia è stata superata tanto che nel 2018 è stato emanato il decreto n. 101 riguardo alle "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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 e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*".

Con il decreto legislativo n.101 del 10/08/2018 infatti il Governo, in accordo con quanto deciso dalla seduta del Consiglio dei Ministeri, ha agito novellando il codice della *privacy* esistente (ovvero il d. lgs. n.196/2003) cambiando la prospettiva dell'approccio alla tutela della *privacy* del codice a causa dell'introduzione del nuovo principio di "*accountability*". Tale concetto consiste nella responsabilità di un ente, pubblico o privato, di rendere conto ai cittadini in merito alle decisioni prese, alle attività svolte, alle risorse impiegate ed infine ai risultati ottenuti. Inoltre riveste molta importanza dal momento che contribuisce alla buona reputazione dell'ente e ne consolida il rapporto di fiducia con la collettività. L'elemento della fiducia è fondamentale tra cittadino ed istituzioni perché è solo grazie a questo che chi necessita di aiuto può rivolgersi a chi davvero può tutelarlo, in particolare i ragazzi ai genitori e questi ultimi alle Istituzioni dello stato in cui si trovano che seguono direttive e norme elaborate nel rispetto di quelle della fonte europea. Questa ha deciso di fare salvi i provvedimenti del Garante e le autorizzazioni, che saranno oggetto di successivo riesame, oltre ai Codici deontologici vigenti, per un periodo limitato e temporaneo.

Il Garante inoltre è tenuto a promuovere modalità semplificate di adempimento agli obblighi del titolare del trattamento, tenendo presente che le imprese avranno

bisogno di tempo per adeguarsi alle norme. Tale periodo di tempo viene chiamato “tregua” e consta di otto mesi durante i quali l’attività ispettiva del Garante dovrà tenere conto di quanto appena considerato. Infatti il testo della norma esplicita che per i primi otto mesi dalla data della sua entrata in vigore, il Garante per la protezione dei dati personali deve tenere presente, ai fini dell'applicazione delle sanzioni amministrative e nei limiti in cui risulti compatibile con le disposizioni del Regolamento (UE) 2016/679, della fase di prima applicazione delle disposizioni sanzionatorie. Trascorsa tale “tregua”, quindi a partire dal 25/05/2018, le norme del Regolamento europeo sono divenute pienamente operative, pertanto se violate possono comportare come conseguenza l’obbligo di risarcimento del danno.

È bene quindi arrivare a definire la struttura di tale decreto: anzitutto, è composto da sei capi, di cui l’ultimo contenente le disposizioni transitorie e finali. Il primo Capo riguarda le modifiche al titolo e alle premesse del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196; mentre al Capo II si trovano le modifiche alla parte I del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196. Il Capo III concerne le modifiche alla parte II del codice in materia di protezione dei dati personali di cui decreto legislativo 30 giugno 2003, n. 196; al Capo IV invece si trovano le modifiche alla parte III e agli allegati del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196; infine al Capo IV sono riportate, come già detto, le disposizioni processuali.

Nell’ambito di tutela del trattamento dei dati di ogni tipo d’età di utente online (quindi anche i minorenni), rivestono particolare importanza dei dati genetici, biometrici e relativi alla salute (che, ex art. 2-septies, viene subordinato anche al rispetto di misure di garanzia disposte dal Garante). Riguardo a questi il comma 7 precisa anche che «Nel rispetto dei principi in materia di protezione dei dati personali, con riferimento agli obblighi di cui all'articolo 32 del Regolamento, è ammesso l'utilizzo dei dati biometrici con riguardo alle procedure di accesso fisico e logico ai dati da parte dei soggetti autorizzati, nel rispetto delle misure di garanzia di cui al presente articolo». Nel medesimo articolo 2 sono presenti anche delle parti relative alle regole deontologiche e all’inutilizzabilità di

determinati tipi di dati, in particolare il quater e il novies. L'art. 2-quater fa salva l'adozione di “regole deontologiche” negli ambiti in cui il Regolamento riserva la materia agli Stati membri: a) trattamenti necessari per adempiere un obbligo legale; b) trattamenti necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri; c) trattamento di dati genetici, biometrici o relativi alla salute; d) talune specifiche situazioni di trattamento di cui al Capo IX.L'art. 2-novies, invece, conferma l'inutilizzabilità dei dati trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali già prevista dall’art. 12 d.lgs. originario.

All’articolo 2 quinquies invece viene trattata la scelta compiuta relativamente al consenso del minore, più precisamente la validità del consenso prestato dal minore in relazione ai servizi della società dell'informazione. È in questo articolo che vengono infatti delineate le condizioni specifiche per la validità del consenso prestato dal minore in relazione ai servizi della società dell'informazione: «il minore che ha compiuto i quattordici anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione» (e non più sedici come era originariamente previsto nello schema presentato alle Commissioni parlamentari e al Garante). La scelta finale segue quanto aveva osservato il Garante che aveva sottolineato che la scelta di fissare il limite a sedici anni non sembrava coerente con altre disposizioni dell'ordinamento dal momento che individuano a quattordici anni il limite di età consentito per esercitare determinate azioni giuridiche (come per esempio il cyberbullismo). Secondo l’opinione del Garante, infatti, sarebbe parso «incoerente ammettere il quattordicenne a prestare il proprio consenso per essere adottato, ma non per iscriversi a un *social network*». Ma proprio perché al minore viene riconosciuta la possibilità di prestare validamente il consenso al trattamento dei propri dati personali in tale occasione, il decreto pone l’obbligo in capo al titolare che offre direttamente ai minori i servizi di redigere «con linguaggio particolarmente chiaro e semplice, conciso ed esaustivo, facilmente accessibile e comprensibile dal minore, al fine di rendere significativo il consenso prestato da quest'ultimo, le informazioni e le comunicazioni relative al trattamento che lo riguardi».

In base al comma 2 «l'esercizio dei diritti di cui al comma 1 non è ammesso nei casi previsti dalla legge o quando, limitatamente all'offerta diretta di servizi della società dell'informazione, l'interessato lo ha espressamente vietato (anche limitatamente ad alcuni diritti e che potrà sempre modificare o revocare) con dichiarazione scritta presentata al titolare del trattamento o a quest'ultimo comunicata». Il Garante aveva rilevato l'opportunità di consentire il rispetto della volontà dell'interessato di vietare l'esercizio dei diritti di accesso ai dati che lo riguardano suggerendo di introdurre un comma 3-bis in base al quale le clausole contrattuali che prevedono disposizioni in contrasto con quanto stabilito dai commi 2 e 3 sono nulle. Il quinto comma, infine, prevede che il divieto non può in ogni caso produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'interessato ovvero dal diritto di difendere in giudizio i propri interessi. A tale proposito risulta esemplificativo il caso tedesco relativo alla richiesta che una coppia di genitori aveva fatto a Facebook al fine di accedere al profilo della figlia scomparsa al fine di accertare le cause del suo decesso. Dopo una sentenza di primo grado favorevole ai genitori e quella di appello favorevole a Facebook, la Corte Federale di Giustizia ha riconosciuto ai genitori il diritto di accedere al profilo privilegiando il diritto successorio.

