Nativi digitali ed abusi online: profili di rischio e soluzioni legali

1. Introduzione e realtà dei nativi digitali.

In questo studio andremo a trattare delle problematiche legate alla digitalizzazione della società, prestando particolare attenzione ai cosiddetti nativi digitali – ovvero i giovani nati nel mondo già informatizzato – e delle risposte legali che sono state formulate per risolvere le nuove modalità di manifestazione delle vecchie forme di abuso.

È pacifico che la rivoluzione del web 2.0 ha fatto entrare Internet sempre di più nelle nostre vite, in modi non necessariamente prevedibili, se prendiamo in considerazione i social network ed il loro impatto sul concetto di reputazione digitale.

Essendosi originariamente diffuso per finalità commerciali, era difficile immaginare un'evoluzione della rete diversa da quella meramente improntata al business, tuttavia l'apertura e l'utilizzo di Internet da parte delle grandi masse ha preso una direzione più personale ed è nato il paradigma delle "quattro C", ovvero contenuti, connessione, comunicazione e comunità, il cui significato era da ritrovarsi nel nuovo concetto di partecipazione dell'utente alla vita online.
Fu proprio questa nuova forma di collaborazione a definire il web come lo conosciamo oggi, tanto nei suoi risvolti positivi, quanto in quelli negativi, essendo lo strumento intrinsecamente neutrale, null'altro che le interazioni personali possono definirne l'uso.
Tenendo quindi conto della natura del mezzo, è quanto meno ovvio e per nulla pessimista aspettarsi che la difficoltà di normare e far rispettare regole, in un ambiente nato come sostanzialmente libero dagli interventi statali, abbia condotto ad un periodo di vuoto legislativo, o comunque ad una complessa opera di adattamento delle

leggi tradizionali, e questo sia poi risultato in uno sviluppo di condotte abusive.

Quindi, mentre da un lato Internet è stato un ottimo medium per la condivisione di conoscenza, per l'innovazione commerciale e per la realizzazione del libero mercato delle idee, dall'altro lato non si può negare che abbia consentito l'emersione di una serie di condotte abusive, precedentemente aborrite, fosse anche solo per il loro impatto sociale negativo, ora divenute più comuni per una falsa percezione dell'anonimato, tra cui spiccano senza dubbio il *cyberharassment* ed il similare cyberbullismo, il *trolling* ed il *flaming*, riconducibili ai precedenti, ma più innocui, il *cyberstalking*, per cui le attenzioni dedicate ad una vittima raggiungono nuovi livelli di morbosità grazie alla possibilità di un controllo pressoché costante, oppure quei comportamenti aventi una natura sessualizzata, come il *sexting*, il *revenge porn* e l'adescamento, o *catfishing*.

Se possiamo dire che queste manifestazioni di odio e molestie sono gestite con difficoltà persino dagli adulti – e spesso nemmeno da loro, ricordando il caso di Tiziana Cantone, ragazza di Napoli morta suicida all'età di 33 anni a seguito della diffusione di un suo video hard amatoriale, poi divenuto virale – gli adolescenti finiscono per trovarsi in una situazione decisamente più rischiosa; infatti molte ricerche hanno avuto modo di documentare come nonostante l'accesso ad Internet avvenga sempre più in tenera età, stimolato anche da una percezione fallata della rete come fondamentalmente sicura, questo non venga poi bilanciato da una formazione adeguata sui profili problematici della vita online.

Non pochi studi infatti attestano che lo smartphone sia divenuto il regalo per eccellenza della Comunione, la cui "flessibilità distributiva", ovvero la sua capacità di garantire la connessione a prescindere dal luogo e dal momento, rende questo strumento perfetto sia per sfruttare le potenzialità di Internet, sia per esporsi costantemente al possibile abuso altrui.
Tuttavia, solo parte dei rischi che i nativi digitali si trovano ad affrontare sulla rete

