



PATENTINO DIGITALE

VERSO UN USO CONSAPEVOLE
E GENERATIVO DEI MEDIA

Istituto
degli
Innocenti





PATENTINO DIGITALE

VERSO UN USO CONSAPEVOLE
E GENERATIVO DEI **MEDIA**



CORECOM
TOSCANA



Polizia di Stato
Compartimento Polizia Postale
e delle Comunicazioni per la Toscana



Ministero dell'Istruzione
Ufficio Scolastico Regionale per la Toscana



REGIONE
TOSCANA



Istituto
degli
Innocenti

Presidente
Maria Grazia Giuffrida

Direttore Generale
Giovanni Palumbo

Area infanzia e adolescenza
Aldo Fortunati

Servizio Formazione
Maurizio Parente

PATENTINO DIGITALE
VERSO UN USO CONSAPEVOLE E GENERATIVO DEI MEDIA

Coordinatori alla realizzazione del rapporto
Francesca Conti, Farnaz Farahi, Sara Ferruzzi, Maurizio Parente,
Maria Cristina Macaluso, Anna Manzini

Segreteria di redazione
Paola Senesi

Progettazione grafica e impaginazione
Rocco Ricciardi

Crediti fotografici
Shutterstock

La presente pubblicazione è stata realizzata dall'Istituto degli Innocenti di Firenze nel quadro delle attività previste dall'accordo di collaborazione tra il Comitato Regionale per le comunicazioni della Toscana e l'Istituto degli Innocenti di Firenze (approvato con DD del Consiglio di amministrazione n. 65 del 30/10/2019).
La riproduzione è libera con qualsiasi mezzo di diffusione, salvo citare la fonte e l'autore.
Luglio 2020

Indice

Introduzione	
Verso un uso generativo dei media	6
1. Comunicare: raccontare e raccontarsi in rete	13
2. Identità digitale e privacy	23
3. Informarsi in rete	29
4. Dialogare sui social	39
5. Hate speech	45
6. Sicurezza e responsabilità	51
7. Responsabilità civili e penali	55
8. Acquistare online in sicurezza	69
9. Carte di credito e bancomat: pericoli e precauzioni	79



INTRODUZIONE

Verso un uso generativo dei media¹

Il presente contributo nasce dal coinvolgimento dell'Istituto degli Innocenti all'interno di un percorso formativo finalizzato a trasmettere agli studenti le competenze minime necessarie a navigare in rete e nei *social network* con consapevolezza e responsabilità e a coinvolgere e sensibilizzare scuola e famiglie perché possano essere dei punti di riferimento per i ragazzi.

Gli studenti delle scuole secondarie di primo grado rappresentano infatti una fascia d'età nella quale la navigazione in rete e la frequentazione dei *social network*, probabilmente già avviata nel corso della scuola primaria, diventa più autonoma dai genitori e con un livello di consapevolezza in via di definizione più strutturata.

Le tecnologie digitali si fondano, in maniera sostanziale, sulla possibilità accattivante di un loro utilizzo facile, veloce ed intuitivo, soprattutto da parte dei ragazzi su cui, fin dall'infanzia, esercitano una particolare tipo di attrazione data la facilità che offrono di un approccio immediato, al punto tale che le nuove generazioni vengono oramai definite come "native digitali". La premessa è che oggi si è passati dalla "società dell'informazione" alla "società informazionale", ovvero da una società in cui l'informazione è importante ad una società fatta di informazioni, che comporta l'emergere di nuovi fenomeni, tra cui la violenza nei social, nel dibattito politico, nel sistema dei media, nella società².

Ma le tecnologie informatiche sono molto più di una comune pratica: sono strumenti per tessere legami in un ambiente particolarmente ampio, ricco e complesso rispetto ai classici contesti di scuola e famiglia. Il recupero di un ruolo attivo di sostegno, accompagnamento e guida è dunque imprescindibile in quanto il mondo virtuale è essenzialmente relazionale e come tale porta con sé, dilatandola e trasformandola, la fenomenologia comunicativa, rappresentativa, espressiva e sociale connessa alla costruzione di identità, al bisogno di far parte e di appartenere ad un gruppo e di essere riconosciuti nella propria soggettività. Si tratta di un insieme

¹ A cura di Farnaz Farahi, consulente esterno Istituto degli Innocenti di Firenze.

² Maffei I., Rivoltella P.C. (a cura di), *Fake news e giornalismo di pace. Commenti al Messaggio di papa Francesco. 52ª giornata mondiale delle comunicazioni sociali*, Scholè, Brescia, 2018.

di processi e manifestazioni ricchi di opportunità come pure di insidie anche gravi, a fronte delle quali i giovani hanno necessità di essere adeguatamente preparati e autorevolmente sorretti. Sono infatti le trappole di internet e dei *social media* a preoccupare gli adulti e a prefigurare dipendenze, patologie, scissioni dalla realtà, rischi di manipolazione, disinformazione, frode, abuso e violenza.

Le nuove tecnologie, quindi, non vanno considerate come sostitutive di altre forme di apprendimento e di interazione umana, ma neanche demonizzate come qualcosa da cui difenderci e da cui tutelare e proteggere i ragazzi. Per superare la crisi educativa, è necessario dunque rinunciare a prospettive catastrofiche e «impegnarsi a superare, con uno sforzo adattivo e integrativo, gli ostacoli posti dal *décalage* tecnologico intergenerazionale. Una riflessione sullo specifico pedagogico dell'educazione nell'era digitale può contribuire a delineare un orizzonte di senso per un cammino di crescita autenticamente generativo in cui [...] condividere e promuovere consapevolezza, progettualità e creatività»³ (Le Grange, 2015).

Si rende allora sempre più necessaria la creazione di una cultura condivisa dei media e del digitale. La comprensione da parte di genitori, insegnanti e educatori delle opportunità offerte dall'utilizzo dei media potrebbe portare a massimizzare le qualità comunicative (la comprensione) e generative (la nascita di nuove idee) di questi strumenti come linguaggio della ricerca educativa.

Coloro che ricoprono oggi un ruolo educativo dovrebbero agevolare l'appropriazione da parte dei giovani del funzionamento di un universo virtuale che, tuttavia, essi stessi non padroneggiano o fanno ancora fatica a padroneggiare. Agli adulti sarà allora demandato il compito di mettersi in gioco e accrescere le loro competenze, perché non si può pensare di educare bambini e ragazzi su qualcosa che ancora noi stessi non abbiamo compreso del tutto. È allora auspicabile che gli adulti, la scuola, i servizi educativi ma anche le famiglie collaborino per trasformare quella che è una "naturale" confidenza dei bambini in una reale competenza. La sensibilizzazione di genitori, insegnanti

³ Le Grange L., *Rethinking learner-centred education: Challenges faced by*, in Koopman O., *Science Education and Curriculum in South Africa*, Palgrave Macmillan, Londra, 2016.

ed educatori ad un utilizzo "ecologico", problematico e riflessivo di questi strumenti in ambito educativo e formativo diviene allora la prima sfida di cui la pedagogia si dovrà occupare⁴.

Il presupposto pedagogico è quello di instaurare una comunicazione generativa, una comunicazione che consenta di generare identità, scambi, relazioni sociali, atti condivisi e che possa contribuire a creare e sostenere una cultura condivisa dell'utilizzo dei media ed una competenza digitale e multimediale già a partire dalla prima infanzia, in cui insegnanti educatori, genitori, bambini e ragazzi siano realmente protagonisti attivi⁵.

Ciò si rende possibile attraverso quella che viene definita *Media Education*, il cui obiettivo principale è quello di fornire gli strumenti idonei a comprendere meglio le dinamiche e i messaggi offerti dai media e a rielaborarli autonomamente, approcciandosi ad essi in maniera critica. In questo senso Baacke operazionalizza quattro dimensioni della competenza digitale. La prima dimensione è relativa alla critica dei *media (Medinkritik)*, ovvero la capacità di analizzare processi sociali problematici, di applicare queste conoscenze analitiche al proprio agire e l'armonizzazione socialmente responsabile di queste dimensioni. Il secondo aspetto di riferisce alla conoscenza dei media (*Medienkunde*), ovvero il sapere sui media e la conoscenza dei sistemi dei media, oltre che la capacità di utilizzare gli strumenti e i prodotti tecnologici. La terza dimensione riguarda l'utilizzo dei media (*Mediennutzung*), inteso sia come una competenza d'uso recettiva dei media, sia come una competenza d'uso interattiva e propositiva con i media (la produzione mediale). L'ultima dimensione è relativa all'organizzazione dei media (*Mediengestaltung*), in riferimento agli sviluppi innovativi dei sistemi medialità e alle forme di organizzazione e di costruzione creativa ed estetica⁶ (Baacke, 1997).

Il termine inglese di Media Education, così come quello tedesco di Medienerziehung, si presta meglio di altri usati in altre lingue per esprimere, in modo diretto e sintetico, la molteplicità degli approcci che si intendono instaurare tra le due realtà dell'educazione e dei media. Media Education indica sia l'educazione con i media, considerati come strumenti da utilizzare nei processi educativi generali, sia l'educazione ai media, che fa riferimento alla comprensione critica dei media, intesi non solo come strumenti, ma come linguaggio e cultura. Si può segnalare anche il terzo livello di educazione per i media rivolto alla formazione dei professionisti. Pier Cesare Rivoltella, durante il convegno "Educazione, apprendimento e nuove tecnologie" del 2015, ha esposto dieci tesi rispetto al rapporto tra educazione e media che sono ancora attuali. La prima tesi riguarda la relazione tra Media Education e Education Technology. L'Education Technology è la didattica che fa uso delle tecnologie e considera i media digitali come supporto alla mediazione nei processi di insegnamento e apprendimento. La Media Education invece è qualcosa di propedeutico alla prima, in quanto lavora sui linguaggi

4 Di Bari C., *Educare l'infanzia nel mondo dei media. Il ruolo dell'adulto in famiglia e nei contesti educativi*, Anicia, Roma, 2017.

5 Anichini A., Boffo V., Mariani A., Cambi F. & Toschi L., *La comunicazione formativa. Strutture, percorsi, frontiere*, Apogee, Milano, 2012.

6 Baacke D., *Medienpädagogik, Grundlagen der Medienpädagogik*, Tubiengen, Niemeyer, 1997.

mediali in genere (che ora sono comunque digitalizzati), considerati come artefatti culturali rispetto ai quali sviluppare pensiero critico e responsabilità. La seconda tesi indica che la logica dei consumi culturali non corrisponde a aut aut, ma a et et: le tecnologie non sono sostitutive, ma integrative. Più che fattore di discontinuità, bisogna considerare il digitale come una ri-mediazione della realtà, cioè a una riconfigurazione in un'altra chiave degli elementi della realtà quotidiana. Il digitale non sostituisce, ma arricchisce le nostre possibilità di intervento nel reale. Secondo la terza tesi non sono i media che fanno cose ai ragazzi, ma sono i ragazzi che fanno cose con i media: più che le tecnologie, ciò che conta sono le pratiche. Il rischio non è quello del determinismo tecnologico, ma quello del modellamento sociale. Il rapporto tra formale e informale viene indagato con la quarta tesi: l'informale, oggi, è fatto di tecnologie. Le nostre esistenze sono permeate dal digitale, che media le nostre conoscenze, la nostra rappresentazione e consapevolezza del passato e le nostre relazioni. Tutto ciò implica grandi rischi, ma anche grandi possibilità, che sta a noi equilibrare. Rinunciare però alle tecnologie, significa per la scuola rinunciare al suo compito, che è aiutare i soggetti all'interpretazione della cultura. I media digitali e sociali sono soprattutto macchine autoriali: sono cioè cose o strumenti con cui si possono fare altre cose e valorizzarle a scuola significa portare in classe la dimensione laboratoriale, quindi mettere al centro l'apprendimento per scoperta e un coinvolgimento totale mente-corpo-cervello. La sesta tesi sottolinea che i media sono anche un curriculum: i media non sono solo strumenti, che devono essere utilizzati in classe, ma sono anche una competenza di base necessaria: per cercare e selezionare informazioni, per collaborare e cooperare; per gestire le relazioni, gestire il tempo, gestire il rapporto con i contenuti. Per condividere e pubblicare. Tutte competenze di base a prescindere dai media sociali, ma che questi rendono indispensabili. Con la settima tesi si sottolinea che non abbiamo bisogno di creare nuovi contenuti digitali perché ce ne sono già abbastanza. La questione è piuttosto selezionare e aggregare i contenuti, commentarli e renderli utilizzabili didatticamente. Qui è lo spazio in cui può e deve inserirsi l'insegnante. L'ottavo punto della tesi di Rivoltella afferma che le applicazioni disponibili non sono utili senza una cornice pedagogica: serve un framework metodologico che dia senso all'applicazione. Oltre alla cornice pedagogica, c'è il metodo che funziona come organizzatore professionale. Misurare e quantificare l'efficacia dell'uso delle tecnologie nella didattica è quasi impossibile: l'unico modo è cambiare le pratiche professionali attraverso la tecnologia. Con la nona tesi si evidenzia il concetto del gioco del "noi" e "loro": affermare che i "nativi digitali" siano già in possesso delle competenze digitali, significa ignorare che la loro è solo una confidenza tecnologica, da trasformare in consapevolezza tecnologica. L'ultima tesi riguarda il rapporto tra tradizione e innovazione: due concetti che non sono antitetici. L'unico modo che la scuola ha per salvaguardare la tradizione è innovare.