Nel caso in cui invece avvenga il reato di "trattamento illecito di dati" (art. 167), sono state introdotte sanzioni e pene che mutano al variare della fattispecie verificatasi. La norma prevede nuove fattispecie di reato tra cui la "Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala" e la "Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala", declinata sempre in relazione a un numero rilevante di persone offese: cfr. artt. 167-bis e 167-ter; ma ne ha anche confermate altre come quella di cui all'articolo 168 ("Falsità nelle dichiarazioni al Garante"). Inoltre l'articolo relativo all'inosservanza di provvedimenti del Garante, numero 170, è stato sostituito. Per quanto concerne le misure minime di sicurezza non più previste dal Regolamento, è stato abrogato l'art. 169: di conseguenza la violazione delle disposizioni in materia di sicurezza sarà sanzionata con misure di carattere amministrativo-pecuniario, ai sensi degli art. 83, par. 5 del Regolamento.

È inoltre stata prevista la cooperazione tra autorità giudiziaria e il Garante, che è competente per l'irrogazione delle sanzioni amministrative eventualmente coincidenti con l'area della rilevanza penale: qui interviene anche la disposizione del comma 6 (mutuata dall'art. 287-terdecies d.lgs. n. 58/1998) volta a disciplinare la possibile convergenza sul medesimo fatto di responsabilità e sanzioni penali e amministrative. È stato infatti previsto che «quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita.[180]

paragrafo 4.2 A livello nazionale Garante per la protezione dei dati personali polizia postale

A livello nazionale per quanto concerne la tutela dei minori sono preposte principalmente due autorità: il Garante per la protezione dei dati personali e la Polizia postale.

La prima autorità, in merito alle funzioni specificamente riguardanti le attività dei minori online, ha il compito di proteggere i loro dati e di fornire ai genitori indicazioni utili per consentire loro di collaborare alla realizzazione di questi obiettivi. A tale fine il sito ufficiale del Garante è provvisto di una pagina apposita intitolata "Pagina informativa sui minori, nuove tecnologie e protezione dei dati".

Anche la Polizia postale ha funzioni specifiche in merito all'attività online dei minori dal momento che si occupa prevalentemente di vittime del computer crime[181]. Tale protezione è svolta dall'Unità di analisi del crimine informatico

[180] F. Valerini (avv. Cassazionista e Dottore di ricerca all'Università di Roma Tor Vergata), "Pubblicate le norme di adeguamento al Regolamento europeo sulla privacy", Diritto e Giustizia, 5/09/2018.

[181] Computer crime: qualsiasi reato che per la sua realizzazione richiede l'ausilio di un pc. È definito dalla legge 547/93 come ogni comportamento previsto e punito dal codice penale e dalle leggi speciali in materia, in cui un qualsiasi strumento informatico o telematico rappresenti un elemento determinante ai fini della qualificazione dell'illecito. F. Caccetta, "Abbandonati nella Rete- Internet e adolescenti", MGC Edizioni, 2016, pag. 162.

(U.A.C.I.[182]) che studia e analizza il fenomeno del computer crime in collaborazione con i maggiori istituti universitari italiani.

Entrambe queste Autorità sono nate nell'anno 1996, ma mentre il Garante per la protezione dei dati personali è stato istituito con la legge 31/12/1996, n. 675, poi confluito nel Codice in materia di protezione dei dati personali (d. lg. 30/06/2003 n. 196), la polizia postale ha conosciuto un diverso processo di sviluppo. La sua genesi infatti è sì da collocare nel medesimo anno 1996, ma a quell'epoca si trattava di Nucleo Operativo di Polizia delle Telecomunicazioni (N.O.P.T.): un'équipe di professionisti impegnati nell'attività di contrasto ai crimini nel settore delle telecomunicazioni. La sua nascita è stato il preludio alla creazione della Polizia Postale nel 1981, con la legge di riforma della Polizia di Stato. Infine il decreto del ministro dell'Interno del 31 marzo 1998, ha portato all'istituzione del Servizio Polizia Postale e delle Comunicazioni al cui interno sono confluite le risorse del N.O.P.T. e della divisione Polizia Postale. Successivamente nel Decreto Interministeriale del 19 gennaio 1999 il Servizio Polizia Postale e delle comunicazioni è stato indicato quale organo centrale del Ministero dell'Interno per la sicurezza e la regolarità dei servizi di telecomunicazioni.

[182] Unità di analisi sul crimine informatico (Computer Crime Analysis Unit). Composta da personale tecnico ed investigativo, tale Unità si occupa di molteplici settori del crimine informatico, le sue attività principali sono: ricerche e studi sul fenomeno della criminalità informatica in collaborazione con Università, Aziende ed Istituzioni;
sperimentazione di nuove tecniche investigative in materia di computer crime;
progettazione di percorsi di formazione sulla sicurezza informatica e computer crime in collaborazione con Università e aziende;
divulgazione di informazioni e risultati di ricerche in contesti scientifici;
assistenza psicologica degli investigatori che si occupano di computer crime (pedofilia).

A seguito della loro istituzione, al Garante e alla polizia postale sono state assegnate delle aree d'intervento in parte differenti, in parte in comunicazione tra loro: differente perché all'Autorità amministrativa indipendente con funzione di controllo[183] sono state assegnate competenze relative alla tutela dei dati degli utenti online, mentre alla polizia postale compete la garanzia della libertà di qualunque forma di comunicazione ai cittadini. In comunicazione tra loro dal momento che riguardano gli utenti online e che questi debbano sottoscrivere contratti che hanno per oggetto i trattamenti dei loro dati personali per comunicare. Infatti questa fattispecie si verifica ogni volta che un navigatore online si iscrive ad un social network: lo scopo è comunicare e il passaggio per accedervi è dato dalla cessione di alcuni dati personali. La quantità e l'utilizzo di questi ultimi sono disciplinati dall'attività del Garante ai sensi del Regolamento generale sulla protezione dei dati personali (UE) 2016/679 (art.51) e del Codice in materia di protezione dei dati personali adeguato alle disposizioni del Regolamento UE attraverso il Decreto legislativo 10/08/2018, n.101 oltre che da vari atti normativi italiani e internazionali.

Nel caso di trattamenti che violino le disposizioni del Regolamento, tale Autorità può rivolgere ammonimenti al titolare del trattamento o al responsabile dello stesso e ingiungere di conformare i trattamenti alle disposizioni del Regolamento; inoltre ha la competenza di imporre una limitazione provvisoria o definitiva del trattamento, incluso il divieto di trattamento, oppure di ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento. Il Garante ha inoltre le competenze per adottare i provvedimenti previsti dalla normativa in materia di protezione dei dati personali, formulando anche pareri su proposte di atti normativi e amministrativi; ed è previsto che tenga dei registri interni delle violazioni più rilevanti e imponga sanzioni pecuniarie ove previsto dal Regolamento e dalla normativa nazionale.
In aggiunta il GPDP ha un dialogo stretto con le autorità nazionali, dal momento che partecipa alla discussione su iniziative normative con audizioni presso il Parlamento e può segnalare al Parlamento stesso e ad altri organismi e istituzioni

[183] Ovvero il GPDP.

l'esigenza di adottare atti normativi e amministrativi relativi alle questioni riguardanti la protezione dei dati personali. Sempre al Parlamento ed al Governo trasmette una relazione annuale sull'attività svolta e sullo stato di attuazione della normativa sulla privacy.

Inoltre il Garante partecipa alle attività dell'Unione europea ed internazionali di settore, anche in funzione di controllo e assistenza relativamente ai sistemi di informazione Europol, Schengen, VIS, e altri; cura l'informazione volta a sviluppare la consapevolezza del pubblico e dei titolari del trattamento in materia di protezione dei dati personali, con particolare attenzione alla tutela dei minori, coinvolgendo, ove previsto, i cittadini e tutti i soggetti interessati con consultazioni pubbliche dei cui risultati si tiene conto per la predisposizione di provvedimenti a carattere generale.[184] Per raggiungere tale obiettivo si avvale della collaborazione delle altre Autorità di controllo e presta assistenza reciproca al fine di garantire l'applicazione e l'attuazione coerente del Regolamento.

