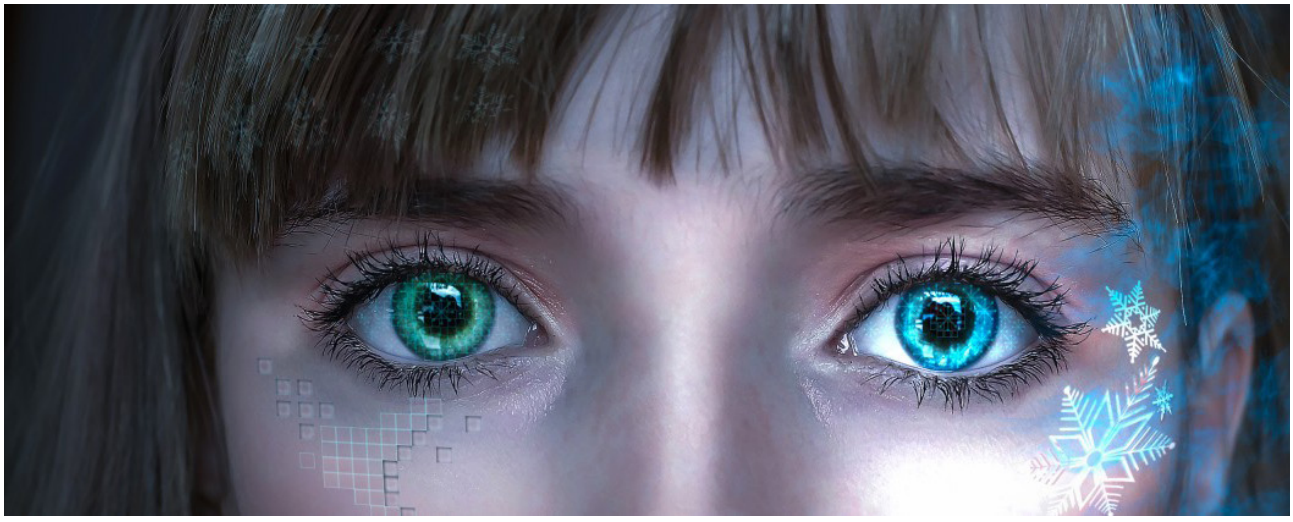
Giovanni Ziccardi
Cittadinanza digitale

Giovanni Ziccardi insegna Informatica giuridica all'Università di Milano, e ha scritto questo capitolo dedicato alla Cittadinanza digitale per il manuale scolastico «Cuori intelligenti. Mille anni di letteratura», curato da Claudio Giunta per Garzanti Scuola, nel fascicolo «1, 2, 3… Maturità. Percorsi di cittadinanza» (nel manuale i capitoli sono corredati da esercizi: qui ne diamo una versione leggermente ridotta).

I
Il cittadino digitale



Cosa significa, oggi, essere un buon cittadino digitale? Significa tante cose, tutte egualmente importanti sia per un uso responsabile delle tecnologie che ormai ci circondano in ogni momento, sia per relazionarsi con gli altri utenti digitali in maniera corretta.
Il cittadino digitale è quello che vive nella società digitale, ossia in una società che accanto alle relazioni "fisiche" tra le persone vede anche delle relazioni digitali, generate da impulsi, da messaggi, da giochi, da servizi, da app e da piattaforme.
Nella società digitale bisogna comportarsi con correttezza esattamente come avviene

nella società "fisica". Un buon cittadino digitale è quindi, prima di tutto, un cittadino che rispetta la legalità, l'affettività e l'empatia[1] nella società "tradizionale" e tiene gli stessi comportamenti anche durante la sua attività online.
Il giurista Stefano Rodotà[2] è stato tra i primi studiosi in Italia a delineare la vita delle persone nella società digitale, sin dai primi collegamenti in rete, quanto tutto era nuovo e sembrava di essere in un Far West, in una "nuova frontiera elettronica" che consentiva per la prima volta possibilità incredibili, ma che presentava, anche, grandi rischi.
Lo studioso individuò, innanzitutto, tre aspetti:

1. un **diritto sui dati** che immettiamo in rete affinché non siano controllati da altri soggetti contro la nostra volontà,
2. un nuovo ambiente dove esercitare **i propri diritti** quando si è online,
3. l'idea di un **corpo elettronico** che ha ciascuno di noi (una specie di profilo che ci rappresenta nell'ambiente digitale).