Lo sviluppo delle competenze digitali si rivela dunque particolarmente importante per una cittadinanza critica, consapevole, attiva e responsabile. L'obiettivo non è quello di mirare a inserire la Media Education o il percorso formativo sul Patentino digitale come un

intervento spot in scuola, ma quello di integrarla armonicamente all'iter del curriculum d'Istituto per promuovere nei ragazzi comportamenti dove il senso critico e la responsabilità di fronte al digitale siano sempre presenti.

Il presente contributo si configura così come importante strumento di consultazione rispetto al mondo digitale, una vera e propria bussola che potrà essere utilizzata tanto da parte dei ragazzi che da parte degli insegnanti e famiglie.

Il primo contributo "Comunicare: Raccontare e raccontarsi in rete" di Mastroianni mira ad evidenziare l'importanza della comunicazione in rete e ne sottolinea le criticità e le potenzialità. L'autore propone alcuni suggerimenti utili per una efficace comunicazione sul web.

Con il secondo contributo, "Identità digitali", Conti propone una disamina dei concetti di identità digitale e di privacy, accompagnata da riferimenti tecnici e suggerimenti per una tutela dei propri dati personali.

All'interno di "Informarsi in rete" il lettore potrà trovare una panoramica sui rischi connessi all'informazione ed un invito ad un uso consapevole delle informazioni rilevate tramite internet, facendo particolare attenzione al fenomeno delle *fake news*.

Con "Dialogare sui social" Mastroianni ci introduce alle potenzialità e alle criticità dell'interconnessione che si verifica sui social, puntando l'accento sulla natura delle relazioni online e dei conflitti che si vengono a creare all'interno dei *social network*.

Attraverso "Hate speech" Andolfi esamina il cosiddetto "discorso d'odio" che si verifica sui social e vengono discusse alcune modalità per contrastare il fenomeno ed i pregiudizi ad esso collegati.

In "Sicurezza e responsabilità" sono delineate le principali forme con cui si può manifestare il fenomeno del *cyberbullismo*, mentre uno sguardo più tecnico viene proposto con il contributo di Pinzani relativo alle "Responsabilità civili e penali" in cui vengono descritti gli illeciti digitali e le relative responsabilità connesse a tali illeciti.

Con "Acquistare online in sicurezza" il lettore viene guidato da Caldesi attraverso il mondo dello shopping online. A partire dalla descrizione del modo in cui sin da bambini si è educati agli acquisti e a divenire consumatori, l'autore suggerisce alcune strategie per un acquisto consapevole.

Il volume si conclude con un contributo dal titolo "I rischi" che integra una serie di informazioni e consigli pratici per un acquisto consapevole, tratti dal sito della Polizia Postale.





1

COMUNICARE:
RACCONTARE
E RACCONTARSI
IN RETE⁷

⁷ A cura di Bruno Mastroianni, Dipartimento di Lettere e Filosofia, Università degli studi di Firenze.

Le parole sono importanti

Comunicare in modo adeguato in rete è un cammino che sicuramente comporta uno sforzo costante e prolungato – molto più complesso delle “cinque regole per avere successo in rete” o dei “dieci passi per rinunciare ai propri profili social” –, ma che parte da una competenza che abbiamo tutti noi, esseri umani, semplicemente in quanto tali⁸, e che spesso diamo per scontata: la parola. In situazioni normali, impariamo a parlare molto precocemente; per questo motivo, il fatto stesso di possedere uno strumento potente e avanzato per la comunicazione e la trasmissione del sapere quale il linguaggio viene considerato “naturale”, e raramente si riflette sulla capacità della parola di costruire o distruggere mondi.

Nel corso degli anni scolastici, si lavora alacremente alla descrizione e comprensione del sistema linguistico e delle norme che lo regolano; tuttavia, concentrandosi soprattutto sulla parte normativa, spesso viene tralasciata la dimensione metalinguistica: cosa possiamo davvero fare con le parole? A cosa ci servono? Che cosa dicono di noi e del mondo in cui viviamo?

La competenza linguistica è insomma centrale, perché la cosiddetta comunicazione deragliata non è frutto della rete e dei social network di per sé, ma è un prodotto completamente umano, sovente provocato proprio da una scarsa attenzione rispetto a quello che si sceglie di dire o non dire.

In altre parole, quasi ogni incidente comunicativo al quale si assiste o del quale ci si ritrova parte in rete non è solo il prodotto volontario della cattiveria umana quanto piuttosto la conseguenza della scarsità di riflessione metalinguistica. Per fare un esempio, spesso i famosi hater altro non sono che adulti tra i cinquanta e i sessant'anni che appaiono avere poca consapevolezza del fatto che l'insulto scritto nero su bianco e firmato nome e cognome sul profilo social di un noto personaggio politico è pubblico e infinitamente longevo; che chi leggerà quel commento si farà, inevitabilmente, una certa idea di chi l'ha postato, idea non mitigata dalla conoscenza personale, ma veicolata solo da quelle specifiche parole; che il fatto di essere dietro a uno schermo non rende realmente anonimi, perfino quando

8 Si veda: https://www.youtube.com/watch?v=fOIM1_xOSro

si sceglie di usare uno pseudonimo; che quell'atto così veloce, apparentemente innocente, potrebbe portare a pesanti ripercussioni mediatiche e in qualche caso anche legali.

Peraltro, l'età dei perpetratori di questo genere di azioni sfata il mito che la scarsa educazione e la superficialità siano caratteristiche prettamente giovanili; questo non toglie che anche i cosiddetti nativi digitali spesso dimostrino di non essere affatto alfabetizzati digitali.

Impariamo a comunicare bene

I problemi, dunque, possono realmente sembrare troppo complicati per essere risolti da noi “comuni mortali”. Al contrario, riteniamo che sia possibile (ri)partire dalle parole per arrivare a competenze comunicative più evolute e tali da rendere ogni persona non solo maggiormente padrona delle proprie parole, ma anche più potente. È una questione di forma e sostanza: non basta avere idee buone, ma occorre anche saperle comunicare nella maniera più corretta a seconda del contesto in cui ci si trova; e da questo passaggio dalle idee alla loro “messa in parola”, che è meno scontato di quanto si possa essere portati a pensare, dipende buona parte delle nostre possibilità di successo comunicativo.

Le massime di Grice: quattro consigli

Un modo tutto sommato semplice di iniziare a riflettere sulla questione viene fornito dalle quattro massime conversazionali individuate negli anni Settanta da Paul Grice; chi ha compiuto studi nell'ambito della comunicazione le conoscerà sicuramente e anzi, magari le considererà quasi banali rispetto a quanto studiato successivamente; tuttavia, nella loro semplicità, sono quattro consigli di puro buon senso comunicativo che possono davvero porsi alla base della comunicazione di ogni persona alle prese con i problemi di una [società ipercomplessa e iperconnessa](#).

- La massima della qualità recita “sii sincero”. In sintesi, se si parla di ciò di cui si è davvero convinti, di ciò in cui si crede, in maniera trasparente e non ingannevole, gli altri se ne renderanno conto. La mancanza di sincerità – per esempio, quando si parla di argomenti che in realtà non conosciamo abbastanza approfonditamente, costringendoci a veri e propri voli pindarici per supplire alla mancanza di competenze – è qualcosa che solo con grande fatica si può tentare di nascondere, sovente in maniera infruttuosa. Di conseguenza, è molto più semplice parlare di ciò che si conosce bene e si condivide.
- La massima della quantità consiglia “non dire né troppo poco né troppo”. Solitamente, sia chi dice troppo poco sia chi dice troppo commette, dal punto di vista della comunicazione, un errore. L'eccessiva stringatezza può destare il dubbio della reticenza, ovvero che si stiano volontariamente omettendo delle cose; dire e scrivere troppo, invece, rischia da una parte di “soffocare” eventuali interlocutori (si pensi solo a quanto è sgradevole un relatore che

non rispetta i tempi prestabiliti a una conferenza), dall'altra di disperdere su particolari secondari l'attenzione di chi sta ascoltando o leggendo. Occorre, invece, sapere quanto dire, nel momento appropriato e rispettando i limiti del proprio spazio, sia che si tratti di un testo scritto sia che ci si misuri con un discorso orale.

- La massima della relazione è “sii pertinente”. Chi ha esperienza di interrogazioni o esami sa bene che il candidato che tende a procedere in maniera dispersiva, partendo magari dalla notte dei tempi invece che rispondere in maniera diretta alla domanda posta, spesso usa questa tattica perché non è ben preparato e cerca, di conseguenza, di gettare fumo negli occhi dell'esaminatore. In un mondo così intasato di comunicazione, sia in entrata che in uscita, la pertinenza di quanto si deve leggere e ascoltare e anche produrre diventa un parametro essenziale per non sovraccaricarsi e non sovraccaricare gli altri. Tra l'altro, proprio perché l'inconsistenza comunicativa è una strategia estremamente diffusa usata per sviare l'attenzione, è anche piuttosto semplice da riconoscere, e non depone mai a favore di chi la impiega.
- Ed ecco, infine, la massima del modo: “sii chiaro”. Italo Calvino, in un saggio del 1988 che ancora adesso può venire considerato uno dei testi basilari per la comunicazione, [Lezioni americane](#), nella lezione dedicata all'Esattezza scrive: «Esattezza vuol dire per me soprattutto tre cose: un disegno dell'opera ben definito e ben calcolato; l'evocazione d'immagini visuali nitide, incisive, memorabili; in italiano abbiamo un aggettivo che non esiste in inglese, “icastico”, dal greco “eikastikós”; un linguaggio il più preciso possibile come lessico e come resa delle sfumature del pensiero e dell'immaginazione». Scegliere di parlare in maniera inutilmente complicata o magari orpello è qualcosa che di fatto va contro la comunicazione stessa: chi si rifugia nei barocchismi, nell'inglesorum o nel latinorum non vuole, in realtà, comunicare veramente, quanto piuttosto creare una distanza, o magari rimarcarla. Essere chiari, scegliere le parole giuste, implica trasparenza di intenti. Chi non ha secondi fini da nascondere può permettersi il lusso di parlare in maniera semplice ed essere diretto.

Riassumendo, le quattro massime poggiano su un assunto piuttosto semplice, ma potente: se si ha ben chiaro in mente che cosa si pensa e che cosa si vuole dire, sarà anche più facile comunicarlo in maniera chiara, soprattutto se avremo l'accortezza di preservare costantemente la relazione con l'altro, in particolare il più svantaggiato dei nostri interlocutori; chi è davvero bravo a comunicare non si rivolge mai all'interlocutore-modello, ma alla persona che incontrerà (per vari motivi) le maggiori difficoltà a comprendere. E parlare in maniera chiara, trasparente e semplice non corrisponde a banalizzare, ma al suo contrario. Mentre banalizzare è una trappola nella quale chiunque di noi può cadere con facilità, la semplicità, la concisione, la comprensibilità sono doti del testo che si possono ottenere con grande impegno e attenzione rispetto a quello che si dice e si scrive⁹. Non è un caso se Pascal, nella Lettera XVI delle Provinciali, si giustifica per la lunghezza della sua missiva scrivendo «Questa lettera è più lunga delle altre perché non ho avuto agio di farla più breve»; e se



⁹ Si veda: <http://www.brunomastro.it/2018/03/breve-ma-intenso-farsi-capire-in-poche.html>

lo dice lui, chi siamo noi per pensare che sia più facile scrivere testi brevi?

Dalle massime di Grice si procede, poi, a entrare nello specifico degli usi delle parole, che in sostanza servono a tre scopi principali.

Presentarsi in rete: parole e immagini per dire chi siamo

Le parole servono, prima di tutto, per parlare di noi stessi, cioè presentarci agli occhi degli altri: operazione che facciamo spesso involontariamente – non avendo piena consapevolezza di come ci dipingano le parole che stiamo usando – ma che può diventare, con uno sforzo tutto sommato contenuto rispetto ai benefici che porta, volontaria e autodiretta.

Il processo di presentazione di sé tramite le parole diventa ancora più rilevante in rete, dove siamo, di fatto, privati dell'aiuto della mimica, della gestualità, della prossemica, del tono della voce, di tutti quegli elementi extralinguistici che aiutano a decodificare correttamente il messaggio che si sta mandando. E per quanto si possano mettere in campo delle strategie compensative (ad esempio emoticon ed emoji), anche tali strategie vanno sapute usare nel modo corretto.

Il compito delle parole di descriverci diventa ancora più rilevante in un mondo in cui, volenti o nolenti, lasciamo una scia pubblica di noi stessi che non ha precedenti nella storia dell'umanità: non occorre più essere VIP per trovarsi in questa situazione, e non serve nemmeno avere degli account social, perché la narrazione di noi stessi dipende oggi anche da quello che immettono in rete di noi i nostri genitori, i nostri amici, i nostri impegni comunitari, mondani o lavorativi, e prosegue con quanto, invece, decidiamo di immettere in rete noi stessi.