Tra le istituzioni con cui collabora il Garante per il raggiungimento dei propri obiettivi figura la polizia postale, che a sua volta si occupa di tutelare la segretezza della corrispondenza e della libertà di qualunque forma di comunicazione dei cittadini, valori riconosciuti e sanciti dall'art. 15 della Costituzione. Per riuscire efficacemente nella realizzazione della sua mission sono state definite otto aree d'intervento quali: pedopornografia; cyberterrorismo, *copyright, hacking*, protezione delle infrastrutture critiche del paese, analisi criminologica dei fenomeni emergenti, giochi e scommesse online.

Per consentire un'adeguata protezione è però necessario che gli utenti sappiano a chi rivolgersi e con quali modalità. Chiunque abbia qualche necessità circa la tutela dei propri dati personali può contattare il Responsabile della protezione dei dati presso il Garante indirizzando una lettera al Garante per la protezione dei personali - Responsabile della Protezione dei dati personali, Piazza Venezia, 11, 00187, Roma, oppure inviando un'email all'indirizzo rpd@gpdp.it. L'interessato può presentare un'istanza al titolare, senza particolari formalità (ad esempio, mediante lettera raccomandata, telefax, posta elettronica, ecc.). Nel sito ufficiale

[184] Informazioni reperite sul sito del GPDP nell'apposita sezione, dove l'Ufficio del Garante ha pubblicato delle schede di sintesi di tali informazioni a scopo divulgativo.

del GPDP è specificato che l'istanza può essere riferita, a seconda delle esigenze dell'interessato, a specifici dati personali, a categorie di dati o ad un particolare trattamento, oppure a tutti i dati personali che lo riguardano, comunque trattati. Il titolare inoltre deve fornire idoneo riscontro all'istanza, ovvero deve inviarla senza ingiustificato ritardo, al più tardi entro 1 mese dal momento in cui riceve l'atto che rende necessaria l'istanza stessa; tenendo in considerazione che tale termine può essere prorogato di 2 mesi, qualora si renda necessario in ragione della complessità e del numero di richieste. In tal caso, il titolare deve comunque darne comunicazione all'interessato entro 1 mese dal ricevimento della richiesta.

Se il titolare ritiene che il trattamento dei dati che lo riguardano non è conforme alla disposizioni vigenti ovvero se la risposta ad un'istanza con cui esercita uno o più dei diritti previsti dagli articoli 15-22 del Regolamento (UE) 2016/679 non perviene nei tempi indicati o non è soddisfacente, l'interessato può rivolgersi all'autorità giudiziaria o al Garante per la protezione dei dati personali, in quest'ultimo caso mediante un reclamo ai sensi dell'art. 77 del Regolamento (UE) 2016/679.

Il titolare del trattamento può quindi agire sostanzialmente in due modi per richiedere la tutela dei propri dati: il reclamo e la segnalazione. Il primo è un atto gratuito circostanziato con il quale si rappresenta una violazione della disciplina rilevante in materia di protezione dei dati personali (articolo 77 del Regolamento UE 679/2016 e artt. da 140-bis a 143 del Codice). Al reclamo segue un'istruttoria preliminare e un eventuale successivo procedimento amministrativo formale che può portare all'adozione dei provvedimenti di cui all'articolo 58 del Regolamento. Avverso la decisione del Garante è ammesso il ricorso giurisdizionale ai sensi degli articoli 143 e 152 del Codice e dell'articolo 78 del Regolamento. La segnalazione può essere fatta da chiunque ai sensi dell'art. 144 del GDPR. Il Garante, dopo aver ricevuto e esaminato ricorsi, reclami e segnalazioni, può vietare i trattamenti illeciti o non corretti e, se necessario, disporne il blocco; promuovere la conoscenza della disciplina in materia di trattamento dei dati personali, ed infine, erogare eventuali sanzioni amministrative e penali.

Più semplice è invece la procedura per rivolgersi alla polizia postale: in questo caso basta una denuncia tramite le *hot line*[185] della polizia postale delle comunicazioni. A quel punto l'istituzione, in collaborazione con gli omologhi uffici di polizia stranieri nel contrasto al *cybercrime* e le altre istituzioni (tra cui Ministero delle Comunicazioni e l'Autorità garante per le comunicazioni) nonché gli operatori privati che si occupano di comunicazioni in genere, gestirà i casi e le emergenze denunciati.

Come già trattato in precedenza, tra i pericoli online più diffusi in cui si possono imbattere gli utenti minorenni figurano il *revenge porn* ed il cyberbullismo.

In merito al *revenge porn* riveste particolare importanza la legge 205 di conversione del Decreto Capienze: essa estende la tutela per soggetti di qualunque nazionalità, anche alle registrazioni audio, oltre alle immagini e video di cui è vietata diffusione; inoltre, la legge recepisce in materia le osservazioni emerse nel corso delle audizioni presso la Camera ed il Senato. Al secondo comma dell'articolo 144-*bis* viene specificato che per i minorenni la richiesta può essere effettuata da chi esercita la responsabilità genitoriale o la tutela.
Ad ogni modo, l'invio al Garante delle immagini o dei video a contenuto sessualmente esplicito riguardanti soggetti terzi, effettuato dall'interessato, non integra il reato di diffusione illecita di immagini o video sessualmente espliciti. Viene inoltre previsto che il Garante, con proprio provvedimento, può disciplinare specifiche modalità di svolgimento dei sopra citati procedimenti e le misure per impedire la diretta identificabilità degli interessati.
Tra i nuovi poteri del Garante in materia di *revenge porn* introdotti dalla legge di conversione del Decreto Capienze vi è anche un importante strumento di tutela utile ed efficace per le vittime di questo fenomeno: la possibilità per gli ultra quattordicenni di inviare segnalazioni e reclami direttamente al Garante privacy. In tale modo anche loro nel momento in cui possiedono il fondato timore che le loro foto o i loro video intimi possano essere diffusi senza il loro consenso su Facebook o Instagram, hanno la possibilità di segnalare questa eventualità

[185] Linea telefonica riservata a comunicazioni d'emergenza

ottenendo come conseguenza che le immagini oggetto di preoccupazione vengano bloccate.
Il canale di segnalazione preventiva è stato attivato in Italia, come programma pilota, nel 2020 da Facebook ed era stato accessibile fino ad ora nel nostro Paese solo attraverso una associazione no profit.
La procedura prevede che le vittime si rivolgano al Garante consultando la pagina www.gpdp.it/revengeporn, per segnalare l'esistenza di immagini video o audio, a sfondo sessuale, ripubblicati senza consenso in modo sicuro e confidenziale. Nella pagina predisposta dal Garante, le potenziali vittime di pornografia non consensuale possono pertanto scaricare un modulo da compilare per fornire all'Autorità le informazioni utili a valutare il caso e a indicare all'interessato il *link* per caricare direttamente le immagini sul programma. Una volta caricate, le immagini sono cifrate da Facebook tramite un codice "hash", in modo da diventare irriconoscibili prima di essere distrutte e, attraverso una tecnologia di comparazione, bloccate da possibili tentativi di una loro pubblicazione sulle due piattaforme[186].