derivano dalle interazioni con altri minori; al di là delle molestie di natura sessuale, l'apparente senso di anonimato e la disponibilità tecnologica possono spingere anche certi adulti a mettere in atto condotte abusive verso gli utenti ritenuti più deboli.
È fondamentale ricordare il caso di Megan Meier, ragazza del Missouri, nonché tra i primi casi mediaticamente più famosi di cyberbullismo.
La ragazza infatti fu molestata online in modo continuativo per svariate settimane da una donna sua conoscente, attraverso un profilo falso, fino al momento del suo suicidio.
Tenendo comunque a mente che impersonare qualcun altro online è una condotta considerata reato dalla maggior parte delle nazioni, il dibattito si concentrò sulla lacuna legislativa contro gli abusi digitali.
Rientrerebbe infatti nel diritto di parola la possibilità di esprimere opinioni critiche nei confronti degli altri utenti, e tutt'ora la discussione su eventuali limitazioni di questo diritto è ancora aperta.

Pertanto, pur essendo tecnologicamente più preparati nell'uso delle nuove tecnologie, dobbiamo chiederci quanto i nativi digitali siano in grado di percepire le minacce del web e le implicazioni giuridiche dei loro comportamenti.
Gli studi condotti nel settore, nello specifico per l'Italia quello di *Save the Children* del 2011, hanno riscontrato una preoccupante noncuranza da parte dei più giovani dei rischi di una vita connessa ed una totale ignoranza delle conseguenze legali di azioni avvertite come "innocenti", quale l'apposizione di like o condivisioni di materiale lesivo.

Insieme a questa "ingenuità digitale", altri grandi ostacoli si frappongono tra la tutela del minore online e le potenzialità legislative dello Stato: le principali sono la perizia dei soggetti molestatori e la difficoltà di garantire un intervento pronto ed efficace.
È infatti proprio la natura del medium a rendere difficoltoso l'intervento legale, essendo la rete una realtà in continua evoluzione, di natura transnazionale e dove è

difficile, se non impossibile, determinare i limiti del proprio spazio rispetto all'intervento di terzi.
Il dato infatti, una volta messo online, perde la connotazione di proprietà personale e chiunque può farne l'uso che vuole, e poiché sono introiettate nello stesso specifiche caratteristiche, tanto in tema di immortalità dell'informazione, quanto ad una sua possibile diffusione globale, le conseguenze sono facilmente immaginabili.
Purtroppo, se da un lato l'intervento istituzionale è limitatamente efficace nel tutelare dai comportamenti degli altri utenti, dall'altro è completamente inerme contro quelle fattispecie autoinflitte ma riconducibili ad un uso deviato dello strumento, quali il *vamping*, il *phubbing*, e la dipendenza da Internet, a cui si riconosce comunque lo Stato di malattia lavorativa, visti i suoi risvolti negativi nella vita delle persone.

Non essendo queste devianze arginabili da parte del potere legislativo, questo studio dovrà quindi concentrarsi sulle interazioni con i terzi, sulle possibilità di danno ai minori, oltre che sulle potenzialità dell'intervento statale.

2. Cyberbullismo e altre forme di cyberharassment.

In tema di cyberbullismo l'elemento che più crea difficoltà è l'assenza di una definizione univoca della condotta.
Il Legislatore italiano ha cercato, con i suoi limiti, di definire le condotte considerabili tali all'articolo 1, secondo comma, della recente legge 71, del 29 maggio 2017, recante "disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", dove risulta

> «qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto di identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti online 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»

Benché voglia essere una definizione più completa possibile, purtroppo la sua stessa natura risulta essere disorganica, illogica e slegata dagli studi condotti in materia di bullismo, soprattutto dal sociologo svedese Dan Olweus.

Vengono infatti accostate condotte di fatto e condotte normative, e allo stesso tempo si circoscrive lo scopo della diffusione online del contenuto alla sola emarginazione sociale del minore.
Dai lavori preparatori della legge risalta infatti l'attenzione posta verso i dati statistici estrapolati da indagini condotte da associazioni private a tutela dei minori, il cui scopo era la quantificazione del fenomeno, non il suo studio, e pertanto resta il rischio di aver circoscritto l'ambito applicativo della legge a condotte che un domani potrebbero non essere più attuali.