I nostri dati

Il primo aspetto, per Rodotà, è sicuramente il diritto alla **privacy**, ossia a che i nostri dati siano in qualche modo protetti e che non siano sfruttati contro la nostra volontà.
La **sorveglianza** è, oggi, la minaccia più grande. Mentre noi agiamo online, il sistema, le piattaforme, le app, i Governi e le multinazionali tengono sotto controllo tutto ciò che noi facciamo e possono usare queste informazioni per danneggiarci. Delle società a noi sconosciute possono raccogliere informazioni su di noi e classificarci, inserirci in determinare categorie che possono condizionare la nostra vita quotidiana.
Spesso sono anche gli utenti a esibire i loro dati, a comunicare informazioni su loro stessi, a essere spregiudicati e diffondere fotografie o video che, poi, possono essere raccolti e usati contro di loro. Siamo in una società dell'**esibizione**, dove il dato è comunicato

direttamente dall'utente senza prevederne, però, l'utilizzo successivo. Tanto che in molti studiosi parlano di una "morte della privacy", dell'utente stesso che non vuole tenere segreti i propri dati, ma li diffonde senza problemi.

In realtà, dice Rodotà, proprio questa esibizione continua dei nostri dati ci porta a riflettere sulla **necessità di una loro protezione**, ossia la volontà di chiudersi e di considerare in ogni momento quali e quanti dati che ci riguardano sono trattati in ogni momento. Il potere di controllo sui nostri dati, secondo Rodotà, è centrale.

I diritti in rete

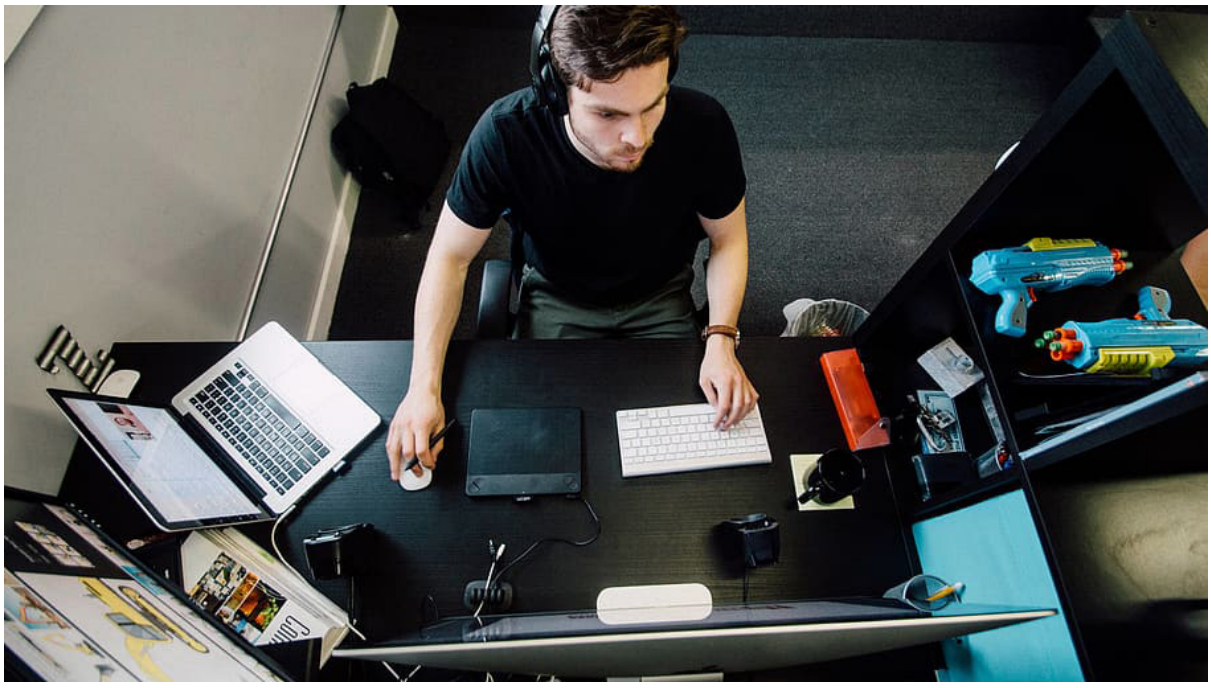
Il diritto alla privacy, primo e imprescindibile, si accompagna ad **altri diritti di libertà** che costituiscono una vera e propria **cittadinanza elettronica**, dove i valori della nostra Costituzione – libertà, eguaglianza tra le persone, dignità e democrazia – prendono vita e trovano una nuova espressione nel mondo online.