Al fine di una maggiore tutela delle vittime la legge prevede oneri non solo per le piattaforme ma anche per i fornitori di servizi di condivisione di contenuti che erogano servizi digitali in Italia; fornitori che sono tenuti ad indicare senza ritardo al Garante o pubblicare nel proprio sito internet un recapito al quale possono essere comunicati i provvedimenti adottati dal Garante. In caso di inadempimento dell'obbligo, il Garante diffida il fornitore del servizio ad adempiere entro trenta giorni. In caso di inottemperanza alla diffida si applica la sanzione amministrativa pecuniaria di cui all'articolo 83, paragrafo 4, del Regolamento europeo per la protezione dei dati personali.

Gli operatori delle Forze dell'Ordine, medici, psicologi, ed insegnanti possono venire a conoscenza di episodi di violenza sui minori solo mediante acquisizione diretta della denuncia della vittima oppure con una informazione indiretta o mascherata dell'abuso. Ma mentre nel primo caso è relativamente semplice

[186] M. Alovisio, "L'impatto della legge di conversione del D.L. 8 ottobre 2021 n. 139 "Decreto Capienze" sulle misure di prevenzione e contrasto del revenge porn", Diritto e giustizia, 20/12/2021.

iniziare l'indagine e incriminare e smascherare i sospetti (anche se poi c'è il problema di stabilire l'attendibilità della vittima o di chi denuncia), nel secondo caso fanno fede abilità e perspicacia dei singoli operatori che si imbattono nella situazione dell'abuso o sospetto di abuso. In quest'ultima tipologia di casi bisogna saper cogliere i segnali, anche involontari, inviati dalla vittima. Per operatori e medici sanitari in genere, vige l'obbligo di segnalare il possibile abuso per mezzo di referto; anche le Forze dell'Ordine sono in tali casi sospetti di riferire all'Autorità Giudiziaria. Il Senato italiano ha recepito, verso la fine del 2012, la "Convenzione per la protezione dei minori contro lo sfruttamento e l'abuso sessuale" divenuta legge con l'introduzione della parola "pedofilia" nel codice penale italiano.

Per evitare che i pedofili abbiano una finestra aperta nella camera di bambini e ragazzi, attraverso i loro pc o telefoni, con canali privilegiati che li facciano sentire al riparo da occhi indiscreti come soprattutto le chat dei social, è consigliabile tenere il computer nella cucina o comunque in una stanza dove si transita spesso in modo da poter controllare cosa accade sullo schermo con cui si interfacciano i minori. In questo modo si assicura al ragazzo la sicurezza di un controllo che anche se non continuo, gli permette di non essere solo e di discernere cosa farebbe off-line e cosa invece no. Solo il 24% dei ragazzi è accompagnato in prima persona da un genitore durante la sua esperienza di navigazione in rete e se il 18% può contare su un controllo saltuario, il restante 58% dei minori è completamente abbandonato alla rete, secondo quanto riportato dall'ICAA[187] in un'indagine del 2008. Inoltre, tra il campione dei genitori intervistati in occasione di tale report, il 66% ha fornito ai figli informazioni riguardo ai rischi della navigazione mentre il 34% non è riuscito, o perché non conosceva le modalità con cui affrontare il discorso o perché non ha le competenze per farlo. Quanto ai minori intervistati, al 52% è capitato occasionalmente su un sito pornografico; il 13% ha affrontato via chat discorsi su tematiche sessuali con un adulto

[187] International Crime Analysis Association, associazione professionale fondata nel 1990 per fornire formazione, letteratura, networking e risorse per lo sviluppo professionale alle persone coinvolte nella professione di analisi del crimine. F. Caccetta, "Abbandonati nella Rete- Internet e adolescenti", MGC Edizioni, 2016, pag. 18.

(presumibilmente pedofilo) ed il 70% che ha avuto incontri online con presunti pedofili, ha evitato di dirlo ai genitori[188].

In merito alle modalità con cui combattere il cyberbullismo e la forma ad esso correlata di *cyberstalking* non si può non fare riferimento all'istituto dell'Ammonimento di cui all'art. 8 legge 11/2009. Esso prevede che fino a quando non è proposta querela per il reato di cui all'art 612-bis del codice penale (riferito agli atti persecutori), la persona offesa può esporre i fatti all'autorità di pubblica sicurezza (carabinieri, polizia di stato, polizia locale) avanzando richiesta di ammonimento verso l'autore della condotta. Da qui la richiesta viene trasmessa al Questore che, qualora ritenga fondata l'istanza (a seguito di informazioni dagli organi investigativi se necessario e sentite le persone informate dei fatti), ammonisce oralmente il soggetto verso cui è stato richiesto il provvedimento, invitandolo a tenere una condotta conforme alla legge e cessare immediatamente i comportamenti segnalati.

Nel caso in cui questa misura non bastasse, l'*offender* può incorrere nella pena prevista dall'articolo 612-bis codice penale a seguito di una procedura d'ufficio (quindi indipendente dalla volontà della vittima). Tuttavia, nonostante la preziosissima collaborazione dei fornitori dei servizi telematici con le Forze dell'Ordine, ai fini della tutela della vittima minorenne si rivelano cruciali la rapidità di denuncia e la conservazione della documentazione riguardante le conversazioni con il persecutore. Tuttavia, anche nei casi di cyberbullismo è bene considerare che l'imputabilità del minore sia subordinata ad un criterio cronologico, in particolare: da 0 a 14 anni non è mai imputabile perché nei suoi confronti è prevista una presunzione assoluta d'incapacità, senza cioè prova contraria, come riportato nell'art 97 codice penale: "*non è imputabile chi nel momento in cui ha commesso il fatto, non aveva 14 anni". Nel caso in cui il minore abbia più di 14 anni, ma comunque meno di 18, è imputabile solo se il giudice ha accertato che al momento del fatto aveva la capacità di intendere e di volere".* L'art 98 del codice penale infatti dispone che è imputabile chi, nel momento in cui

[188] F. Caccetta, "Abbandonati nella Rete- Internet e adolescenti", MGC Edizioni, 2016, pag. 87 e ss.

ha commesso il fatto, aveva compiuto 14 anni, ma non ancora 18, se aveva la capacità di intendere e di volere.

paragrafo 4.3 Alcuni casi noti all'opinione pubblica.

Un recente fatto di cronaca relativo al suicidio di una bambina di dieci anni a seguito alla sua adesione alla "*blackout challenge*"[189] ha fatto particolarmente scalpore. La piccola protagonista, Antonella, dal giorno del suo decimo compleanno aveva ricevuto un cellulare e questo regalo l'aveva resa felicissima, era sempre stata attratta dai social che seguiva dal telefono della madre per imparare a truccarsi e acconciare i capelli, tanto da aver deciso di voler diventare un'estetista. Possedeva 10 account Facebook, 3 su Instagram e uno su Tik Tok. La madre teme che proprio tramite un contatto conosciuto su quest'ultimo la piccola sia venuta a conoscenza di tale serie di sfide e sia stata convinta a parteciparvi, in nome della popolarità online che tanto le stava a cuore. I genitori sono concordi nell'affermare che la loro figlia era molto obbediente e gentile, pertanto non avevano mai sentito il bisogno di requisirle il cellulare per controllarglielo, erano convinti che il loro insegnamento in merito al fatto che in famiglia tutti si dicessero tutto per aiutarsi fosse costantemente messo in pratica dalla piccola, con la quale peraltro entrambi avevano un buon rapporto, anche in termini di confidenza e fiducia, o almeno, così credevano.
Invece qualche segreto lo aveva, a cominciare dalla password del telefonino che ha reso necessario l'ausilio di un tecnico informatico per sbloccarlo e consentire agli agenti che si sono occupati del caso di fare chiarezza su quanto accaduto. L'unica cosa certa già prima dello sblocco del cellulare era che Antonella avesse chiesto in prestito al padre una sua cintura con cui poi aveva tentato la prova

[189] La "blackout challenge", una delle discendenti della challenge "Blue whale", è una sfida online che consiste in una serie di prove di coraggio (così definite da chi le sottopone all'attenzione dei ragazzi) sempre più pericolose che culminano con la loro morte. I ragazzi che vi aderiscono in genere lo fanno spinti dalla volontà di entrare a fare parte di gruppi esclusivi, per sentirsi potenti, per essere leaders, per potersi vantare con gli amici. A. Ananasso La Repubblica, articolo online, 21/01/2021.

della "*blackout challenge*" di schiacciarsi la carotide per poi liberarla un attimo prima di soffocare ma a causa della perdita dei sensi non ci è riuscita in tempo[190].