Non si è tenuto conto infatti dei tre elementi essenziali del fenomeno bullismo, identificati da Olweus in aggressione intenzionale, sia essa fisica o verbale, ripetizione nel tempo della condotta e squilibrio delle forze, ulteriormente esacerbati dall'utilizzo del web come strumento di violenza.

Riprendendo quanto introdotto prima, uno dei primi casi di cyberbullismo, nonché uno dei più rilevanti fu quello che coinvolse Megan Meier, nel 2006, storico nell'evidenziare le potenzialità di un uso degenere della rete, quanto il livello generale di impreparazione delle necessarie risposte legali.
La principale responsabile fu infatti condannata esclusivamente per violazioni secondarie dei termini di servizio di Myspace, avendo usato un account falso per contattare la ragazza, non essendo prevista all'epoca alcuna criminalizzazione del suo

comportamento.

Forse l'assenza di casi di tale rilevanza mediatica permette di giustificare in tal senso la lentezza con cui ci si è mossi a livello europeo riconducendo pertanto questa a tale motivazione, in assenza ancora una vera e propria normativa unica comunitaria, sostituita da programmi e strategie internazionali, volte a spingere i vari stati dell'unione a formulare le loro risposte secondo certe linee guida.
Le più rilevanti previsioni legali in questo campo sono incluse nella *Data Protection Directive 95/46/EC*, che però limita l'intervento al consenso sul trattamento dei dati, e sull'assenza dello stesso in caso di *cyberharassment*, permettendo l'intervento dell'autorità di protezione dei dati, al fine della rimozione del contenuto, ma senza effettivamente tutelare dalla violenza subita.

Questo apre l'interessante possibilità di considerare l'aspetto del diritto alla privacy come una potenziale risposta a tali condotte abusive, che però incontra il suo principale limite nella libertà di parola, e nella possibilità di attribuire ad una persona determinate condotte o fatti realmente avvenuti, comunque mitigabile dalla previsione del diritto all'oblio, tutti diritti previsti dal Convenzione Europea sui Diritti Umani.

Tuttavia, l'assenza di intervento legislativo non significa che a livello europeo non si sia preso in considerazione il problema, anzi, è già dal 2006 che si ha modo di vedere il primo testo di *Raccomendations on empowering children in the new information and communication enviroment*, seguito poi da ulteriori dichiarazioni e raccomandazioni.

Essendo la definizione di Olweus introiettata nel panorama europeo, sarà buona pratica andare ad analizzare come i singoli elementi che la compongono risultino potenziati dall'uso della tecnologia.

Partendo dal concetto di aggressione intenzionale, si può notare una continuità logica con la ripetizione della condotta, e tenendo conto della precedentemente citata flessibilità distributiva è facilmente intuibile lo squilibrio di forze in campo. Infatti il bullo avrà la possibilità di tenere la propria vittima in un persistente Stato di pressione psicologica, non avendo questi modo di trovare rifugio in nessun luogo e in nessun orario.

La generica concezione di atti intenzionali risulterebbe strumentale all'applicabilità della regolamentazione sul cyberbullismo ad azioni eterogenee poste in atto con strumenti diversi tra di loro, e a tal proposito accademicamente si sono formate due tesi differenti finalizzate al raggruppamento di tali atti in modo organico, la prima distingue in base ai diversi strumenti utilizzabili dall'aggressore per mettere sotto pressione la vittima, mentre la seconda, più adeguata a distinguere i vari episodi, incentra la propria diversificazione sulla condotta e lo scopo.

Ulteriori distinzioni si possono fare sull'identità del cyberbullo, infatti la spersonalizzazione dell'aggressione, compiuta dall'altro lato di uno schermo, solitamente in un posto considerato sicuro, ha svolto la funzione di incrementare la componente femminile tra i perpetratori, in quanto normalmente le ragazze sono avverse all'aggressione fisica.