Abbiamo proiettato la protezione dei dati personali in una dimensione più ricca, senza arbìtri, ma interpretando correttamente una disciplina che vuole collocata tale protezione nel quadro dei diritti e delle libertà fondamentali, legata alla tutela della dignità. Emerge un legame profondo tra libertà, eguaglianza, democrazia, dignità e privacy, che ci impone di guardare a quest'ultima al di là della sua storica definizione come diritto ad essere lasciato solo. Senza una forte tutela delle loro informazioni, le persone rischiano sempre di più d'essere discriminate per le loro opinioni, credenze religiose, condizioni di salute: la privacy si presenta così come un elemento fondamentale della società dell'eguaglianza.

Senza una forte tutela dei dati riguardanti i loro rapporti con le istituzioni o l'appartenenza a partiti, sindacati, associazioni, movimenti, i cittadini rischiano d'essere esclusi dai processi democratici: così la privacy diventa una condizione essenziale per essere inclusi nella società della partecipazione.

> Per Rodotà è proprio grazie alla tutela della privacy che è possibile esercitare liberamente anche gli altri diritti ed essere, anche in questa nuova società digitale, cittadini attivi. L'avvento della rete e delle nuove tecnologie, se da un lato potrebbe introdurre nuovi ostacoli all'accesso di diritti ritenuti ormai acquisiti, dall'altro permette di **allargare il concetto di cittadinanza** a forme di partecipazione un tempo ignote. Questa è un'enorme opportunità per la democrazia e va difesa e tutelata.

Corpo elettronico



Per Rodotà è importante anche l'idea di "corpo elettronico", ossia l'**insieme delle informazioni** raccolte sul nostro conto e il **modo con cui noi ci presentiamo online**: con che profilo, modo di parlare, di interagire con gli altri utenti. Secondo Rodotà, il corpo elettronico deve avere la stessa protezione del corpo fisico.

Senza una forte tutela del "corpo elettronico", dell'insieme delle informazioni raccolte sul nostro conto, la stessa libertà personale è in pericolo e si rafforzano le spinte verso la costruzione di una società della sorveglianza, della classificazione, della selezione sociale: diventa così evidente che la privacy è uno strumento necessario per salvaguardare la società della libertà. Senza una resistenza continua alle microviolazioni, ai controlli continui, capillari, oppressivi o invisibili che invadono la stessa vita quotidiana, ci

ritroviamo nudi e deboli di fronte a poteri pubblici e privati: la privacy si specifica così come una componente ineliminabile della società della dignità.

Una carta dei diritti in Internet[3]

Il buon cittadino digitale non ha una "Costituzione" da seguire, ma molti Stati hanno elaborato dei **principi specifici per la vita online** che sono molto interessanti. L'Italia è stata uno dei primi Paesi al mondo a elaborare una Carta dei Diritti in Internet sempre grazie al lavoro prezioso di Stefano Rodotà. Tra le varie regole, tutte importanti, meritano forse una particolare attenzione, le seguenti

- **Il diritto di accesso.**
  Tutti dovrebbero poter accedere, oggi, a Internet. Soprattutto le persone più povere, gli emarginati, gli abitanti di Paesi che non sono ricchi come gli Stati occidentali. Collegarsi alla rete è fondamentale per la cultura, per i contatti, per allargare gli orizzonti e conoscere culture e abitudini che, grazie alla contaminazione, ci aiutano a crescere e a migliorare. Collegandosi a Internet, ogni persona riesce a garantirsi un pieno sviluppo individuale e sociale.