A seguito di tale caso il GPDP ha imposto a Tik Tok il blocco all'uso dei dati degli utenti per cui non fosse stata accertata l'età e ha richiesto a Facebook, che controlla anche Instagram, di riferire quanti altri profili avesse la minore, ma soprattutto, come fosse stato possibile che una bambina di 10 anni fosse riuscita a farsene più di uno in più social differenti. Facebook ha fornito entro i successivi 15 giorni un riscontro circa le precise indicazioni sui metodi d'iscrizione ai social e sulle verifiche dell'età dell'utente adottate al fine di controllare il rispetto della età minima d'iscrizione.

Inoltre, il 27/01/2021 il Garante ha avviato un'iniziativa verso Tik Tok e gli altri social maggiormente usati dai minori avviando un'istruttoria in merito all'accesso ad essi da parte degli utenti minorenni. Tik Tok, dal canto suo, si è impegnata a rimuovere tutti i propri utenti italiani con meno di 13 anni entro il 9/02/2021 e a richiedere di indicare la data di nascita per l'utilizzo dell'applicazione, utilizzando sistemi di intelligenza artificiale per individuare gli utenti. Inoltre il suddetto social ha manifestato il suo impegno nel lancio di una campagna informativa sull'app e altri canali, rivolta prevalentemente ai genitori, in merito alla pubblicazione di banner informativi riguardo agli strumenti di sicurezza e ponendo gli utenti a conoscenza del fatto che verranno inviate loro notifiche *push* prima di bloccarli. Nel frattempo il Garante insieme al Telefono Azzurro avvierà nelle televisioni nazionali una campagna di sensibilizzazione per richiamare i genitori a svolgere un ruolo attivo di vigilanza e prestare maggiore attenzione quando ai loro figli verrà richiesta l'età per accedere a Tik Tok.

Ma non è stata questa l'ultima volta che Tik Tok è finita nell'occhio del mirino del Garante della Protezione dei Dati Personali: anche nell'anno successivo al 2021 gli sono state rilevate delle criticità. Tra queste vi è senz'altro la poca chiarezza circa le informazioni rese agli utenti, le impostazioni predefinite poco rispettose

[190] R. Marceca, la Repubblica online, 23/01/2021.

del quadro normativo in materia di *privacy*[191], nonché la scarsa tutela in merito al divieto d'iscrizione dei minori che è facilmente arginabile dichiarando una data di nascita falsa. Il GPDP avvia quindi un'istruttoria in base alla necessità di garantire ai più piccoli la tutela della privacy attraverso un'informativa agli utenti che prenda in considerazione anche la situazione specifica dei minori ed i rischi ai quali essi si espongono. Il 7 febbraio 2022 il Garante ammonisce quindi la piattaforma social in merito all'illiceità di profilare gli utenti ed inviare pubblicità mirata senza l'esplicito consenso; una settimana dopo il *social network* ha informato l'Autorità di aver sospeso il progetto di personalizzazione della pubblicità per gli utenti maggiorenni.

Anche più recentemente l'attenzione resta puntata sui *social network* e la loro sicurezza per i minorenni che vi si iscrivono. In particolare, il 10/05/2022 si è tenuta l'ultima riunione del Tavolo tecnico del Ministero della Giustizia sulla tutela dei diritti dei minori nell'ambito dei *social network* e dei servizi digitali in genere. La Sottosegretaria Anna Mancina ha sostenuto che l'accesso alla rete sia un diritto da assicurare ai minorenni in quanto fa parte della loro costruzione dell'identità, in perfetto accordo con quanto detto dal Ministro della Giustizia Marta Cartabia. Per consentire tutto questo sono inoltre state fatte delle proposte d'intervento come: il diritto all'oblio dei contenuti pubblicati; il provvedimento che verifica i profitti online creati dai minori (ispirato ad una legge francese) ed infine, un nuovo sistema di verifica dell'età basato sulla certificazione dell'identità da parte di terzi (presumibilmente i genitori)[192].

Il secondo caso, invece, viene qui riportato per mostrare il potere persuasivo dei media rispetto all'opinione pubblica e riguarda due adolescenti di Los Angeles scappate di casa e che ha fatto puntare il dito contro il social Myspace[193]. All'inizio

[191] In particolare, il social preimposta come "pubblico" il profilo degli utenti andando così contro alla normativa sulla protezione dei dati personali che prevede l'adozione di misure organizzative e tecniche per scegliere se rendere i propri dati accessibili o meno da un numero indefinito di persone.

[192] d.m. 21 giugno 2021 – Presidente On. Avv. Anna Macina, Sottosegretario di Stato alla Giustizia, relazione finale del tavolo tecnico sulla tutela dei diritti dei minori nel contesto dei social networks, dei servizi e dei prodotti digitali in rete.

[193] Myspace, nato negli Stati Uniti nel 2003, è stato il primo social network a permettere la personalizzazione del proprio profilo per mezzo di immagini, video e suoni, tanto che all'inizio veniva utilizzato dai musicisti come vetrina per avere visibilità, e dagli appassionati di musica per segnalare i propri gruppi musicali agli amici. La versione italiana della stessa piattaforma si è diffusa nel maggio del

delle indagini infatti, erano convinti che fossero state rapite da qualche adescatore conosciuto in chat e la notizia sensazionalistica si è diffusa a macchia d'olio negli Stati Uniti scatenando sospetti verso i social network e Myspace in particolare. Il tutto mentre i responsabili della piattaforma non solo hanno attivamente collaborato alle indagini, consentendo di ritrovare in breve tempo le ragazze, ma anche quando alla fine si è scoperto che in realtà la piattaforma non aveva affatto messo le giovani nelle grinfie di qualche pericoloso molestatore. Quando la polizia le ha trovate, le minorenni hanno confessato di essersi messe d'accordo per scappare insieme e poter vivere così la loro storia d'amore ostacolata dai familiari di entrambe.

Nonostante questa verità, quando sono state intervistate alcune famiglie residenti nelle zone di Los Angeles che avevano seguito la vicenda dagli inizi, è emerso che avessero capito che le ragazze erano state salvate dal rapimento di un pedofilo conosciuto in una chat di Myspace: ignoravano completamente la verità e si erano semplicemente lasciate convincere da questa teoria completamente infondata, dando per scontata la sua attendibilità[194]. D'altra parte simili storie, sfruttando il meccanismo delle *echo chambers*, che conoscono a propria volta florida espansione in rete, non è raro che si diffondano rapidamente, poggiandosi su paure e pregiudizi delle persone. In questo modo però ad aumentare sono solamente timori che non hanno fondamento e che tolgono attenzione ad aspetti che ne meriterebbero molta di più, come ad esempio le dinamiche che spingono gli adolescenti verso i comportamenti a rischio. D'altra parte è risaputo che la mente umana è spaventata da ciò che non comprende, così come i genitori inesperti in ambito informatico lo sono circa l'utilizzo di Internet ed in particolare dei *social network*, in questo caso, da parte dei figli, tanto che come dimostrato da questo fatto di cronaca non si è esitato a scagliarsi contro il social stesso ed i suoi gestori. Tutti accusati di aver messo le due ragazze in contatto con un

2007 e ha conosciuto notevole fortuna, tanto che nel 2009 è stato il social network più utilizzato al mondo. I. Casadei, "Genitori social ai tempi di Facebook e Whatsapp- gestire opportunità e rischi delle nuove tecnologie", A. Bilotto, Red!, 2014, pag. 21.