Per verificarlo, il punto di partenza che consigliamo è quello di cercarsi con Google: inserire il proprio nome e cognome nel motore di ricerca più potente che esiste oggi e verificare chi siamo agli occhi di chi interroga questo strumento per sapere qualcosa di noi. Siamo ben rappresentati? Ci sono informazioni di cui ci vergogniamo? Spesso, scopriremo che la rete è disseminata di "briciole" che ci riguardano e che non sempre sono state messe in circolo da noi o con il nostro beneplacito. Mentre, però, giocare in difesa è molto difficile – per esempio, anche invocare il diritto all'oblio è un'operazione complessa e che richiede tempo – è in un certo senso molto più semplice adottare una strategia che non sia paranoica ("mi discrivo da ovunque"), ma semplicemente lungimirante ("scelgo io cosa mostrare o non mostrare di me"): è molto meglio, insomma, agire preventivamente, piuttosto che doversi ingegnare nella gestione della crisi a posteriori,

a danno avvenuto.

Se finora può essere sembrato che il fulcro dell'operazione riguardasse le parole che scegliamo di usare, ricordiamo che i nostri primissimi "biglietti da visita" in rete sono solo parzialmente verbali: le immagini che scegliamo come nostre foto profilo sui vari social, assieme alle poche righe di presentazione che normalmente le accompagnano (che alcuni chiamano tagline), sono i primi elementi di noi che gli altri vedono, e in base ai quali possono farsi una prima idea di chi siamo.

Che immagine convoglierà di uno o una giovane la scelta di una foto profilo in costume da bagno, adattissima per riscuotere successo tra i propri coetanei, ma magari meno consona per rappresentarlo o rappresentarla agli occhi dei suoi docenti o di un possibile datore di lavoro? D'altro canto, essendo oggi del tutto normale curare contatti di lavoro tramite i social, anche l'opzione di mettere come propria foto profilo un vaso di fiori o un tramonto in nome della privacy non è probabilmente la scelta migliore: a chi piace interloquire con un oggetto inanimato?

Similmente, con quanta leggerezza ci permettiamo di essere spiritosi o sfrenati nella nostra descrizione (magari specificando che ci siamo laureati presso "L'università della vita"), senza pensare che un qualsiasi "cacciatore di teste" aziendale sicuramente scandaglierà con attenzione i nostri profili, tentando di capire chi siamo veramente, al di là di quanto dichiarato nel curriculum?



like



2

2. IDENTITÀ DIGITALE E PRIVACY¹⁰

¹⁰A cura di Francesca Conti, consulente esterno Istituto degli Innocenti di Firenze.

Cos'è l'identità digitale

Esistono due accezioni dell'espressione identità digitale, la prima è l'insieme di tutte le informazioni che troviamo online su una persona, ma anche su un'azienda o un marchio. In realtà l'identità digitale è un concetto più circoscritto, si tratta dell'insieme di informazioni che, all'interno di un determinato sistema informatico, si riferiscono a una specifica persona.

Alla luce di questa seconda definizione ogni utente della rete possiede con molta probabilità più identità digitali, possiamo infatti considerare ogni account social che una sola persona possiede come identità digitali. Ad ogni social, infatti, ci si iscrive e successivamente si accede grazie a credenziali di accesso, ovvero username e password.

Con la digitalizzazione della pubblica amministrazione e di molti servizi come quelli postali e bancari l'identità digitale diventa un tema molto delicato e di fondamentale importanza ed è necessario che l'autenticazione dell'utente avvenga in maniera assolutamente sicura.

Alcuni esempi di questo tipo di identità digitale sono:

SPID, Sistema pubblico d'identità digitale. Ci si può iscrivere tramite il sito poste.it e/o il sito gov.it, si riceve la propria SPID personale con la quale è possibile, utilizzando gli strumenti digitali, gestire tutte le comunicazioni da e verso la pubblica amministrazione e accedere ai servizi online della pubblica amministrazione.

PEC, posta elettronica certificata che identifica in maniera univoca il mittente o il destinatario di un messaggio, che quindi assume valore legale a tutti gli effetti. Gli iscritti agli ordini professionali hanno l'obbligo di aprire una PEC per poter comunicare con il proprio ordine professionale. La PEC è però utile per tutti, perché anche con la PEC si può comunicare con la pubblica amministrazione, inviare comunque comunicazioni ufficiali ad aziende, società etc. La PEC sostituisce in tutto e per tutto la Raccomandata con ricevuta di ritorno, sempre in uso.

La firma digitale, questa ha lo stesso valore legale di una firma autografa, quindi, a tutti gli effetti, è come se la persona avesse fisicamente firmato un documento.

Quanto detto rende chiaro perché il furto di identità digitale sia uno

dei rischi maggiori dell'utilizzo della rete. È a rischio la privacy perché il ladro d'identità può accedere a tutti i dati sensibili del derubato.

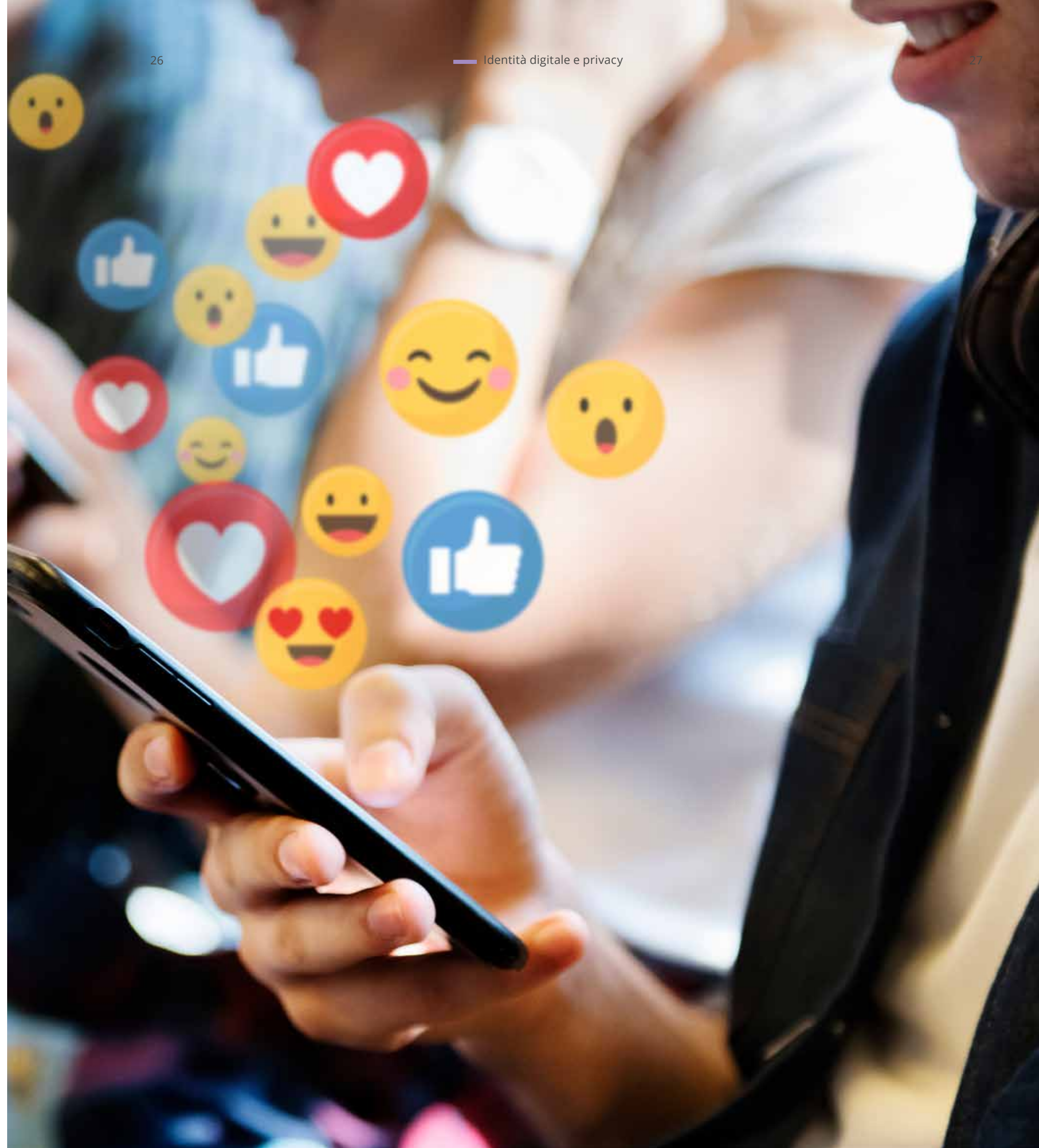
L'identità digitale non va confusa con l'identità virtuale. Infatti mentre l'identità digitale non è altro che un riflesso, un prolungamento di ciò che siamo offline veicolato dagli strumenti digitali, l'identità virtuale è più vicina al concetto di avatar "che viene usato proprio per indicare una dimensione di immaginario digitale, in cui un utente fornisce una rappresentazione fantastica di sé stesso, anche di tipo visuale, come in Second Life". cit. Enciclopedia Treccani.

Cos'è la privacy e perché è un bene da tutelare

Il termine privacy indica il diritto alla riservatezza delle informazioni personali e della propria vita privata. Le normative per la privacy che si sono susseguite negli ultimi anni sono state pensate per salvaguardare e tutelare la sfera privata del singolo individuo, impedendo che le informazioni riguardanti la sfera personale siano divulgate senza l'autorizzazione dell'interessato e che soggetti terzi si intromettano nella sfera privata. La tutela dei dati personali rappresenta il diritto dell'individuo ad avere il controllo sulle informazioni e sui dati riguardanti la sua sfera privata e quello di impedire la rilevazione di informazioni sul proprio conto, affinché questo avvenga la legislazione deve fornire gli strumenti necessari. Il decreto 196 del 2003 "Codice in materia di protezione dei dati personali" è entrato in vigore dal 1° gennaio 2004, nel 2016 per uniformare le normative sulla privacy nazionali e migliorare la protezione dei dati personali dei cittadini europei dentro e fuori l'Unione, il 4 maggio 2016 viene pubblicato in Gazzetta Ufficiale il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, cosiddetto GDPR (General Data Protection Regulation).

Con questo regolamento, la Commissione europea si propone come obiettivo quello di rafforzare la protezione dei dati personali di cittadini dell'Unione europea (UE) e dei residenti nell'UE, sia all'interno che all'esterno dei confini dell'UE, restituendo ai cittadini il controllo dei propri dati personali, semplificando il contesto normativo che riguarda gli affari internazionali, unificando e rendendo omogenea la normativa privacy dentro l'UE.

Il testo affronta anche il tema dell'esportazione di dati personali al di fuori dell'UE e obbliga tutti i titolari del trattamento dei dati (anche con sede legale fuori dall'UE) che trattano dati di residenti nell'UE ad osservare e adempiere agli obblighi previsti.



Contenuti e algoritmi

L'abbondante disponibilità e raggiungibilità delle informazioni impone di avere capacità di discernimento dell'attendibilità dei contenuti e consapevolezza sui meccanismi della conoscenza. Ciò apre un problema non indifferente per il cosiddetto "cittadino mediamente informato", che si ritrova tra le mani, per così dire, la possibilità di gestire in quasi-autonomia la sua dieta mediatica e informativa. Allo stesso tempo, per il funzionamento delle piattaforme tramite gli algoritmi e la profilazione, l'utente medio è sottoposto a una continua offerta di contenuti e connessioni che rispondono pienamente alle sue aspettative, ai suoi gusti, alle sue inclinazioni. Da questo punto di vista, il web e i social network possono diventare un luogo "che dà sempre ragione", in cui trovare costante conferma delle proprie idee e creare cerchie di contatti con persone di opinioni simili che interagiscono rinforzandosi l'un l'altra, con un livello minimo di contraddizioni rispetto alla propria visione del mondo.

Tale comportamento impoverisce molto le potenzialità che la rete offre, essendo la dimensione in cui sarebbe possibile l'incontro con la differenza di prospettive, di idee, di culture, di opinioni, ecc.¹² Il punto è che tale incontro con la differenza deve essere desiderato e non può essere imposto. Non ci può essere l'algoritmo che allarga la visione del mondo: gli algoritmi fanno il loro lavoro cercando di proporci ciò che ci può interessare in base alle preferenze che abbiamo espresso in precedenza. Non ci può essere nemmeno un'autorità esterna che decide cosa è meglio sottoporre all'attenzione: quel ruolo di selezione che un tempo era monopolio dei media, con la rete è impossibile da ripristinare; ora le testate e i giornalisti sono inseriti nel sovraccarico informativo e subiscono la concorrenza dei contenuti che vagano nel web e che intercettano o meno i gusti e le aspettative degli utenti.



¹² Si veda: <http://www.brunomastro.it/2018/11/la-comunicazione-che-mette-tutti.html>

Farsi domande, piuttosto che cercare risposte

Se una soluzione dall'alto è difficilmente praticabile, insomma, ci vuole qualcosa che sia all'altezza della disintermediazione che si è creata: deve maturare in ciascun utente la consapevolezza che per vivere online in modo proficuo occorre attuare alcune strategie per non finire vittime delle proprie convinzioni e della tendenza a vedere il mondo a immagine e somiglianza delle proprie credenze.