- **Il diritto alla conoscenza e all'educazione in rete.**
  Oltre all'accesso, tutti dovrebbero conoscere a fondo come funziona la società digitale, soprattutto per esercitare i suoi diritti. E tale educazione al digitale dovrebbe arrivare soprattutto dalla scuola e dalle istituzioni.

- **La neutralità della rete.**
  I contenuti che circolano in rete, le informazioni, i dati, non devono essere discriminati o bloccati, ma la persona deve essere in grado di ricevere qualsiasi tipo di informazione per avere un'idea corretta di ciò che accade nel mondo.

- **Il diritto alla inviolabilità dei sistemi, dei dispositivi e dei domicili informatici.**
  Importante è il principio della protezione dei propri dati, dei propri sistemi e del cosiddetto domicilio informatico. I nostri dati informatici è come se fossero dentro al nostro "domicilio", e nessuno può entrare per leggerli, modificarli o rubarli.

- **Il diritto all'oblio.**
  Anche la possibilità di rimuovere a un certo punto i propri dati, affinché non rimangano in eterno, è importante. Ciò avviene grazie alla deindicizzazione, ossia facendo sì che alcuni dati non siano più indicizzati dai motori di ricerca e non appaiano, quindi, all'atto di effettuare una ricerca in Google o in altri servizi simili.

II

La reputazione online e il cyberbullismo

Nel 2019 l'Università degli Studi di Milano e il CORECOM (Comitato regionale per le comunicazioni) della Lombardia, in collaborazione con l'Ordine degli Avvocati di Milano, hanno elaborato un **decalogo**, pensato soprattutto per gli studenti adolescenti, che mira a diffondere un uso responsabile delle tecnologie.

1. Tutto ciò che viene fatto online è pubblico

Il primo punto da far comprendere è che lo strumento utilizzato non consente l'intimità, la riservatezza o la chiusura. Non esiste il "mio" profilo, la "mia" bacheca, la "mia" chat, il "mio" canale, il "mio" account Instagram, il "mio" spazio web, il "mio" blog. Tutto ciò che viene fatto è pubblico. È visibile dai professori, dai genitori, dagli amici, è ricercabile sui motori di ricerca, e non esistono gruppi realmente chiusi né esiste intimità o confidenza. L'e-mail è come una cartolina, lo screenshot consente di violare ogni confidenza o intimità, e anche se una galleria di foto viene impostata come privata, il tag fa perdere il controllo della chiusura e, improvvisamente, apre, anche contro la nostra volontà, alla visione di altri soggetti. Ci sono alcune limitate possibilità di cancellare messaggi o immagini da WhatsApp o da altre app, ma se uno ha due telefoni – o effettua subito lo *screenshot* – salta anche questa tutela. "Pubblico" vuol dire che anche tutto ciò che è intimo, e viene condiviso, rischia di diventare pubblico. Diventa importante, allora, pensare prima a cosa sarà del messaggio, della foto o del video fatto circolare, e a che possibili effetti dannosi avrà. Molte piattaforme come Facebook o Instagram o Twitter consentono di alzare i parametri della propria privacy e comunque di essere meno esposti.

2. Tutto ciò che viene fatto online è amplificato

Siamo in presenza dello strumento più potente per la diffusione, oggi, dei messaggi, quindi, se ci mettiamo nei panni della vittima, la percezione del danno è fortissima. "Amplificato" vuol dire che raggiunge tantissime persone e tantissimi luoghi, anche di più del parlato. Da una classe, da un piccolo circolo o da un gruppo, può arrivare a tutto il mondo. La vittima si sente, allora, enormemente esposta, e il messaggio è più forte dell'offesa di persona. Occorre comprendere, pertanto, la potenza del mezzo che si ha in mano, un enorme megafono che, soprattutto nei panni di una vittima, ha un impatto tremendo. È, poi, un mezzo che può essere ossessivo-compulsivo, ossia i messaggi possono essere ripetuti in un tempo brevissimo, quindi l'amplificazione si potenzia ancora di più.