[194] d. boyd, "It's complicated – La vita sociale degli adolescenti sul web", Castelvecchi, 2014, pag. 152 e ss.

fantomatico molestatore che, a detta dei genitori delle due protagoniste della vicenda, le avrebbe rapite.
Non è chiaro se i genitori in questione fossero già a conoscenza del fatto che le ragazze fossero fuggite appena hanno deciso di avvisare le autorità, così come resta ancora oscuro se anche la menzione del social e del timore che questo le avesse messe in contatto col rapitore fosse stata fatta al solo scopo di concentrare l'attenzione pubblica e quella delle forze armate sul caso, al fine di farlo risolvere più celermente dandogli maggiore risonanza mediatica.
Eppure, nonostante la mobilitazione mediatica notevole attorno al caso, non è stata diffusa in maniera accurata assieme alla notizia del ritrovamento delle minori, l'informazione che i gestori del social (Myspace) si erano impegnati sin da subito nella collaborazione con le Forze Armate, tanto da consentire non solo un tempestivo ritrovamento delle due giovani, ma anche tale da fare chiarezza sulla natura del loro gesto.
Dopo due ore dalla loro sparizione, la quindicenne e la tredicenne protagoniste di tale vicenda, si erano collegate al proprio account da un computer in una zona di Los Angeles differente dal condominio dove vivevano con le loro famiglie e dal quale erano scappate. Tuttavia è stata proprio la registrazione di tale attività online su Myspace che ha permesso alle forze dell'ordine di localizzarle e inviare loro una squadra di salvataggio che le riportasse sane e salve alle rispettive famiglie.

Tuttavia, se è vero che internet può facilitare conversazioni inappropriate tra adolescenti ed adulti, è altrettanto vero che è alquanto difficile che tali conversazioni si spostino su un piano offline senza che il minore ne sia cosciente. Se l'utente minorenne agisse con discrezione, evitando di fornire le informazioni personali tra cui quelle relative al proprio domicilio (oltre al fatto di non adottare comportamenti a rischio che potrebbero renderlo ricattabile), durante la conversazione online esso si troverebbe fisicamente distante dai propri interlocutori eventualmente pericolosi. Inoltre la maggior parte delle volte che un minore viene rapito a seguito di tale attività in rete non finisce nelle mani di uno

sconosciuto (evento peraltro assai raro[195]), ma si scopre essere stato rapito invece dal genitore che non ha il diritto alla custodia del figlio.

[195] d. boyd, "It's complicated – La vita sociale degli adolescenti sul web", Castelvecchi, 2014, pag. 152.

Conclusione:

Nell'elaborato è stata dedicata attenzione alle questioni legate all'attività online degli utenti minorenni, ed in particolar modo alla stipulazione di contratti in rete e poi si è proseguito con un affresco sui rischi maggiormente diffusi cui possono andare incontro i minori nel corso della propria navigazione. Il tema è di stretta attualità non solo per la numerosa frequenza con cui si verificano tali fatti, ma anche per la pericolosità delle conseguenze che comportano soprattutto per quei soggetti che sono stati definiti dal GDPR come "*utenti particolarmente vulnerabili*".

La contrattazione online da parte dei minori, in particolare, è un fenomeno relativamente recente che ha conosciuto una notevole diffusione soprattutto nell'ultimo trentennio. La velocità della crescita di tale fenomeno tuttavia è stata più elevata di quella della sua regolamentazione da parte del legislatore e questo ha reso necessario lo sviluppo di opere di sensibilizzazione rivolte ai ragazzi e alle loro famiglie al fine di fornire loro delle informazioni che avessero la funzione di prevenire comportamenti in rete potenzialmente dannosi per i minorenni nonché per le loro famiglie. Tra questi comportamenti figurano quelli trattati nel terzo capitolo, ove si è voluta fornire una panoramica sui maggiori pericoli del web per i suoi giovani e giovanissimi utenti. Il cyberbullismo infatti viene trattato non solo dal punto di vista del fenomeno in sé, ma anche prestando attenzione ai profili psicologici di chi lo attua e di chi lo subisce; la medesima modalità di trattazione viene usata anche per l'analisi dei danni derivanti dal *revenge porn* così come dalla diffusione inconsapevole dei dati personali. Tali criticità vengono analizzate sia come dinamiche che si instaurano e innescano determinati comportamenti a rischio online, sia sotto l'ottica delle conseguenze che essi generano: in particolare sulle vittime o comunque sui soggetti danneggiati.

L'analisi delle criticità sopra citate nasce dalla volontà non solo di conoscere bene quali esse siano ma anche di capire le modalità con cui vanno affrontate e con cui potrebbero essere arginate. Per arrivare alla realizzazione di simili obiettivi è tuttavia d'obbligo analizzare bene le cause che portano al compimento di certe azioni e alle dinamiche che si innescano nei soggetti protagonisti, ovvero i

minorenni. Pertanto è necessario anche comprendere la realtà in cui vivono, in modo da capire le motivazioni che li spingono ad avvicinarsi al mondo online; oltre alla definizione legale di chi sia il minore, quali tipi di minorenni siano riconosciuti dalla legge e quali azioni possano concretamente compiere nel rispetto della legge stessa.

In questo senso si tenta di comprendere le ragioni che li spingono ad attuare determinati comportamenti in rete. Questi possono essere di varia natura: una particolare attenzione è stata rivolta alla contrattazione online e alla protezione dei dati, visto il significativo incremento che hanno conosciuto tali fattispecie soprattutto durante e dopo la pandemia scatenata dal coronavirus che ha costretto il mondo al lockdown. Con la descrizione di questi comportamenti a rischio per i minori che li compiono, si è reso necessario porre l'attenzione anche sulle situazioni in cui i minori non sono solo protagonisti attivi ma anche vittime, come accade ad esempio nelle situazioni di cyberbullismo.