Questo profilo risulta essere molto interessante nel momento in cui prendiamo in considerazione le principali differenze tra il cyberbullo e la sua controparte offline, rilevando in primo luogo una maggiore leggerezza nel mettere in atto le condotte abusive, dovuta tanto alla concezione della rete come un luogo avulso dalle regole sociali, quanto all'idea di anonimato, che però risulta essere secondaria in molti casi, volendo l'aggressore mettere in mostra le sue "vittorie"; secondariamente si può notare la maggiore facilità a perseguitare la vittima, pervertendo la costante reperibilità che lascia Internet ai propri utenti – e come detto in precedenza annullando qualsiasi possibilità per la vittima di trovare rifugio – e la capacità dell'odio

di diventare transnazionale, andando a complicare ulteriormente la possibilità se non di salvaguardare la vittima, quanto meno di punire l'aggressore.

Nel momento in cui vengono a mancare gli elementi della reiterazione o della disparità di forze, i comportamenti non possono più considerarsi bullismo secondo Olweus, ma vengono viste come forme secondarie di aggressione, che possono risultare limitate nel tempo, o semplicemente bidirezionali, a tali condotte si possono ricondurre i nomi di *flaming* e *trolling*.

Dal lato opposto può posizionarsi il *Cyberstalking*, dove la condotta assume elementi di natura persecutoria, e diventa, almeno nel panorama italiano, un reato perseguibile *ex* articolo 612 *bis* del Codice Penale.

3. Sexting e adescamento online.

Il *sexting*, ovvero lo scambio di materiale di natura erotica, non è nato assieme a Internet.
Ovviamente in passato era decisamente meno diffusa questa pratica, sia per via dello stigma sociale legato ad una spensieratezza sessuale, sia per la difficoltà di procurarsi detto materiale, dovuto anche per la necessità di relazionarsi con un professionista, quale il fotografo, per lo sviluppo della pellicola.
L'avvento della fotografia digitale ha senza dubbio semplificato il processo di produzione, ma è da riconoscersi nell'avvento di Internet, e ancora di più negli smartphone, l'abbattimento delle ultime barriere tecniche alla rapidità di condivisione.
Questa pratica di per sé non è intrinsecamente negativa, tanto quanto possono essere le varie forme di molestie digitali, in quanto nella sua versione primaria, ovvero dove le due parti sono direttamente coinvolte e considerate legalmente capaci, non è altro che una forma di esercizio del diritto di espressione.
Tuttavia, come anticipato poco sopra, il dato digitale non ha un proprietario in grado

di esercitare il diritto di possesso e pertanto, perdendone il controllo, colui che produce il contenuto sessuale si espone al rischio del *sexting* secondario, ovvero la condivisione senza il proprio permesso del materiale in questione.

Il *sexting* secondario, che è probabilmente una delle forme più dannose di attacco alla reputazione – ed infatti fu la causa scatenante del precedentemente citato "caso Cantone" – non sembra però una pratica destinata a cadere in disuso; bisogna riconoscere difatti che questa forma di "intimità digitale" permette tanto agli adulti, quanto agli adolescenti, di poter esplorare liberamente la propria sessualità, e recenti studi hanno dimostrato come l'incidenza del fenomeno sia in crescita, soprattutto tra le fasce più giovani della società.
Per quanto si possa riconoscere un valore sostanzialmente neutro a queste interazioni relazionali, è pacifico che nel momento in cui uno dei due soggetti sia un minore mentre l'altro un adulto, il disvalore di tale condotta incarni il fatto tipico dei reati ex articoli 600 *ter* e 600 *quater*.
La digitalizzazione di questo approccio però comporta problematiche non necessariamente successive alla produzione del contenuto; come abbiamo visto per il fenomeno delle molestie, difatti, la spersonalizzazione creata dall'utilizzo della rete non garantisce che la persona con cui stiamo interagendo sia veramente chi sostiene di essere – anzi, come si può vedere per la *sextortion*, l'utilizzo di profili falsi per acquisire materiale di ricatto è la norma – esattamente come l'eccessiva confidenza del proprio controllo sulla situazione spingono i soggetti ad esporsi a pericoli che solo successivamente arriveranno a danneggiarli.