Come fare? Se si cercasse di controllare ogni informazione aspettandosi di poterne discernere l'attendibilità in base al contenuto, ovviamente ci si troverebbe di fronte a un'operazione impossibile: occorrerebbe essere già esperti di ogni tema anche solo per informarsi. Per questo, le pratiche del *fact-checking*, seppur importantissime, non aiutano il cittadino mediamente informato in quella sua quotidiana "lotta" per capire se ciò che gli passa davanti è o non è attendibile.

Una strada percorribile è allora quella di capovolgere la questione: non tanto concentrarsi sul contenuto delle informazioni, che può essere di difficile analisi, ma su ciò che sta attorno a esse e che ne indica la provenienza (le fonti), le circostanze (il contesto), lo stile. Il modo con cui sono presentate e da chi, spesso rivela anche qualcosa della loro attendibilità. In *Tienilo acceso* abbiamo proposto una strada non tanto tesa a stabilire in modo incontrovertibile l'attendibilità di un contenuto, quanto alla possibilità di scorgerne limiti, lacune, imprecisioni, falle.

A nostro avviso, questo primo sguardo d'insieme sulle informazioni può diventare un'abitudine alla portata della gran parte degli utenti. Invece di tentare lo sforzo titanico di rendere ciascuno uno studioso tuttologo, si può almeno fare in modo di renderlo un utente che si faccia domande prima di prendere per buona un'informazione. Sono domande semplici, ma fondamentali, che possono essere poste in pochi secondi per giudicare i limiti di un certo contenuto a un primo sguardo.

Questa idea del limite per noi è fondamentale: in una situazione di non-competenza ("non sono esperto di una materia") e di sovraccarico ("ricevo fin troppe informazioni su temi che non sono sicuro siano rilevanti"), la sfida è molto più quella di saper riconoscere i limiti di

ciò che incontro più che quella di tenere tutto sotto controllo. In altre parole, se il cittadino immerso nel caos informativo della rete almeno riesce a riconoscere ciò che è da scartare, è già un passo avanti.

Riconoscere le fake news: cinque domande fondamentali da porsi

Le domande sono fondamentalmente cinque, e vengono dalla tradizione del buon giornalismo:

1. Chi lo dice? Individuare la fonte è il primo passo; se le informazioni sono senza fonte o di fonte incerta o indefinita, vanno prese per poco attendibili.
2. Quando? La data e le circostanze sono molto importanti. Spesso ci sono bufale che tornano ciclicamente; individuarne la provenienza temporale è sufficiente per smascherarle.
3. Qualcuno conferma? La verificabilità di un'informazione è fondamentale. La sua verifica può venire dal testo stesso che si legge, se è riportata una qualche fonte che conferma, oppure dall'esterno: si può raggiungere una fonte che possa confermare? Se non c'è nessuna di queste possibilità, di solito ci si trova di fronte a un'informazione poco attendibile.
4. Chi lo conferma? Se c'è una qualche voce che dà conferma dell'informazione, occorre porsi qualche domanda sulla sua autorevolezza. Uno schema semplice per giudicare l'autorevolezza può essere basato su due parametri: vicinanza al fatto e competenza. La vicinanza fa valutare se la fonte è diretta o indiretta rispetto a ciò che sta raccontando (un testimone o una vittima ad esempio sono fonti dirette). La competenza ci fa valutare se chi sta parlando ha le conoscenze adeguate per giudicare il fenomeno di cui parla. Un esempio per tutti: durante un terremoto una fonte diretta è un terremotato che racconta, ma questo racconto non è detto che sia competente quanto il giudizio di un sismologo che, pur non essendo una fonte diretta, sa meglio giudicare il fenomeno. Fonti dirette e competenti hanno maggiore attendibilità, fonti indirette e incompetenti ne hanno minima.
5. Qualcun altro ne parla? Il confronto è la strada di fatto più semplice per capire quanto un'informazione sia attendibile. Di solito a portata di pochi click si può cercare un'altra versione. La maggior parte delle volte, nell'abitudine a cercare un confronto, si risolve il non cadere in una bufala. Pensiamo al caso del messaggio ricorrente "di' a tutta la tua lista di contatti su Messenger che XY è un hacker...": copiando e incollando il testo su Google praticamente

tutti i risultati riportano che è una bufala. Eppure, molte persone continuano a farlo girare, solo per la pigrizia di non spendere qualche secondo in un facilissimo confronto.

Nessuno si illude che queste domande siano sufficienti. In realtà sono come una base minima di partenza. Senza queste è facilissimo cadere nei propri pre-giudizi: non ci vogliono nemmeno notizie false, è sufficiente la propria distorsione cognitiva.

Altre semplici domande che ci si può porre riguardano lo stile e il modo di presentarsi di un contenuto, che rivelano quanto la sua narrazione sia manipolata *ad hoc* per suscitare una reazione:

- quando un fatto viene riportato in modo manicheo (bianco/nero, buoni/cattivi, giusto/sbagliato) di solito sta cercando di ottenere la nostra reazione attraverso una cosiddetta *formulazione binaria*¹³ che porti a schierarsi assolutamente a favore o contro quel fatto;
- quando la notizia è funzionale ai propri pregiudizi: giovani maleducati, stranieri violenti, islamici terroristi, populistici ignoranti, progressisti buonisti... solitamente i fatti contenuti in tali notizie sono addomesticati per ottenere tale effetto;
- quando il contenuto è riportato con stile complottista¹⁴: “ti stanno nascondendo la verità”, con un “loro” tanto generico quanto indefinito (i poteri forti, le banche, i governi, le lobby);

quando eventuali voci contrarie, anche se argomentate, vengono automaticamente azzittite e ritenute inaccettabili, di solito si è in uno di quei casi in cui una bolla di opinioni omogenee sta forzando le informazioni in una precisa direzione.

In tutti questi casi la difesa possibile (e applicabile da tutti) è la stessa: fermarsi, aspettare, resistere all'idea di farsi immediatamente un'opinione. È un metodo se vogliamo “per sottrazione”, che aiuta a perdere l'illusione e anche la fretta psicologica di dover sempre intervenire. Quella che Antonio Pavolini nel suo *Oltre il rumore*¹⁵, a partire dalla FOMO (la *Fear Of Missing Out*, la paura di rimanere tagliati fuori) ha rielaborato in FOMI: *Fear Of Missing In*, l'insopprimibile esigenza di esprimere la propria opinione e sentirsi parte del flusso sul tema su cui stanno tutti intervenendo in base al momento.

¹³ Cfr. Cosenza G., *Semiotica e comunicazione politica*, Laterza, Roma-Barci, 2018.

¹⁴ Mastroianni B., *La “coperta corta” delle nostre certezze. Perché siamo tutti un po' complottisti*, in <https://www.brunomastro.it/2017/07/la-coperta-corta-delle-nostre-certezze>.

¹⁵ Pavolini nel suo *Oltre il rumore*, Informant, 2016.

Diventare direttori delle proprie timeline

E qui si passa a un ulteriore aspetto della conoscenza del mondo in base alle connessioni in rete. Il funzionamento dei social network si basa praticamente su ogni piattaforma su due criteri:

- le connessioni che abbiamo stabilito (i follow su Twitter e Instagram, le amicizie su Facebook e così via);
- gli algoritmi che scelgono cosa mostrarci come più rilevante tra ciò che proviene da quelle connessioni.

Questo significa che, volendo, ogni utente può intervenire su questo meccanismo per renderlo più efficiente e capace di aprire orizzonti, invece che chiudersi in bolle di interessi e opinioni omogenee. In altre parole, la tendenza automatica delle piattaforme può essere in ogni momento “corretta” dall'azione umana, basta volerlo. La questione, così come quella del discernere l'attendibilità delle informazioni, non è tecnica quanto culturale e diremmo motivazionale: se si vuole si può.

Una strada è quella di utilizzare alcune funzioni che le piattaforme mettono a disposizione. Ognuna ha le sue. Qui possiamo fare l'esempio di Facebook che nelle impostazioni della “sezione notizie” ci permette di intervenire su come vediamo i contenuti che provengono dalle nostre connessioni. Possiamo scegliere ad esempio di “vedere per primi” alcuni contatti rispetto ad altri. Così come possiamo scegliere di “non seguire” una persona a cui abbiamo dato l'amicizia, in modo da non vedere più i suoi contenuti nella nostra timeline.

Si può fare la stessa cosa con i post: indicare all'algoritmo che non si vogliono vedere contenuti di un certo tipo oppure attivare notifiche o salvare contenuti di altro genere per affermare che c'è un interesse esplicito. Insomma, esiste tutta una serie di azioni che ci permettono, volendolo, di personalizzare la propria presenza in connessione con altri in modo che non sia del tutto autoriferita e affidata agli automatismi degli algoritmi. In *Tienilo acceso* abbiamo indicato alcune strade pratiche; alla base della gestione delle proprie connessioni proponiamo tre criteri per riuscire ad avere sempre un po' di stimolo all'apertura e alla riflessione:

- Cercare connessioni con persone con prospettive diverse dalla propria (quanto alla visione del mondo e alla sensibilità) e metterle tra i “vedi per primo”.
- Che queste persone siano rilevanti e competenti, cioè siano persone che sanno ciò che dicono, e che lo dicano mettendoci talvolta in

difficoltà: troppo facile connettersi con “diversi” che poi sono scarsi o poco rilevanti, solo per avere il piacere di smentirli facilmente: è sempre una forma di autoreferenzialità.

- Che siano attendibili: il fatto di non diffondere notizie false o inutili è un criterio fondamentale di selezione all’ingresso.

Con un giro di connessioni sulle varie piattaforme curato in questo modo, si può ottenere una risposta dalla propria vita connessa molto stimolante in termini di nuove conoscenze, connessioni, idee.

Certo, i social non bastano, anzi una dieta mediatica basata solo su ciò che viene dalle proprie connessioni sarebbe davvero povera. C’è bisogno di costruirsi piuttosto una piccola biblioteca di risorse online per informarsi sui temi di interesse e per andare a fonti autorevoli e attendibili, ma intanto vivere usando questi accorgimenti nei propri spazi di interazione può essere il primo movimento verso una presenza online più costruttiva e soddisfacente.





DIALOGARE SUI SOCIAL¹⁶

¹⁶A cura di Bruno Mastroianni, Dipartimento di Lettere e Filosofia, Università degli studi di Firenze. Tratto da Vera Gheno, Bruno Mastroianni, *Comunicare bene in rete, le regole (che tutti dovrebbero seguire) per una internet migliore*, 29.1.2019 in <https://www.agendadigitale.eu/cultura-digitale/comunicare-bene-in-rete-le-regole-che-tutti-dovrebbero-seguire-per-una-internet-migliore/>

Noi e gli altri, tutti interconnessi

Veniamo al tema fondamentale dell'iperconnessione: la questione del parlare con gli altri. Di solito, infatti, quelli che abbiamo trattato finora sono i due aspetti spesso al centro dell'attenzione: quello del sovraccarico informativo, che può portare a distorsioni nella conoscenza del mondo, e quello del sovraccarico di valutazione su sé stessi (l'esposizione pubblica online), che può portare a modalità distorte della formazione della propria identità e immagine di fronte agli altri. Ci si concentra molto su questi due fattori, mentre si trascura un po' il terzo sovraccarico a cui chiunque sia connesso è sottoposto continuamente: il sovraccarico di discussioni.

Non è un caso che in generale questo terzo aspetto venga sostanzialmente ricollegato a definizioni sintetiche e onnicomprensive a cui abbiamo accennato all'inizio, come quelle del cyberbullismo e dell'odio online, che a volte rischiano di trattare in modo riduzionistico qualcosa di complesso e articolato.

L'interconnessione portata dai social "nelle tasche di tutti" infatti ha prodotto un fenomeno di fondo: quello dell'avvicinamento di differenze. L'incontro con la differenza prima della connessione era molto più sporadico e intenzionale, e investiva momenti e dimensioni specifiche dell'esistenza. Oggi chiunque è presente online, in ogni momento, è esposto alla differenza (di visione del mondo, di linguaggio, di cultura, di valori) di chi gli sta attorno, non importa quanto distante.

Questo dissenso, cioè questo sentire e percepire la realtà in modo diverso, irrompe continuamente nelle timeline di tutti, e produce una mole enorme di discussioni che spesso deragliano in litigi. Non è solo né principalmente odio, non è bullismo: è molto più quotidianamente lotta tra differenti visioni che si affrontano, prodotte da persone che non hanno le capacità di farlo.

Litighiamo tanto perché disputiamo poco

La sensazione è che ci siano tanti litigi online perché ci sono troppe discussioni. In realtà è l'esatto opposto: si litiga tanto perché si ha poca capacità di affrontare divergenze di opinione. Andare allo scontro, infatti, è il modo migliore per porre fine a un confronto: si smette di parlare dell'argomento da cui si era partiti, si va sul personale, ci si insulta e ognuno può tornare a "casa" nelle sue convinzioni senza aver spostato di un millimetro le sue idee.