È oltretutto importante considerare che tali comportamenti nascono da motivazioni ed esigenze differenti: per comprendere un fenomeno, infatti, è bene conoscerne le cause scatenanti in modo da poterlo analizzare nel modo più corretto possibile al fine di trovarvi una soluzione adeguata. Per questo la tesi ha posto l'attenzione sulle nuove generazioni, sulle loro idee in merito ad argomenti quali socialità e privacy, che oggi sono concetti molto differenti rispetto a quelli concepiti dalle generazioni precedenti. I luoghi d'incontro, nonché le opportunità di conoscere nuovi amici e di fare rete con altre persone per crescere sono radicalmente mutate con l'avvento di Internet, dei social media. Forse, alla luce dei fatti accaduti dal 2020 in poi si potrebbe anche considerarla in parte una fortuna. Tuttavia è bene che questa venga amministrata con saggezza dalle nuove generazioni che necessitano di guide, rappresentate dagli adulti di riferimento. Ecco quindi che gli "immigrati digitali" si trovano a dover fronteggiare il gap generazionale con i propri figli caratterizzato dal differente significato associato allo stesso significante[196], dalla differente ottica con cui vengono viste

[196] La stessa parola viene intesa in modo differente da genitori e figli: ad esempio la "privacy" per i primi veniva intesa come la possibilità di non condividere i propri fatti personali se non a voce con qualche

ed utilizzate le nuove tecnologie[197], dalla credenza circa le superiori capacità delle nuove generazioni relative all'uso della rete, e infine dalla necessità di proteggere i propri figli dai numerosi pericoli sconosciuti che si aggirano nel mondo virtuale tanto quanto in quello reale. Tuttavia è proprio la scarsa conoscenza del virtuale a mettere i genitori maggiormente in allarme circa il fatto che i figli frequentino tale luogo piuttosto che il mondo offline: di quest'ultimo conoscono rischi, pericoli, rimedi e metodi di prevenzione, dal momento che anche loro vi hanno trascorso la giovinezza, quanto al primo invece necessitano di una più specifica formazione per poter essere delle guide sicure per i minorenni[198].

Nel corso di tale trattazione sono stati riportati alcuni strumenti online a loro disposizione per poter perseguire tale scopo tra cui *software* che limitano il numero dei siti visualizzabili dai minori, forme di sicurezza per le applicazioni maggiormente diffuse e utilizzate (come Facebook e Google play, per esempio), numeri verdi da chiamare in caso di contratti particolari stipulati online, nonché chat che consentano loro di mettersi in contatto con altri genitori e professionisti per condividere le loro preoccupazioni. Tuttavia le modalità descritte, per quanto numerose e varie, ancora non raggiungono tutti i potenziali interessati in merito alle conoscenze che potrebbero fornire e queste ultime sono talvolta incomplete, perché vengono veicolate da studiosi ma raramente da coloro che hanno esperienza sul campo. Si fa quindi riferimento alle Forze Armate impegnate a seguire i casi in corso e con alle spalle l'esperienza di averne risolti in precedenza. La necessità di un loro intervento è stata riconosciuta come desiderabile dai suoi stessi membri, come sostiene il carabiniere Francesco Caccetta[199], che per mostrare la validità di quanto affermato riporta l'esempio degli Stati Uniti d'America, in cui alcuni membri dell'FBI, adeguatamente formati

persona fidata mentre per i secondi comporta il pubblicare informazioni in rete in merito ad un determinato aspetto di sé in modo da non dovere rendere pubblici anche gli altri.

[197] Spesso motivo di apprensione negli adulti che non sanno come utilizzarle mentre anche se i più giovani hanno lacune in merito alle competenze necessarie per utilizzarle al meglio, le utilizzano serenamente nella convinzione che siano intuitive e quindi possano imparare nuove funzionalità mano a mano che proseguono con il loro uso.

[198] D. Lovara, "I bambini sono sempre gli ultimi", bur Rizzoli, saggi, 2020, introduzione e pag. 73 e ss.

[199] F. Caccetta, "Abbandonati nella Rete- Internet e adolescenti", MGC Edizioni, 2016.

in tale compito, regolarmente si recano negli istituti scolastici nelle zone della loro giurisdizione per fare formazione in merito a rischi e opportunità offerti dalla Rete ai minorenni.

Anche in Italia sarebbe interessante formare un nuovo corpo di forze dell'Ordine con la specifica formazione che gli consenta di essere divulgatori adeguati sia per i minorenni che per le loro famiglie in merito a materie quali la sicurezza online. In tale modo si arginerebbe il problema dello scarso numero di forze dell'ordine disponibili per tale compito divulgativo. Il nuovo corpo, dopo un'adeguata formazione, andrebbe a collaborare poi con gli altri membri delle Forze dell'Ordine impegnate a risolvere concretamente i casi. Inoltre dovrebbero essere organizzati dai Comuni incontri serali, nei quali i membri delle Forze Armate o gli esperti del mondo digitale espongano ai genitori i rischi legali, psicologici e psicofisici in cui incorrono i figli minorenni lasciati soli nella navigazione online. Assieme a tali informazioni andrebbero comunicate anche le misure di prevenzione che garantiscano una certa sicurezza a genitori e figli, nonché i contatti delle Istituzioni cui rivolgersi al verificarsi in casi di problemi, in modo da potere agire tempestivamente per assicurare la tutela dei minorenni che navigano in internet.

Volgere lo sguardo ad altri Stati permette di osservare se sia possibile adottare soluzioni maggiormente efficaci ed efficienti, e consente di cogliere la complessità della regolamentazione dell'attività online nonché il diverso contenuto che viene attribuito alla capacità del minore nei vari ordinamenti. La necessità di trattare tale tematica nasce infatti dalla imponente molteplicità di possibilità e di rischi offerti dal mondo online che estende la sua rete di diffusione

anche all'esterno dei confini nazionali dei singoli Stati e viene regolamentato in maniera differente da Paesi anche territorialmente contigui. La difficoltà di regolamentazione dell'attività in rete è dovuta proprio alle caratteristiche della stessa, la quale si evolve più velocemente delle leggi che la regolamentano e che valica i confini dei singoli Stati avendo di per sé una natura globalizzante che la rende il mezzo perfetto per favorire la globalizzazione stessa di cultura, servizi e pericoli. Non può quindi riscontrarsi uniformità né nelle Autorità preposte ai controlli, né nei procedimenti da seguire in caso di lesione dei diritti dei minorenni.

Si tratta di temi complessi, disciplinati da una legislazione in parte carente in parte articolata che ha conosciuto notevole sviluppo negli ultimi decenni. L'analisi del tema della tesi da un punto di vista giuridico non poteva prescindere dall'analisi dell'aspetto psicologico e umano che caratterizza i comportamenti dei soggetti protagonisti, i minori e i genitori, perché solo la comprensione del fenomeno consente di capire la ratio della disciplina e i metodi preventivi più efficaci per evitare comportamenti potenzialmente dannosi.

Bibliografia:

1. Antonina Astone, “I dati personali dei minori in rete- dall’internet delle persone all’internet delle cose”, Giuffrè Francis Lefebvre, 2019.
2. Patrizio Bianchi, “4.0 la nuova rivoluzione industriale”, ilMulino, 2018.
3. danah boyd, “It’s complicated”, prefazione Fabio Chiusi, traduzione di Federico Bertagna, Castelvecchi (Lit edizioni), 2014.
4. Andrea Bilotto, Iacopo Casadei, “Genitori social ai tempi di Facebook e Whatsapp- gestire opportunità e rischi delle nuove tecnologie”, Red!, 2014.
5. Francesco Caccetta, “Abbandonati nella Rete- Internet e adolescenti”, MGC Edizioni, 2016.
6. Aldo Cazzullo; con Rossana e Francesco Maletto Cazzullo, “Metti via quel cellulare– un papà. due figli. una rivoluzione”, Mondadori, strade blu, 2017.
7. Maddalena Cinque, “Il minore contraente- contesti e limiti della capacità”, Cedam, 2007.
8. Cesare Cornoldi, Chiara Meneghetti, Angelica Moè; Claudia Zamperlin, “Processi cognitivi, motivazione e apprendimento”, il Mulino, 2018.
9. Antonella Dario, Antonino La Lumia, “Minori, internet e social network”, Giuffrè editore, 2021.
10. Marco Faccioli, “Minori nella rete”, Keyeditore, 2015.
11. Carola Frediani, “Cybercrime”, Hoepli, 2019.
12. Vera Gheno e Bruno Mastroianni, “Tienilo acceso- posta, commenta, condividi senza spegnere il cervello”, Longanesi, 2018.
13. Michele Iaselli, “Investigazioni digitali”, Giuffrè editore, 2020.
14. Giuseppe Lavenia, “Mio figlio non riesce a stare senza smartphone”, Giuntiedu, 2019.
15. Daniele Lovara, “I bambini sono sempre gli ultimi”, bur Rizzoli, saggi, 2020.
16. Tamara Maggi, “Giovani connessioni- orientarsi con i figli nel web”, San paolo edizioni, 2020.
17. Angelica Mucchi Faina; Maria Giuseppina Pacilli, Stefano Pagliaro, “L’influenza sociale”, il Mulino, 2012.