È in questo panorama che le iniziative europee per la tutela del minore sono entrate in gioco, a partire dal 2007, data in cui venne redatta a Lanzarote l'omonima convenzione, mirante a uniformare le risposte europee al problema, fondando i principi del testo pattizio sul

«diritto di ogni minore a ricevere da parte della sua famiglia, della società e

dello Stato e misure di protezione rese necessarie dal suo status di minorenne»

L'Italia ha ratificato tale Convenzione il 23 ottobre 2012, all'interno della legge numero 172, abbracciando la visione secondo cui il minore non è più solo un soggetto debole la cui tutela è cura dello Stato e della famiglia, ma diventa il figlio di tutti i soggetti che incontra sulla rete, e di conseguenza merita di ricevere assistenza, cura e tutela da parte di chiunque.
Tale legge ha avuto un impatto rivoluzionario sull'ordinamento italiano, ma per ora ci concentreremo sull'introduzione dell'articolo 609 *undecies* all'interno del Codice Penale, rubricato "adescamento di minorenni", volto a punire "qualsiasi atto volto a carpire la fiducia di un minore" prevedendo nello specifico anche l'utilizzo della rete Internet.

A differenza però della soluzione comunitaria, la legge italiana fa un passo oltre, in quanto non solo punisce l'adescamento andato a termine, ma configura il reato ex articolo 609 *undecies*, come reato di pericolo astratto, andando a porre l'antigiuridicità della condotta nel momento ideativo del reato, andando a colmare la lacuna della legislazione precedente, ovvero la legge 38/2006, che configurando il reato come di pericolo concreto, consentiva la non punibilità nel momento in cui l'adescamento non si concretizzava.

Tuttavia, per poter rendere il reato suscettibile di anticipazione della tutela penale, è Stato necessario identificare almeno dal punto di vista della dottrina le condotte che si presumono essere pericolose, e recenti studi hanno permesso di suddividere il fenomeno del *grooming* in cinque fasi tipiche.

Inizialmente, durante il cosiddetto *friendship forming stage*, l'adescatore, in seguito ad un processo di selezione della vittima basato su alcune specifiche vulnerabilità della stessa, inizia ad instaurare un rapporto con lei, solitamente entrando in discussione come un normale utente, e costruendo quella che è considerata una prima

conoscenza virtuale.
Successivamente, durante il *relationship forming stage*, viene consolidata l'amicizia con l'interlocutore, con la finalità di entrare nelle grazie della vittima come punto di riferimento per questioni sempre più personali.
L'ingresso in questa fase è sintomatico di come il *groomer* sia riuscito ad abbattere le barriere della naturale diffidenza.
Quasi contemporaneamente all'inizio della seconda fase, il perpetratore mette in atto il *risk assestment stage*, ovvero in base alle informazioni carpite al minore valuta se sia il caso o meno di continuare la relazione.
In questa fase è interesse dell'adescatore capire dove vive la vittima, e che livello di controllo sulla sua attività online esercitino i genitori.
Nel momento in cui ottiene la certezza di poter agire senza intralci, il pedofilo da inizio all'*esclusivity stage*, la fase in cui si cerca di porre come unica fonte di confidenza del minore, creando una forma di intimità virtuale volta a far sentire questi a suo agio, e poter quindi intaccare il lato più recondito della personalità del minore, i suoi desideri, in un'atmosfera di complicità.
È proprio quando si approfondisce questa fase che si può considerare raggiunto l'obiettivo del *groomer*, ovvero quando gradualmente sfuma nella fase nota come *sexual stage*, e ha la possibilità di decidere se mantenere il rapporto nella virtualità o stabilire un contatto reale col minore.

Ciò che rende davvero complesso intervenire per tempo non è solo la riservatezza che l'adescatore convince il minore a adottare, ma anche la volontà sociale di ignorare siffatte realtà fintanto che non si verifichino raccapriccianti episodi criminali che coinvolgano i minori, come i recenti casi delle *grooming gangs* in Inghilterra, organizzazioni criminali volte al commercio di minori, che nel silenzio mediatico hanno avuto modo di adescare e abusare più di 700 adolescenti.