Il tema non è nato con la rete; lo dimostra il lavoro di alcuni come Adelino Cattani (cfr. ad esempio *Botta e risposta. L'arte della replica*, Il Mulino, 2001,) che ormai da decine di anni promuovono palestre di dibattito nelle scuole e nelle università, proprio per rispondere alla mancanza di competenze nella discussione. La rete lo ha messo al centro dell'attenzione perché ormai è sotto forma di dibattito praticamente ogni azione di comunicazione quotidiana: dall'intervento in un gruppo WhatsApp ai commenti in un post fino alle discussioni sotto un articolo di giornale. E non solo il cittadino medio, ma anche le istituzioni, gli stessi media, gli intellettuali, i personaggi pubblici, tutti per il fatto di essere inseriti in un sistema di comunicazione globale (caratterizzato da quella che Manuel Castells ha definito "autocomunicazione di massa"¹⁷), sono sottoposti alla costante pressione di dover discutere su tutto.

È un vero e proprio sovraccarico: le discussioni possono essere troppe, troppo estenuanti, troppo improduttive, creando una condizione di costante scontro che porta alla reazione opposta della rinuncia. Certi fenomeni dello spegnimento e della disiscrizione dai social derivano proprio da questo disagio per il continuo diverbio.

Anche qui, la proposta non può che essere pensata in modo sostenibile e applicabile dal cittadino mediamente informato e connesso, che di certo non può trasformarsi in un disputatore di professione, né può passare la vita a sostenere tutte le discussioni possibili. Ma il tema si pone anche per chi ha un ruolo preminente in società (divulgatori, giornalisti, intellettuali, istituzioni, media, università, aziende), che è chiamato a gestire il sovraccarico di discussioni disintermedie.

¹⁷ Castells M., *Comunicazione e potere*, Università Bocconi, Milano, 2009.

Come discutere nel sovraccarico

Quale strada percorrere? Nello scenario altamente differenziato della connessione in rete sarebbe illusorio pretendere di tenere sotto controllo l'accordo preliminare tra i discutenti. Pensare di poter discutere solo con chi ha reali intenzioni di confrontarsi, sebbene opportuno in situazioni controllate, è impossibile da realizzare online, dove l'assenza di selezione all'ingresso è la base su cui si fonda la partecipazione alla discussione. Applicare una "nuova selezione" significherebbe solo chiudere le discussioni in cerchie ristrette, cosa di un certo sollievo per i discutenti impegnati, ma di nessun effetto sul dibattito aperto che continuerebbe con le sue caratteristiche scomposte.

Anche il richiamo ai buoni principi della discussione di per sé non serve a molto: se le persone commentano in modo istintivo, aggressivo e con modalità inopportune, è inutile farglielo notare, perché quelle modalità deragliate sono esse stesse l'espressione di un disagio: se bastasse fare riferimento a principi non si capisce perché dovrebbero esprimersi in tal modo.

Non rimane che percorrere una terza via, anche questa "per sottrazione" come le precedenti: perdere l'illusione di poter controllare le discussioni e invece accettare di affrontarle per quel che si può portare come proprio personale contributo. Anche in questo criterio c'è di fondo il valore del limite: riconoscere ciò che si può realmente fare è di solito riuscire a dare un contributo davvero utile.

La disputa felice

Ne *La disputa felice*¹⁸ è stato delineato un vero e proprio percorso adatto a tutti per riuscire a stare nelle discussioni, qualsiasi discussione, in modo soddisfacente senza perdere tempo e, soprattutto, apportando davvero qualcosa. La strada è quella di lavorare principalmente su sé stessi e i propri limiti:

- limitarsi a intervenire dove si è realmente competenti e si ha esperienza diretta, secondo la massima di Grice della sincerità;
- farlo avvicinando le proprie espressioni, i propri argomenti, i propri ragionamenti all'altro che ascolta e al suo mondo di convinzioni, insomma riconoscere "il mondo" dell'altro;
- rimanere sempre sul tema e tornarci continuamente, chiaramente argomentando, anche quando l'altro offende, provoca, insulta;
- avere la pazienza di spiegare e rispiegare sempre, e avere anche la creatività di cambiare l'ordine dei propri ragionamenti abituali, sovvertendoli, modificandoli e accettando di metterli alla prova di fronte al dissenso altrui;
- coltivare l'autoironia¹⁹ e il distacco da sé stessi e dalle proprie convinzioni cercando sinceramente di imparare sempre qualcosa dal dissenso altrui.

Il tutto con un'idea chiara in mente: non ogni discussione riuscirò, ma il fatto di porsi in ciascuna come un disputatore disposto al collaudo delle proprie idee ha sempre un effetto sociale. Anche se l'interlocutore diretto non ne vorrà sapere e rimarrà nell'ostilità delle sue posizioni contrapposte, ognuna di queste interazioni online avverrà sempre in pubblico e di fronte a un pubblico di altri utenti che assiste. Quella moltitudine silenziosa potrà, dal modo con cui si argomenta, farsi una sua idea sui contendenti e sulle loro argomentazioni, recepire informazioni, conoscere nuovi aspetti, ecc.

¹⁸ Mastroianni B, *La disputa felice*, Cesati, Firenze, 2017.

¹⁹ Mastroianni B, *Ironia online: istruzioni per l'uso*, in <http://www.brunomastro.it/2018/11/ironia-online-istruzioni-per-luso.html>



5

HATE
SPEECH²⁰

²⁰ A cura di Cristiana Andolfi, psicologa.

Definiamo il discorso d'odio

Il termine “Hate speech” (in italiano “discorso di incitamento all’odio”) è stato introdotto dal Consiglio d’Europa nel 1997, con la Raccomandazione No. R (97) 20 del Comitato dei Ministri degli Stati Membri sull’“Hate Speech”, inserito nel 2016 nel Documento “Recommendations and declarations of the Committee of Ministers of the Council of Europe in the field of media and information society”.

La Raccomandazione afferma che per “Hate speech” vanno intese tutte quelle forme di espressione che diffondono, incitano o promuovono l’odio razziale, la xenofobia, l’antisemitismo o altre forme di odio basate sull’intolleranza, inclusa l’intolleranza espressa attraverso forme aggressive di nazionalismo e etnocentrismo, discriminazione e ostilità verso minoranze, migranti o persone di origini straniere.

Oggi, oltre alle minoranze etniche e religiose, sono ritenute a rischio di discriminazione anche donne, anziani, giovani, diversamente abili e persone LGBTI.

Non si tratta di un semplice insulto, ma di una espressione, verbale o scritta, che mira a produrre degli effetti concreti negativi ai danni di un singolo o di gruppo di persone a rischio di discriminazione.

Come nasce un Discorso di incitamento all’odio? Ogni persona, al fine di rendere il mondo prevedibile e controllabile, tende a categorizzare, organizzare e generalizzare le informazioni su di sé e sugli altri. In particolare, vengono definiti stereotipi le impressioni che le persone si formano sui gruppi (in base a razza, genere, età, categorie di ruolo, orientamento sessuale) associandovi particolari caratteristiche o emozioni. Di per sé, lo stereotipo è neutro. Acquisisce un valore positivo o negativo quando gli viene associato un giudizio di valore e, in questo caso, si viene a creare un pregiudizio. Spesso i pregiudizi sono basati su impressioni distorte o approssimative e possono guidare il comportamento verso varie forme di discriminazione.

La discriminazione è il trattamento ingiusto di una persona o gruppo di persone derivante da un pregiudizio negativo. Quando questo comporta una limitazione dei diritti umani, a sua volta, si configura una vera e propria violazione di Diritto.

Gli stereotipi inizialmente vengono appresi dalla famiglia, nei contesti

di apprendimento formale e informale, dagli amici e dai media. I bambini imparano stereotipi e pregiudizi semplicemente osservando e imitando gli adulti significativi nella loro vita. Le loro parole e azioni riflettono le norme sociali di riferimento che indirizzano gli atteggiamenti e i comportamenti di bambini e ragazzi nei confronti di altri gruppi etnici, religiosi o altre categorie di persone.

Con lo sviluppo individuale gli stereotipi possono modificarsi, in base ad esperienze dirette o interazioni con membri del gruppo verso cui si prova un certo pregiudizio, o, ancora, grazie all’apprendimento e alla raccolta di maggiori informazioni incoerenti con lo stereotipo di partenza che possono smentire il pregiudizio.

I nuovi media, in particolare, rappresentano un canale molto potente di stereotipizzazione e diffusione degli stereotipi, sia attraverso le pagine web che attraverso i social media network. I fattori che favoriscono l’uso di un linguaggio aggressivo e discriminatorio sono legati alle caratteristiche della comunicazione mediata dalle nuove tecnologie, ovvero:

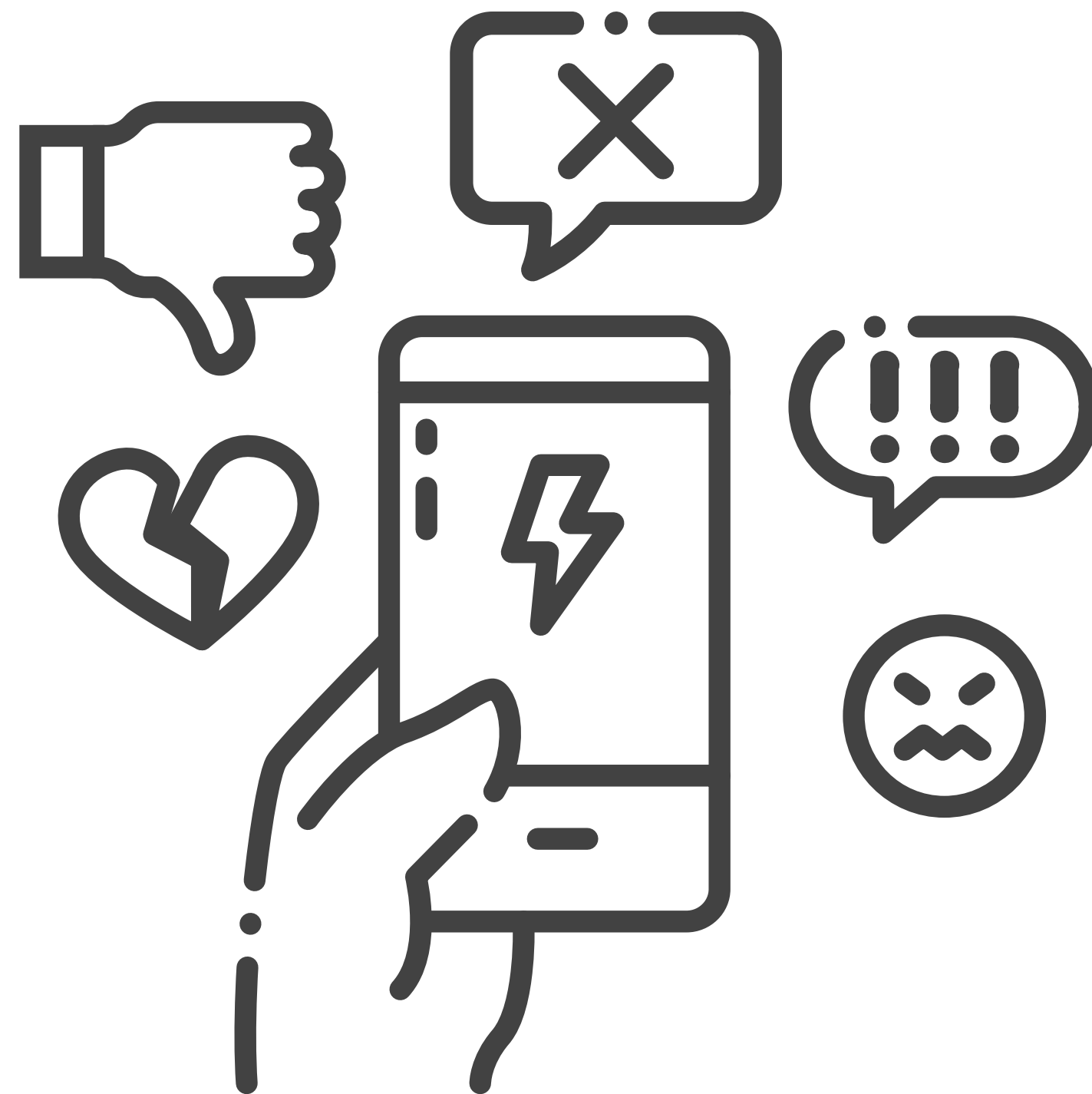
- possibilità di anonimato da parte dell’*hater*;
- indebolimento delle remore etiche per la distanza che si crea tra azioni e loro conseguenze;
- impossibilità di osservare le reazioni emotive provocate dall’azione e quindi impossibilità provare senso di colpa o vergogna, con una conseguente deresponsabilizzazione rispetto al danno apportato;
- minimizzazione della responsabilità personale poiché già altri hanno condiviso informazioni simili.