3. Tutto ciò che viene fatto online rimane per sempre

Il messaggio rimane per sempre. La rete non rimuove, o rimuove con grandissima difficoltà e non dimentica, e ripropone i contenuti anche dopo tanto tempo. Ciò comporta la necessità di pensarci prima, di riflettere prima di mandare un messaggio, una foto o un video, perché si sta ipotecando il futuro. Diventa molto importante capire la difficoltà tecnica di rimuovere, dopo, i contenuti.

4. Tutto ciò che viene fatto online diventa virale

Un contenuto prende vita, viene condiviso, diventa *trending topic*[4] e, quindi, più visibile in rete. Anche se parte in un contesto intimo, il contenuto inizia a circolare e non si può più fermare. Oggi la condivisione, i cuori, i like, il numero di commenti sono la nuova valuta, sono l'indice di gratificazione di un adolescente. Più sei "virale", più vali, ma il problema è che vieni condiviso anche se non vuoi, e i tuoi contenuti, al di fuori del contesto di origine, perdono il significato che avevano per assumerne uno nuovo.

5. Occorre proteggere la privacy propria e altrui

Il rispetto della privacy propria e altrui è centrale. La privacy "propria" significa non condividere dati intimi, che possono mettere in pericolo la sicurezza della persona. I dati si possono anche correlare, quindi anche un dato singolo, apparentemente inutile, può essere, se unito ad altri, un'informazione importante. Rispetto della privacy altrui vuol dire non violare i dati di altri. Se vediamo circolare un dato intimo di una persona, bisogna avvertirla e cancellarlo, non condividerlo, soprattutto su gruppi WhatsApp. Comprendere quali sono i dati più intimi è altrettanto importante: sessualità, salute, geo-localizzazione, riprese della propria abitazione, foto intime, video in classe, video dei professori, video di risse e di bullismo, video di disabili aggrediti. Anche il *sexting*[5] è molto diffuso, ma si può rivelare veramente pericoloso, così come forme di bullismo messe in atto da amici o amiche "del cuore", che prima si fanno confidare particolari intimi della vita della vittima e poi li rendono pubblici.

6. Occorre prestare attenzione ai fake e alle false identità/contatti

È facilissimo rubare l'identità, e in rete è complicato validare l'identità altrui. Diventa allora obbligatorio diffidare di qualsiasi contatto che domandi informazioni, che chieda foto; anche le informazioni sui social network sono spesso false, totalmente o parzialmente. Facilissimo è, oggi, creare un falso profilo, anche in poche ore, che sia credibile, per poi domandare contatti o foto. Nel mondo fisico abbiamo dei parametri che ci aiutano: sesso, età presunta, luogo dove abita il soggetto. Nel digitale, invece, tutto è diverso. Il *phishing*[6] è il metodo tipico, oggi anche personalizzato, ossia mirato a un soggetto dopo averne studiato le abitudini, per rubare dati. Diventa necessario anche riflettere sul valore, online, di termini come "amicizia", "relazione", "contatto". Sono veramente tutti amici quelli che in rete chiamiamo tali?

7. La diffidenza online è una virtù

Nell'ambiente digitale, la diffidenza è una virtù. Essere sempre diffidenti, e diffidare di richieste di qualsiasi tipo: informazioni, foto, richieste di cliccare su link o di aprire allegati, telefonate che domandano informazioni o promesse di riservatezza. È opportuno alzare sempre le cautele, non mostrare mai il viso, non esporre l'ambiente dove si è, verificare una persona indagando su fonti aperte e cercare di evitare di essere vittima di *stalking* limitando le informazioni o i contatti.

8. Non cambiate carattere online

Il mezzo telematico può cambiare il carattere, ha un effetto disinibitorio. Le persone più calme possono diventare delle furie: volgari, bestemmiatrici, disinibite, aggressive. Occorre, al contrario, ricordarsi sempre di essere online quello che si è offline, e di non approfittare della mancanza del soggetto per aggredirlo, né far circolare voci o pettegolezzi malevoli (anche perché in rete non si è mai, realmente anonimi).

9. Essere curiosi in relazione alle tecnologie

Più si conoscono le tecnologie che si usano, più si è sicuri. Diventa importante investire tempo nel conoscere le tecnologie, le funzioni, dove vengono salvate le informazioni, come bloccarle, come proteggersi, come elevare il livello di privacy, come proteggere le proprie credenziali, gli account, le password.