18. Carolina Perlingieri, "La tutela dei minori di età nei "social networks"." Rassegna di diritto civile 4 (2016): 1324-1340. Print.
19. Walter Quattrociocchi, Antonella Vicini, “Misinformation – Guida alla società dell’informazione e della credulità”, FrancoAngeli, 2016.
20. Ruben Razzante, “Informazione: istruzioni per l’uso”, Cedam, 2014.
21. Giuseppe Riva, “Nativi digitali”, ilMulino, 2019.
22. Roberto Senigaglia, “Minore età e contratto- contributo alla teoria della capacità”, G. Giappichelli editore, 2020.
23. Arianna Thiene, “Ragazzi perduti <<online>>: illeciti dei minori e responsabilità dei genitori”, Dogi, 2018.
24. David Weinberger, “La stanza intelligente, la conoscenza come proprietà della rete”, Codice edizioni, 2012.
25. Relazione annuale del GPDP 2021 (pagine: 126, 128, 137-140, 151-157, 194-198)
26. Liuc Papers n.138 (pubblicazione periodica dell’Università Carlo Cattaneo, 2003, collana cessata)
27. Francesca Puppoli, ogni immagine è stata ideata da me, disegnata a mano, trasformata in pdf ed inserita nella tesi.

Sitografia:

1. https://www.dirittoegiustizia.it/#/documentDetail/9507972
   "L'impatto della legge di conversione del D.L. 8 ottobre 2021 n. 139 "Decreto Capienze" sulle misure di prevenzione e contrasto del revenge porn", Mauro Alovisio, Diritto e giustizia, scritto il 20/12/2021, consultato l'ultima volta il 16/09/2022.
2. https://www.dirittoegiustizia.it/#/documentDetail/9141421
   "Il Garante Privacy presenta al Parlamento la relazione annuale delle attività svolte e descrive le prossime sfide", Mauro Alovisio, Diritto e Giustizia, scritto l'8/05/2019, consultato l'ultima volta il 2/09/2022.
3. https://www.dirittoegiustizia.it/#/documentDetail/9176379
   "Protocollo di Intesa contro il cyberbullismo fra il Garante Privacy e la Polizia Postale", Mauro Alovisio, scritto il 16/01/2018, consultato l'ultima volta il 16/09/2022.
4. https://www.dirittoegiustizia.it/#/documentDetail/9163577
   "Il consenso alla pubblicazione di dati dei minori di anni 14 in internet spetta ai genitori", Valentina Antonia Papanice, Diritto e giustizia, scritto il 17/04/2019, consultato per l'ultima volta l'1/09/2022.
5. https://www.dirittoegiustizia.it/#/documentDetail/9158720
   "Pubblicate le norme di adeguamento al Regolamento europeo sulla privacy", Fabio Valerini, Diritto e giustizia, scritto il 5/09/2018, consultato l'ultima volta il 30/08/2022.
6. https://www.diritto.it/contratto-quale-eta-si-puo-firmare/
   "Contratto, a quale età si può firmare?", Alessandra Concas, Diritto e giustizia, scritto il 23/05/2018, consultato l'ultima volta il 13/09/2022.
7. https://www.euroconsumatori.org/it/minorenni_in_internet
8. https://www.letture.org/investigazioni-digitali-michele-iaselli
9. https://per-legal.com/home/gli-acquisti-online-del-minore/
10. https://dbhub.it/minori-e-contrattazione-anche-online/
    "Minori e contrattazione, anche online", Valentina Zani, dbHUB, scritto il 31/03/2022, consultato l'ultima volta il 15/09/2022.

11. https://www.altalex.com/documents/news/2020/12/18/sicurezza-on-line-minori-rapporto-eta-consenso-digitale
"La sicurezza on line dei minori in rapporto all'età del <<consenso digitale>>", Caterina Cernicchiaro, Altalex, scritto il 18/12/2020, consultato l'ultima volta il 16/09/2022.
12. https://www.questionegiustizia.it/articolo/cyberbullismo_scuola_famiglia-e-servizi-dopo-la-legge-71-del-2017_20-12-2017.php
"Cyberbullismo: famiglia, scuola e servizi dopo la legge 71 del 2017", Maria Pia Fontana, Questione giustizia, scritto il 20/12/2017, consultato l'ultima volta il 14/09/2022.
13. https://vitolavecchia.altervista.org/chi-sono-i-nativi-digitali-quali-sono-le-caratteristiche/
"Chi sono i nativi digitali? Quali sono le loro caratteristiche?", Vito Lavecchia, Altervista
14. https://www.agendadigitale.eu/scuola-digitale/scuola-competenze-e-nativi-digitali/
15. https://www.treccani.it/enciclopedia/manuel-castells-olivan/
16. https://protezionedatipersonali.it/gruppo-di-lavoro-art-29
17. https://www.focus.it/tecnologia/digital-life/riconoscimento-facciale-ultima-frontiera-marketing-shopping
"Il supermercato ti riconosce dalla faccia", Rebecca Mantovani, Focus, scritto il 23/04/2017, consultato il 13/09/2022.
18. https://www.smartius.it/ecommerce/acquisti-online-minorenni-come-prevenirli/
19. https://www.federalismi.it/ApplOpenFilePDF.cfm?artid=26959&dpath=document&dfile=15072014172042.pdf&content=Corte%2Bdi%2BCassazione%2C%2B%2BSentenza%2Bn%2E%2B25774%2F2014%2C%2Bin%2Bmateria%2Breato%2Bdi%2Bsostituzione%2Bdi%2Bpersona%2B%2D%2Bstato%2B%2D%2Bdocumentazione%2B%2D%2B
consultato il 16/09/2022.
20. https://www.bolognatoday.it/cronaca/come-funziona-app-polizia-youpol.html consultato il 16/09/2022.

21. https://www.bolognatoday.it/cronaca/youpol-app-polizia-droga-bullismo.html consultato il 16/09/2022.
22. https://www.poliziadistato.it/articolo/135e74a0112e9af858848025 consultato il 16/09/2022.
23. http://dati.istat.it/Index.aspx?QueryId=23020# consultato l'ultima volta il 17/09/2022.
24. https://www.punto-informatico.it/nativi-digitali-analfabetismo/ "Nativi digitali: analfabetismo che non ti aspetti", Giacomo Dotta, 19/10/2018, ultima consultazione il 19/09/2022, dal sito Punto informatico.
25. https://www.sistemapenale.it/it/scheda/cybercrime-rassegna-novita-marzo-aprile-2021
26. https://www.ilpost.it/2018/03/19/facebook-cambridge-analytica/
27. https://www.repubblica.it/cronaca/2021/01/23/news/antonella_mi_ha_chiesto_una_cintura_e_io_glielo_data_credo_che_in_quei_5_minuti_nella_doccia_non_fosse_in_se_-283852976/ Romina Marceca, la Repubblica, 23/01/2021.