Contrastare l'hate speech

Le azioni efficaci per il contrasto del fenomeno dell'hate speech, quindi, dovrebbero:

- promuovere e valorizzare l'educazione al rispetto dell'altro, alla tolleranza, all'inclusione e all'uguaglianza, sia in famiglia che a scuola (attraverso specifiche attività scolastiche curricolari ed extracurricolari), ma soprattutto fornendo per primi un modello di adulto significativo dai quali i bambini possano apprendere;
- responsabilizzare i bambini e i ragazzi rispetto alle conseguenze delle loro parole e azioni;
- favorire un uso consapevole e critico delle nuove tecnologie, attraverso una migliore conoscenza del funzionamento di Internet e delle peculiarità della comunicazione attraverso i nuovi media, per far riflettere i ragazzi sulle possibili conseguenze di ciò che pubblicano e/o condividono online;
- promozione dell'educazione civica e ai Diritti Umani.

Per contrastare la diffusione del fenomeno e per sensibilizzare i fruitori della Rete, il Consiglio d'Europa ha istituito il "No hate speech movement" (vedi sitografia), mentre per segnalare un Discorso di incitamento all'odio, in Italia è possibile rivolgersi all'Ufficio Antidiscriminazioni Razziali (UNAR), contattabile telefonicamente attraverso numero verde o attraverso la compilazione di un form online.





6

SICUREZZA E RESPONSABILITÀ²¹

Il cyberbullismo

Secondo la definizione pubblicata sul sito del Ministero dell'Istruzione, Università e Ricerca (MIUR), "il cyberbullismo definisce un insieme di azioni aggressive e intenzionali, di una singola persona o di un gruppo, realizzate mediante strumenti elettronici (sms, mms, foto, video, email, chatt rooms, instant messaging, siti web, telefonate), il cui obiettivo è quello di provocare danni ad un coetaneo incapace di difendersi". Si tratta di una azione prevaricatoria in una relazione caratterizzata da un forte squilibrio di potere, volontaria, ripetuta nel tempo, attraverso uno o più dispositivi elettronici.

Le principali forme in cui si manifesta il cyberbullismo sono:

- Flaming, ovvero l'invio di messaggi violenti e volgari che hanno lo scopo di suscitare tensioni e conflitti verbali tra due o più utenti della rete;
- Harassment (molestie), invio o pubblicazione di messaggi insultanti e offensivi con l'obiettivo di provocare disagio psichico e emotivo;
- Denigration (denigrazione), divulgazione di informazioni false o dispregiative, con lo scopo di danneggiare la reputazione di una persona o le sue amicizie;
- Impersonation (sostituzione di persona), appropriazione dell'identità virtuale di una persona con lo scopo di compiere a suo nome azioni che potrebbero metterla in imbarazzo o procurarle difficoltà relazionali;
- Outing o Trickery (inganno), guadagnarsi la fiducia di una persona per ottenere sue informazioni private e in un secondo tempo pubblicarle online o condividerle con terzi;
- Exclusion (esclusione), esclusione deliberata di una persona da un gruppo online per ferirla;
- Cyberstalking (cyber-persecuzione), persecuzione attraverso messaggi, chiamate o social network verso una persona mirate a incutere paura;
- Happy slapping (schiaffo allegro), diffusione di video che ritraggono una vittima mentre sta subendo violenza fisica o psichica.

Si possono distinguere gli attacchi alla persona, mirati a tormentare l'altro attraverso offese o minacce attraverso sms, messaggi, chat, social network ecc, dagli attacchi alla reputazione, che implicano l'esistenza di un pubblico vasto, compiacente e partecipe alle

umiliazioni.

Il cyberbullismo è un fenomeno favorito dalla possibilità per il molestatore di rimanere anonimo e di sentirsi più disinibito dato che non entra in contatto diretto con la sua vittima. Non necessariamente conosce personalmente la vittima, ma il suo potere all'interno della relazione aumenta in virtù del fatto che può perpetrare più a lungo i suoi comportamenti meschini e condividerli con altri, imporsi pur non essendo fisicamente presente. Le conseguenze per la vittima sono influenzate dal fatto che non esistono, in questo tipo di prepotenze, confini spazio-temporali e i contenuti condivisi hanno un pubblico potenzialmente infinito; inoltre, difficilmente il materiale o i messaggi condivisi possono essere cancellati definitivamente dalla rete, influenzando la vita della vittima anche a distanza di anni.

Gli interventi che si sono rivelati più efficaci prevedono un coinvolgimento diretto di famiglie, istituzioni, agenzie educative e il loro personale. La sfida per gli adulti è quella di informare e informarsi sulla veloce evoluzione del fenomeno e sulle varie forme di comunicazione e i potenziali rischi del web, ma soprattutto dare il buon esempio, favorendo lo sviluppo di competenze relazionali positive, autostima e assertività nel singolo e sostenendo l'ascolto, il confronto e il dialogo a livello di gruppo.

L'adozione di politiche scolastiche chiare e condivise sui fenomeni del bullismo e cyberbullismo favorisce il coinvolgimento degli alunni, delle famiglie e del personale scolastico, garantendo un tempestivo intervento qualora si presentassero situazioni a rischio. Infatti, a seguito dell'emanazione della legge n. 71 del 29 maggio 2017, le scuole sono obbligate a intervenire tempestivamente in presenza di un episodio di cyberbullismo, convocare le famiglie e, in caso fosse necessario, rivolgersi alle autorità competenti.

È importante ricordare che bullo e vittima sono ruoli che chiunque potrebbe rivestire. Fermo restando che è indispensabile tutelare chi subisce le prepotenze e punire chi le mette in atto, entrambi presentano importanti fragilità personali e, per questo, sarà importante comprendere accuratamente le dinamiche dei fatti, le relazioni preesistenti tra i protagonisti, ascoltare la vittima per comprendere l'impatto psico-emotivo dell'accaduto sulla sua vita e capire quali siano state le motivazioni del bullo/i.



7

RESPONSABILITÀ: CIVILI E PENALI²²

Cos'è la "responsabilità"?

È la possibilità di prevedere le conseguenze del proprio comportamento e correggerlo sapendo a cosa possiamo andare incontro. Si parla di responsabilità giuridica quando la nostra libertà di azione è limitata da una legge che ci impone un dovere, che può consistere nell'obbligo di tenere un certo comportamento (allacciarsi le cinture di sicurezza in macchina) o di tenere un determinato comportamento (non guidare in stato di ebbrezza). Se ci comportiamo contrariamente a quella norma, si compie un «illecito» che comporta una sanzione.

Illeciti civili e penali

L'illecito può essere civile o penale a seconda che si violi una legge di tipo civile o, invece, una legge penale. Le leggi civili regolano i rapporti tra privati (famiglia, lavoro, commercio, contratti, ecc.). Quando si commette un illecito civile, se si provoca un danno a qualcuno, la «punizione» prevista è il risarcimento del danno subito dal soggetto danneggiato.

La legge penale, invece, individua tutte quelle condotte che, per la loro gravità, sono considerate reati (furto, omicidio, rapina, stalking, ecc.). Per i reati la sanzione («punizione») è anche il carcere. Il risarcimento del danno può essere applicato anche nei casi di reati penali.

Il secondo comma dell'articolo 185 codice penale stabilisce che: "Ogni reato, che abbia cagionato un danno patrimoniale o non patrimoniale, obbliga al risarcimento il colpevole...". Per danno patrimoniale si intende quindi un danno economico: se mi hanno rubato l'auto, il danno patrimoniale consiste nella perdita dell'auto. Per danno non patrimoniale si intende il patimento morale che ne deriva: se hanno divulgato senza il mio consenso un video che mi ritrae nuda, subisco un danno morale e un danno all'immagine.

In relazione alla norma violata (civile o penale), si avranno, quindi, altrettanti tipi di responsabilità: responsabilità civile e responsabilità penale.

La responsabilità civile

Nel caso di illecito civile, chi provoca un danno ingiusto alla persona o alle cose che gli appartengono deve risarcire economicamente il danno subito dal soggetto danneggiato.

Il danno risarcibile a chi lo subisce può essere: danno morale (subire sofferenze morali), danno biologico (danno riguardante la salute, l'integrità fisica e psichica della persona, es. se in un incidente stradale mi sono rotta un braccio), danno esistenziale (danno alla persona, alla sua esistenza, alla qualità della vita, alla vita di relazione...), danno materiale (es. il vetro rotto... ecc.).

Cosa succede se un minore viola una delle norme che vietano certi comportamenti e provoca un danno a qualcuno? Chi se ne assume la responsabilità?

Secondo il codice civile, a rispondere degli illeciti civili compiuti dai minori sono i genitori ed eventualmente la scuola (per gli illeciti compiuti nell'orario scolastico). Per cui, solo al compimento dei 18 anni si diventa responsabili civilmente degli illeciti civili commessi e si è tenuti personalmente a provvedere al risarcimento del danno. Il danno provocato da chi ha compiuto i 18 anni verrà risarcito economicamente da chi lo ha commesso, non dai genitori.

La responsabilità penale

L'art. 27 comma 1 della Costituzione stabilisce che per la commissione di un reato è responsabile solo colui che ha commesso personalmente il fatto contrario alla legge penale. Per cui, se un minore commette un reato ne risponde solo lui/lei penalmente, non i suoi genitori. Secondo il codice penale nessuno può essere punito per un reato se, al momento in cui lo ha commesso, non aveva compiuto i 14 anni di età. Quindi il minore che ha compiuto i quattordici anni è responsabile penalmente se le proprie azioni costituiscono un reato. Non ne sono responsabili i genitori o gli insegnanti.

Gli illeciti digitali

Cyberbullismo (legge 71/2017): “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”. La maggior parte delle condotte descritte nella legge costituiscono un reato punibile dal codice penale.

Non tutte le forme di cyberbullismo costituiscono un «reato», per esempio, l'esclusione, classica forma di cyberbullismo o di bullismo che si manifesta escludendo il bullizzato dal gruppo, non è un reato. Costituisce comunque un illecito civile perché provoca un danno ingiusto al soggetto bullizzato che, per effetto dell'esclusione, subisce un danno psicologico per il quale potrebbe richiedere il danno morale o esistenziale)

Sostituzione di persona, furto di identità commette il reato chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici.

Esempio: creo un profilo falso su un social network ad una persona. Oppure accedo alla casella di posta elettronica di una persona e inizio ad inviare mail denigranti ad alcune persone, spacciandomi per quella persona.

La diffamazione, commette il reato chiunque, comunicando con più persone, offende l'altrui reputazione, chiunque offende attribuendo un fatto determinato. Se l'offesa è recata col mezzo della stampa o con qualsiasi altro mezzo di pubblicità, ovvero in atto pubblico, la pena è della reclusione da sei mesi a tre anni o della multa non inferiore a 516 euro. Esempio: su un social network o su una chat offendo una persona o le attribuisco alcuni fatti offensivi (ipotesi: dico che è un raccomandato).

Pornografia minorile, commette il reato chiunque utilizzando minori di anni diciotto, realizza esibizioni o spettacoli pornografici, ovvero produce materiale pornografico, recluta o induce minori di anni diciotto a partecipare a esibizioni o spettacoli pornografici ovvero dai suddetti spettacoli trae altrimenti profitto, faccia commercio del materiale pornografico di cui al primo comma, con qualsiasi mezzo, anche per via telematica, distribuisce, divulga, diffonde o pubblicizza il materiale pornografico di cui al primo comma, ovvero distribuisce o divulga notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto.

Viene definito materiale pornografico quello che ritrae o rappresenta visivamente un soggetto minore di diciotto anni implicato o coinvolto in una condotta sessualmente esplicita.

Atti persecutori (stalking) commette il reato chiunque, con condotte reiterate, minaccia o molesta taluno in modo da cagionare un perdurante e grave stato di ansia o di paura ovvero da ingenerare un fondato timore per l'incolumità propria o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva ovvero da costringere lo stesso ad alterare le proprie abitudini di vita.

Esempio: una ragazzina viene perseguitata dall'ex con continui ed insidiosi messaggi che le mettono paura al punto di generare stati di ansia e paura, che possono arrivare a compromettere la sua quotidianità.

Revenge porn, commette il reato chiunque, dopo averli realizzati o sottratti, invia, consegna, cede, pubblica o diffonde immagini o video di organi sessuali o a contenuto sessualmente esplicito, destinati a rimanere privati, senza il consenso delle persone rappresentate, chi avendo ricevuto o comunque acquisito le immagini o i video li invia, consegna, cede, pubblica o diffonde senza il consenso delle persone rappresentate al fine di recare loro nocimento. La pena è aumentata se i fatti sono commessi dal coniuge, anche separato o divorziato, o da persona che è o è stata legata da relazione affettiva alla persona offesa ovvero se i fatti sono commessi attraverso strumenti informatici o telematici o se i fatti sono commessi in danno di persona in condizione di inferiorità fisica o psichica o in danno di una donna in stato di gravidanza.

Interferenze illecite nella vita privata, commette il reato chiunque, mediante l'uso di strumenti di ripresa visiva o sonora si procura indebitamente notizie o immagini attinenti alla vita privata svolgentesi nei luoghi indicati nell'articolo 614 (abitazione, privata dimora), chi rivela o diffonde, mediante qualsiasi mezzo di informazione al pubblico, le notizie o le immagini ottenute nei modi indicati nella prima parte di questo articolo.