Nel momento in cui vengono trattate tali tematiche però, l'approccio tenuto dal punto di vista giornalistico è solitamente sensazionalistico, e finisce con avere poco

impatto sulla necessità di un serio dibattito, anche accademico, dimostrando come la migliore arma del pedofilo è la non volontà di affrontare la questione e relegarla solo alle pagine di cronaca nera, recando danno in primo luogo alle vittime, che vengono private della necessaria formazione sull'argomento, in modo da avere un più efficace strumento di difesa dagli abusi.

4. Risposte legali ed extralegali.

È proprio in tema di formazione del minore che sono stati mossi i primi passi per una tutela extra istituzionale, da parte dei Social Network Service Providers, tra i quali Facebook in prima linea, attraverso la predisposizione nel 2009 di una carta di autoregolamentazione, stipulata in concerto con organizzazioni non governative e la commissione europea, titolata "*safer social networking principles for the EU*", che prevedeva tramite un'opera di collaborazione tra i firmatari l'approntamento di linee guida e buone pratiche finalizzate a migliorare la sicurezza delle interazioni online poste in essere da minori, attraverso l'uso dei social network.

Dei sette principi fondanti la carta, è possibile notare due linee di pensiero principali: la prima diretta ad instaurare una migliore consapevolezza sulle potenzialità dello strumento da parte degli utenti, mentre la seconda finalizzata a concretizzare l'impegno da parte dei sottoscrittori di operarsi per rendere le piattaforme dei luoghi relativamente più sicuri per i soggetti più deboli.
Al di là delle intenzioni, questa manovra, cui fecero comunque seguito altre dichiarazioni di intenti da parte delle stesse società, incontrò non pochi problemi attuativi, tra disomogeneità degli interventi da parte dei singoli provider e la talvolta assente implementazione delle misure di sicurezza previste, quanto meno nel breve termine, rendendo palese come i potenziali conflitti di interesse commerciale potessero ostacolare l'effettiva tutela del minore.
Pertanto, risulta pacificamente la necessità, se non di un intervento diretto da parte delle figure istituzionali, quantomeno la predisposizione di un *framework* minimo

all'interno del quale lasciare libertà di movimento a queste iniziative private.

Il Legislatore italiano si è mosso nella direzione più tradizionale, andando a normare, prima con la legge 172/2012 (a protezione dei minori contro l'abuso e lo sfruttamento sessuale dei minori) e poi con la legge 71/2017 (prevenzione e contrasto del cyberbullismo) i profili per la tutela del minore dagli abusi online.
Se però la prima risulta essere più incisiva, prevedendo nuove figure di reato e una generale riforma del diritto penale a salvaguardia del minore, come riportato nel paragrafo precedente, la seconda ha preso un approccio meno drastico e più finalizzato alla rieducazione del cyberbullo minore che alla sua penalizzazione, attraverso l'introduzione di una procedura di ammonimento per certi versi simile a quella già prevista per il reato di stalking.

Un ulteriore elemento estremamente rilevante di tale legge è la previsione di una procedura di *notice & takedown*, sulla falsariga della *eraser button law* californiana, avente lo scopo di eliminare i contenuti d'odio su richiesta della vittima, ma che cerca di fare un passo in più, dando al soggetto richiedente la possibilità di rivolgersi all'autorità Garante della privacy nel caso in cui il provider non agisca in breve tempo, in modo da far ingiungere a questi l'adempimento.

Ciononostante, è importante rilevare la necessaria predisposizione di accordi internazionali finalizzati ad uniformare le forme di tutela in modo univoco, nello stesso modo in cui la *General Data Protection Regulation* intervenne a salvaguardia dei dati personali, al fine di controbattere la problematica della transnazionalità di Internet in modo efficace.

5. Conclusioni.

Tenendo conto di quanto evidenziato in questa introduzione, emerge plasticamente come il principale problema derivante dal sempre più precoce accesso alla rete sia