Accesso abusivo a sistema informatico commette il reato chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

Violazione, sottrazione e soppressione di corrispondenza commette il reato chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne da altri prender cognizione,

una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, chi rivela, in tutto o in parte, il contenuto della corrispondenza, è punito, se dal fatto deriva un documento ed il fatto medesimo non costituisce un più grave reato.

Prendere precauzioni sui social

Art. 10 Codice civile

Qualora l'immagine di una persona o dei genitori, del coniuge o dei figli sia stata esposta o pubblicata fuori dei casi in cui l'esposizione o la pubblicazione è dalla legge consentita, ovvero con pregiudizio al decoro o alla reputazione della persona stessa o dei detti congiunti, l'autorità giudiziaria, su richiesta dell'interessato, può disporre che cessi l'abuso, salvo il risarcimento dei danni.

La legge sul diritto d'autore prevede che "il ritratto di una persona non può essere esposto, riprodotto e messo in commercio senza il consenso di questa...", salvo che si tratti di persone famose. Il volto di una persona ritratto in una fotografia è considerato dato personale. Il codice della privacy, infatti, sanziona con l'obbligo del risarcimento del danno l'eventuale violazione dell'altrui diritto alla riservatezza.

Possiamo pubblicare qualunque immagine o foto di cui siamo in possesso, ma nel momento in cui vi sono altre persone: avvisiamole della nostra volontà di pubblicazione, richiediamo sempre un consenso, meglio se via e-mail o comunque scritto, provvediamo all'immediata rimozione se ci viene richiesta. Inoltre è sempre meglio evitare di pubblicare foto di minori anche se sono i nostri figli.

Il diritto all'oblio non esiste. La rete non garantisce il c.d. diritto all'oblio: ciò che circola in rete non si può mai più cancellare. È permanente, indelebile e chiunque un domani potrà vederlo. Prima di postare qualsiasi foto, video, commento, ricordiamoci che ciò che pubblichiamo non si cancella mai. Si può eliminare dal nostro profilo del social network ma non dalla rete. Pensiamo, prima di postare, se oggi ci conviene apparire, o se è meglio tutelare la nostra privacy, il nostro futuro.

Se facciamo circolare foto o video compromettenti di un compagno, senza il suo consenso, quella foto e quel video non verranno mai cancellati dalla rete, e il compagno vittima di cyberbullismo potrebbe addirittura avere difficoltà un domani nel trovare un posto di lavoro, con un evidente danno economico. Di conseguenza il risarcimento economico cui sono tenuti i soggetti responsabili civilmente (genitori) può essere veramente elevato.

Il sexting è l'invio in confidenza al fidanzato/a amico/a di fotografie

a sfondo sessuale via smartphone o altri dispositivi attraverso l'utilizzo della rete Internet, se queste immagini, ottenute tramite la confidenza tra due persone, vengono divulgate illegittimamente in rete, si tratta di cyberbullismo.

Strumenti di tutela

L'art. 2 della legge 71/2017 sul cyberbullismo prevede che il minore da quattordici ai diciotto anni che abbia subito un atto di cyberbullismo, o il suo genitore, possano inoltrare un'istanza per l'oscuramento, la rimozione o il blocco di qualsiasi dato personale del minore, diffuso nella rete. L'istanza di oscuramento va inoltrata al gestore del sito internet o del social media. Se entro ventiquattro ore dal ricevimento dell'istanza i soggetti responsabili non hanno comunicato di avere preso in carico la segnalazione, ed entro quarantotto ore provveduto, l'interessato può rivolgere analoga richiesta, mediante segnalazione o reclamo, al Garante per la privacy, il quale provvede entro quarantotto ore dal ricevimento della richiesta.

L'ammonimento

Nel caso in cui non si ravvisino reati perseguibili d'ufficio o non sia stata formalizzata querela o presentata denuncia, è possibile rivolgere al Questore un'istanza di ammonimento nei confronti del minore ultraquattordicenne autore della condotta molesta. La richiesta potrà essere presentata presso qualsiasi ufficio di Polizia e dovrà contenere una dettagliata descrizione dei fatti, delle persone coinvolte ed eventuali allegati comprovanti quanto esposto. Qualora l'istanza sia considerata fondata, anche a seguito degli approfondimenti investigativi, il Questore convocherà il minore responsabile insieme ad almeno un genitore, ammonendolo oralmente e invitandolo a tenere una condotta conforme alla legge. La legge non prevede un termine di durata massima dell'ammonimento ma specifica che i relativi effetti cesseranno al compimento della maggiore età.





8

ACQUISTARE
ONLINE
IN SICUREZZA²³

Bambini consumatori

I bambini vengono educati agli acquisti, ossia ad essere consumatori, principalmente da:

- il carrello del supermercato;
- la tv
- il web

Il carrello del supermercato è dotato di un apposito seggiolino per i più piccoli, lo scopo non è solo agevolare la spesa dei genitori, ma indurre il bambino a mettere nel carrello giocattoli e caramelle che, non casualmente, sono alla sua portata di mano.

La tv, in particolare con l'avvento del digitale terrestre, contribuisce ad alimentare i desideri di acquisto dei bambini attraverso intense campagne pubblicitarie a loro dedicate. Da considerare che i canali gratuiti che trasmettono H24 programmi per bambini sono 8 e solo 1 (RAI Yoyo dedicato ai più piccoli), non contiene messaggi pubblicitari.

Il web, ultimo in ordine di arrivo, fa sintesi dei due precedenti: il bambino non solo viene bombardato da messaggi pubblicitari ma può acquistare direttamente online. Acquisti che sono richiesti dai giochi di ultima generazione e agevolati da forme di pagamento sempre più semplici (carta prepagata, PayPal, credito telefonico, ecc).

Da una indagine informale durante un corso di educazione finanziaria in una scuola secondaria di primo grado è risultato che circa il 30% dei bambini di 11 anni ha dichiarato di fare acquisti online affermando di aver speso, in alcuni casi, più di 1000 euro.

Il problema è la perdita della percezione del valore del denaro da parte dei bambini, portati quindi ad acquistare compulsivamente.

Come educare all'acquisto?

La pubblicità è ritenuta giuridicamente "*dolus bonus*" ossia "dolo consentito". In sostanza la pubblicità è un inganno, normalmente tollerato negli affari, perché sostanzialmente innocuo. Si tratta di bonaria "millantazione" della merce, e si considera che ogni persona di media avvedutezza possa valutare il messaggio pubblicitario con circospezione e fare una scelta consapevole, per questo il la pubblicità non perfettamente veritiera non è generalmente causa di annullamento dell'acquisto.

Ma leggere con circospezione, con senso critico, il messaggio

promozionale di un prodotto richiede la conoscenza delle regole che vengono seguite dai pubblicitari per indurre all'acquisto, regole di cui di seguito facciamo una breve sintesi.

Regole base della pubblicità

La pubblicità ha tre regole:

- Informare - ossia far conoscere il prodotto
- Persuadere - convincere all'acquisto
- Ricordare - perché il prodotto, se di consumo, deve essere acquistato abitualmente (questo succede, per esempio, quando vediamo nei supermercati delle persone che offrono assaggi di prodotti molto conosciuti, come la Nutella, l'obiettivo non è far conoscere il prodotto ma invitare all'acquisto: "qui e ora").

Far conoscere il prodotto è importante, non si comprende ciò di cui si ignora l'esistenza che sia un prodotto o un marchio. Affinché tutti possano conoscere un prodotto la pubblicità si affida alla maggior parte dei canali possibili: tv, radio, giornali, internet. La Crossmedialità, ossia possibilità di mettere in connessione i mezzi di comunicazione l'uno con l'altro, grazie allo sviluppo e alla diffusione di piattaforme digitali, è uno dei sistemi utilizzati in pubblicità non solo per far conoscere il prodotto, ma anche per renderlo appetibile. L'importanza di un prodotto inconsciamente si valuta infatti anche sulla base della sua esposizione mediatica. Se lo stesso prodotto lo trovo nei giornali, in tv e sui social sono indotto a ritenere che abbia una grande reputazione e quindi sia da tenere in considerazione.

In pratica se vedo l'immagine del prodotto ovunque sono già predisposto all'acquisto, ma non basta: devo essere convinto, persuaso. Per questo devo essere condizionato, manipolato.

La persuasione

Persuadere significa convincere per raggiungere i propri scopi. È l'anima della pubblicità. Si tratta di tecniche molto efficaci e convincenti che inducono il consumatore ad acquistare anche prodotti di cui un momento prima non ne sentiva la necessità o il desiderio.

Tecniche che si basano sulla conoscenza dei meccanismi mentali che ci inducono a fare le scelte.

Noi pensiamo che le nostre decisioni siano razionali. In realtà dobbiamo fare i conti con le nostre emozioni, e con le semplificazioni che la nostra mente fa di continuo. Semplificazioni che ci aiutano a fare un sacco di cose contemporaneamente del tipo: parlare e camminare, che può sembrare semplice ma sono fra le cose più complicate che abbiamo imparato nella nostra vita. Ci vengono automaticamente, come, per chi guida, mettere il piede sul freno quando il semaforo è rosso.

Il nostro cervello usa preferibilmente scorciatoie, e non il ragionamento, quando deve fare scelte.

Immaginiamo di essere arrabbiati con qualcuno ed abbiamo il cellulare in mano con un social aperto. Automaticamente siamo indotti ad offendere, a dare sfogo alle nostre emozioni. Non attiviamo il nostro pensiero razionale che ci induce a capire le conseguenze di ciò che facciamo.

La stessa cosa avviene negli acquisti. Se l'offerta ha uno sconto del 50% + un ulteriore 40% e scade proprio nel fine settimana sarò indotto all'acquisto. La prima semplificazione è che 50+40 fa 90 e poi esiste un tempo limitato. Se usiamo il pensiero razionale calcoliamo prima il 50% poi il 40% sul rimanente e vediamo che lo sconto è del 70%, ma questo sconto va calcolato su un prezzo che probabilmente è più alto di quello reale, perché la pubblicità ci ha bloccato su un valore "ancora" sulla base del quale deve partire la nostra scelta.

Daniel Kahneman in "Pensieri lenti e veloci"²⁴, definisce il nostro pensiero intuitivo (pensiero veloce): primitivo, inconsapevole e automatico. È sempre in allerta, non lo controlliamo, ed è emozionale, veloce e impulsivo. Può svolgere più compiti nel medesimo tempo,

²⁴ Kahneman D., *Pensieri lenti e veloci*, Mondadori, Milano, 2013.

non causa affaticamento, dà immediatamente senso a qualsiasi cosa che ci viene proposta, ma viene influenzato molto e molto facilmente.

Il pensiero razionale (pensiero lento) invece è metodico e cauto, occupa tutta la nostra mente impedendo di fare contemporaneamente altri ragionamenti razionali e, spesso, si lascia sopraffare dal pensiero intuitivo soprattutto quando ci sono delle emozioni forti di mezzo, o quando è messo sotto pressione. Poi, diciamo pure, siamo sempre pigri e indotti ad utilizzare l'istinto piuttosto che affrontare un faticoso ragionamento.

Tutto ciò è perfettamente conosciuto da chi si occupa di pubblicità.

Ed ecco che le armi della persuasione entrano in campo, e qui merita citare un altro studioso che ha classificato le tecniche più utilizzate per convincerci: Robert Cialdini.

Ecco le armi che lui ritiene vincenti:

La reciprocità. Si verifica quando si fa un omaggio a qualcuno, e l'altro si sente in dovere di ricambiare in qualche modo ciò che ha ricevuto. Contraccambiare è una regola sociale che istintivamente ci sentiamo di rispettare per non essere tacciati di ingratitudine. In virtù di questa regola siamo obbligati a ripagare favori, regali, inviti. Una tecnica di persuasione che sfrutta questo principio è quella dei campioni gratuiti, si fornisce ai clienti una piccola quantità di prodotto con l'"innocente" intenzione di informare il pubblico, mentre ciò mette in moto l'obbligo di ricambiare il dono con l'acquisto.

L'impegno e la coerenza. Chi non è coerente delle scelte fatte rischia di essere etichettato come inaffidabile o superficiale. Una tattica persuasiva che sfrutta questo principio è la tecnica del "piede nella porta" che consiste nell'ottenere acquisti cominciando con un piccolo impegno. Questo viene fatto, per esempio, dalle associazioni benefiche che, prima di chiedere soldi per la propria raccolta fondi, richiedono un piccolo impegno, ovvero una firma contro o a favore di qualcosa. Il "Mi piace" è una prima forma di Impegno (piccolo) verso una azienda sui social. L'utente è molto più disposto a comprare (impegno più grande) da un marchio "che conosce" quindi che ha già espresso un "Mi piace" rispetto ad uno che non ha mai sentito.

Dopo una presa di posizione o una scelta iniziale siamo portati istintivamente a difenderla per essere coerenti con l'impegno preso.

La riprova sociale. Secondo questo principio uno dei mezzi che usiamo per decidere che cos'è giusto è cercare di scoprire che cosa gli altri considerano giusto. Soprattutto in situazioni ambigue, in cui siamo dubbiosi su come agire, è più facile che guardiamo al comportamento altrui e lo prendiamo per buono. Come quando nello scegliere fra due negozi vicini siamo portati ad entrare in quello dove c'è più gente

Un esempio di come agisce la "riprova sociale" possiamo vederlo nella scelta degli indumenti da parte degli adolescenti. I brand scelti sono spesso quelli che sono apprezzati dalla maggior parte dei coetanei, questo risponde al desiderio di avere una grande "riprova sociale" da parte dei ragazzi.

La simpatia. Da alcune ricerche di psicologia sociale risulta che si tende ad attribuire automaticamente alle persone di bell'aspetto altre caratteristiche positive come talento, gentilezza, onestà e intelligenza. Inoltre se la persona è familiare, simile a noi o di nota

fama il prodotto risulta più appetibile. Nella pubblicità questo è molto comune, i testimonial spesso sono persone conosciute oppure al limite hanno difetti in cui ci riconosciamo, comunque ci ispirano simpatia.

L'autorità. Le affermazioni di persone autorevoli sono convincenti. Una medicina indicata dal dottore non si discute e non si cerca neanche un farmaco equivalente. Questo perché abbiamo un naturale e radicato senso di obbedienza che ci è insegnato fin dalla nascita. Quindi, riconosciuta l'autorevolezza del soggetto, si eseguono le azioni senza discuterle. Un aneddoto interessante: un medico aveva ordinato di somministrare delle gocce nell'orecchio destro di un paziente che soffriva di otite, ma aveva abbreviato la prescrizione scrivendo invece di "right ear" "Rear"; l'infermiera del reparto leggendo "place in rear" (mettere di dietro), somministrò il numero prescritto di gocce per via rettale. Sia l'infermiera che il paziente sapevano benissimo che non si cura così l'infezione dell'orecchio, ma nessuno dei due pensò di mettere in dubbio l'autorevolezza del medico.

La scarsità. La tecnica si basa sul fatto che ci appaiono più desiderabili prodotti quando la loro disponibilità è limitata o quando abbiamo pochissimo tempo a disposizione per acquistarli.

I venditori conoscono bene questa tecnica di persuasione e spesso creano delle offerte valide solo per pochi giorni, oppure sfruttano il principio dell'edizione limitata.

Tutti conoscono le offerte di una nota marca di divani che finiscono rigorosamente il fine settimana, o skins di noti videogiochi vendute in edizione limitata.

Regole per acquisti online

Essere capaci di scegliere senza cadere nelle trappole della persuasione non basta, ma aiuta a fare scelte consapevoli, e magari sostenibili economicamente (non spendere più del necessario) socialmente (fare acquisti di prodotti che rispettano chi lavora), ma anche nel rispetto dell'ambiente (prodotti a basso impatto, riciclabili, evitare acquisti inutili o di aziende che inquinano).

Inevitabilmente, fatta la scelta si passa all'acquisto "online" e, a questo punto, non dobbiamo mai dimenticarci delle regole da seguire:

- essere informati sull'affidabilità del rivenditore, magari attraverso recensioni su appositi portali;
- leggere sempre e con attenzione le condizioni generali di vendita e contratto e non acquistare mai con troppa fretta;
- verificare completezza e trasparenza delle informazioni sul negozio online dove acquistare, ad esempio accertandosi che ci siano tutti i dettagli del negozio (modalità di pagamento, recesso, contatti, pec per reclami,...);
- accertarsi di fare transazioni solo su siti con connessione protetta (https)
- verificare sempre la descrizione di un prodotto e fare attenzione a offerte super convenienti, sono solitamente campanelli di allarme;
- attenzione anche alle richieste di pagamenti online anticipati;
- stampare e conservare con cura la documentazione di acquisto.

Infine: ricordarsi che per legge esiste il diritto di recesso (o ripensamento) per gli acquisti online, questo significa che entro 14 giorni il prodotto può essere sempre restituito (naturalmente integro). I 14 giorni decorrono:

- per beni materiali, dal giorno in cui il consumatore ne entra in possesso;
- i contratti di servizi, dal momento della conclusione (sottoscrizione) del contratto (art. 49 del Codice del Consumo).

Il gioco d'azzardo

Il gioco d'azzardo si sta diffondendo online anche grazie alla pubblicità molto invasiva sui social.

È bene sapere che i giochi basati sulla "fortuna" in realtà sono progettati e realizzati sulla base di precise regole matematiche. La fortuna è quindi un elemento eccezionale che può premiare solo chi gioca occasionalmente. Il giocatore abitudinario perde infatti ad un ritmo stabilito dall'algoritmo del gioco. Il giocatore abitudinario inoltre rischia di diventare patologico. Il gioco diviene una vera e propria malattia, una dipendenza da curare alla stregua del fumo, dell'alcol e della droga.

Conoscere le regole può servire per starne lontano, o, almeno, a considerarlo per quello che dovrebbe essere: un gioco occasionale. Perché la fortuna è cieca ma la matematica no.



9

CARTE DI CREDITO E BANCOMAT: PERICOLI E PRECAUZIONI²⁵

Pagare on line con carta: possibili rischi

Il recente, esponenziale incremento dell'utilizzo dei mezzi di pagamento elettronico (bancomat e carte di credito/debito) ha richiamato l'attenzione delle organizzazioni criminali sia in relazione alla semplicità delle tecniche utilizzate sia in relazione ai notevoli profitti che tali attività consentono.

I malviventi attraverso gli skimmers - di dimensioni tali da poter essere occultati con facilità negli sportelli ATM - immagazzinano, all'interno di una memoria a prom, i dati acquisiti dalle carte di pagamento dall'ignaro utente. Contestualmente, tramite una microcamera nascosta o una tastiera sovrapposta, rilevano il PIN digitato.

I dati così acquisiti consentiranno di creare carte clonate in grado di essere utilizzate per prelievi e transazioni illecite.

Consigli

Di seguito sono indicati alcune elementari cautele da adottare al fine di prevenire la possibilità di clonazione:

- Controllare, quando la carta di credito viene recapitata, che il plico sia integro; che rechi l'intestazione della vostra banca o di chi emette la carta o della società incaricata all'invio;
- Attivare, ove possibile, il servizio ALERT via SMS al fine di poter essere informati in tempo reale delle spese effettuate sia con il bancomat che con la carta di credito;
- Non cedere mai la carta ad altre persone;
- In caso di pagamento presso esercenti non perdere mai di vista la carta per la durata dell'intera operazione;
- Quando si effettua un accesso presso gli sportelli bancomat, è opportuno verificare sempre la fessura dove viene inserita la carta. Lì, solitamente, viene nascosto lo "skimmer". Una tastiera numerica, del tutto simile all'originale, può essere sovrapposta per acquisire il codice PIN. Quest'ultimo può essere sottratto anche attraverso micro telecamere occultate in punti strategici del Bancomat.
- Non conservare MAI il PIN insieme al supporto magnetico.
- In caso di smarrimento o furto della carta bloccarla immediatamente e sporgere denuncia presso il più vicino Ufficio di Polizia.

eCommerce e dintorni

E-commerce che cos'è?

Il commercio elettronico è sicuramente il servizio con le maggiori prospettive di crescita tra quelli messi a disposizione su Internet. Tale fenomeno porterà a rivoluzionare le dinamiche economiche sia dal punto di vista delle imprese (a qualunque ramo appartengano) che dal lato del consumatore. Le reti, tradizionalmente utilizzate come mero veicolo per la trasmissione dei dati, diventano oggi un mercato globale nel quale è possibile scambiare ogni tipo di bene e servizio. Oltre alla possibilità di acquistare beni direttamente fruibili on line (servizi informativi, software, dischi, libri) la Rete offre beni che vengono solo ordinati elettronicamente e necessitano, quindi, di un'attività di consegna successiva tramite i canali tradizionali.

Il commercio elettronico rappresenta una nuova opportunità di business offerta agli utenti (produttori, commercianti, consumatori e banche) per ridurre i costi, migliorare la qualità dei prodotti e dei servizi, nonché per ridurre i tempi di consegna.

Agli indubbi vantaggi che il commercio elettronico porta alle imprese ed ai consumatori, si accompagnano, tuttavia, nuove sfide e nuovi rischi per chi compra e per chi vende, dovuti anche alle dimensioni globali del fenomeno. C'è la necessità di creare fiducia e confidenza tra le parti in gioco, soprattutto per quanto riguarda l'identità dei soggetti, l'individuazione della sede del fornitore, l'integrità e la sicurezza dei messaggi scambiati, la protezione dei dati personali, la validità e l'efficacia del contratto stipulato per via telematica o informatica, la sicurezza nei pagamenti.

Consigli pratici per evitare di cadere in truffe

Porre attenzione al “feedback” assegnato al venditore. È preferibile che sia alto.

In caso di primo acquisto, soprattutto su siti non conosciuti o su negozi online di recente costituzione valutare la possibilità di pagamento con modalità di contrassegno.

Utilizzare il servizio di deposito a garanzia che permette all’acquirente di pagare una società che svolge il trasporto e, solo dopo l’avvenuta ricezione dell’oggetto, di autorizzare il pagamento al mittente.

Il bonifico bancario è molto sicuro poiché si ha traccia di tutta la transazione. È necessario però recarsi presso la propria banca o ottenere un conto corrente online ed effettuare lo stesso tramite Internet.

Chiedere al venditore più dati possibili così da avere una ragionevole certezza della identità della persona.

Verificare tramite motore di ricerca, l'esistenza di segnalazioni da parte di altri utenti riguardanti il venditore/acquirente.

Diffidare di prodotti venduti a prezzi estremamente vantaggiosi.

È sempre consigliato acquistare e vendere nel territorio italiano in quanto la tutela legale è completa.

Preferire l’utilizzo di carte prepagate che possono essere ricaricate in anticipo con la quantità di denaro da utilizzare.

Dubitare di venditori che non forniscono utenze di telefoni fissi.

Dubitare di chi fornisce indirizzi ubicati presso caselle postali.

Evitare di fornire ove possibile dati personali e diffidare da richieste di ulteriori dati oltre quelli già forniti.

Il phishing

Il phishing è una particolare tipologia di truffa realizzata sulla rete Internet attraverso l’inganno degli utenti. Si concretizza principalmente attraverso messaggi di posta elettronica ingannevoli: Attraverso una e-mail, solo apparentemente proveniente da istituti finanziari (banche o società emittenti di carte di credito) o da siti web che richiedono l’accesso previa registrazione (web-mail, e-commerce ecc.). Il messaggio invita, riferendo problemi di registrazione o di altra natura, a fornire i propri riservati dati di accesso al servizio. Solitamente nel messaggio, per rassicurare falsamente l’utente, è indicato un collegamento (link) che rimanda solo apparentemente al sito web dell’istituto di credito o del servizio a cui si è registrati. In realtà il sito a cui ci si collega è stato artatamente allestito identico a quello originale. Qualora l’utente inserisca i propri dati riservati, questi saranno nella disponibilità dei criminali.

Con la stessa finalità di carpire dati di accesso a servizi finanziari online o altri che richiedono una registrazione, un pericolo più subdolo arriva dall’utilizzo dei virus informatici. Le modalità di infezione sono diverse. La più diffusa è sempre il classico allegato al messaggio di posta elettronica; oltre i file con estensione .exe, i virus si diffondono celati da false fatture, contravvenzioni, avvisi di consegna pacchi, che giungono in formato .doc .pdf. Nel caso si tratti di un c.d. “financial malware” o di un “trojan banking”, il virus si attiverà per carpire dati finanziari. Altri tipi di virus si attivano allorché sulla tastiera vengono inseriti “userid e password”, c.d. “keylogging”, in questo caso i criminali sono in possesso delle chiavi di accesso ai vostri account di posta elettronica o di e-commerce.

Come proteggersi da queste tipologie di raggio

- Gli Istituti di Credito o le Società che emettono Carte di Credito non chiedono mai la conferma di dati personali tramite e-mail ma contattano i propri clienti direttamente per tutte le operazioni riservate. Diffidate delle e-mail che, tramite un link in esse contenute, rimandano ad un sito web ove confermare i propri dati.
- Nel caso riceviate una e-mail, presumibilmente da parte della vostra banca, che vi fa richiesta dei riservati dati personali, recatevi personalmente presso il vostro istituto di credito.
- Se credete che l' e-mail di richiesta informazione sia autentica, diffidate comunque del link presente in questa, collegatevi al sito della banca che l'ha inviata digitando l' indirizzo internet, a voi noto, direttamente nel browser.
- Verificate sempre che nei siti web dove bisogna immettere dati (account, password, numero di carta di credito, altri dati personali), la trasmissione degli stessi avvenga con protocollo cifrato.
- Controllate, durante la navigazione in Internet, che l' indirizzo URL sia quello del sito che si vuole visitare, e non un sito "copia", creato per carpire dati.
- Installate sul vostro computer un filtro anti-spam.
- Controllate che, posizionando il puntatore del mouse sul link presente nell' e-mail, in basso a sinistra del monitor del computer, appaia l' indirizzo Internet del sito indicato, e non uno diverso.