10. In caso di dubbio, parlarne

Non bisogna vergognarsi, ma se ci si sente a disagio con l'uso della tecnologia, è bene parlarne con un interlocutore affidabile. Il disagio, spesso, si capisce dalla tensione quando arrivano messaggi, dall'insonnia, dal controllo costante del telefono, dal timore di essere al centro dell'attenzione. Fare rete, soprattutto nel bullismo, è fondamentale, così come parlarne in famiglia, a scuola, o segnalare anche in maniera anonima e condividere il disagio con gli amici.

III

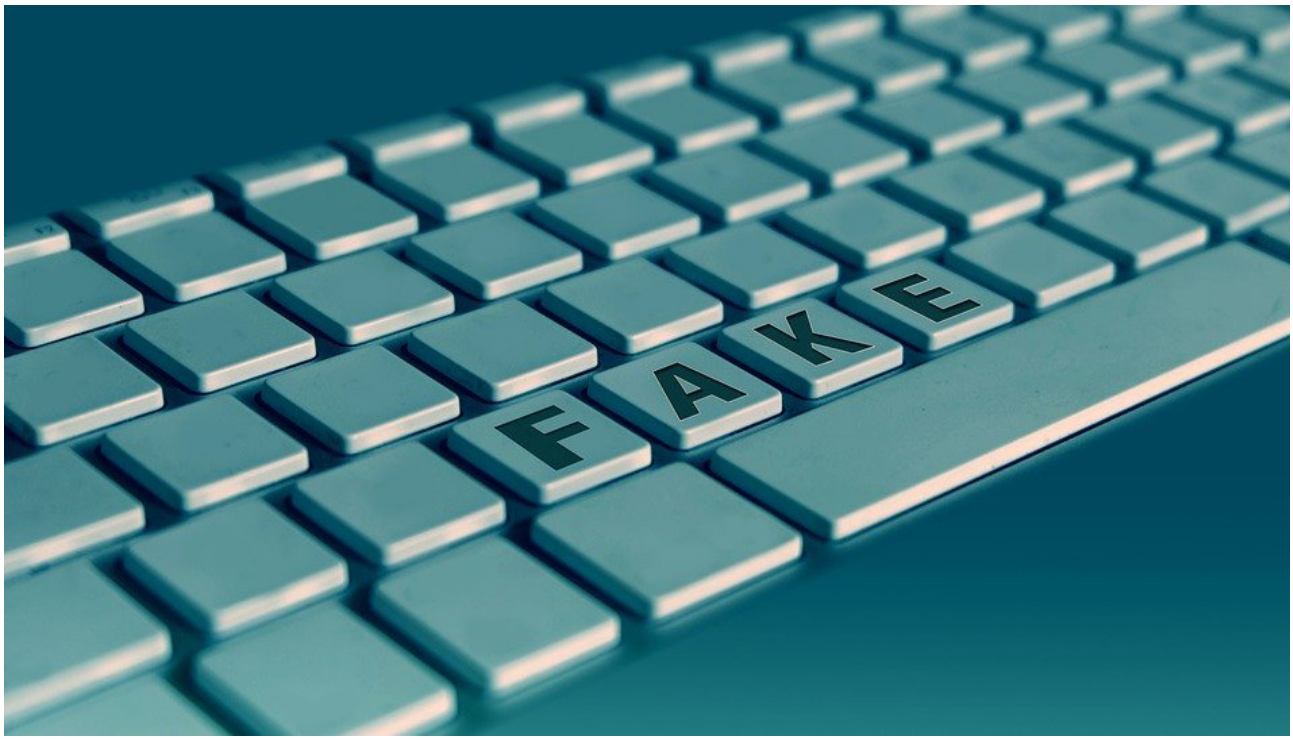
Odio e parole ostili

Con riferimento al **dialogo in rete**, diventa importante il modo con cui ci si relaziona con gli altri. Spesso le discussioni si "scaldano" e sono usati termini che possono offendere, creando un ambiente digitale che non è sano e che crea conflitti.
L'iniziativa "Parole Ostili" ha elaborato una serie di regole molto interessanti.

https://paroleostili.it/scarica-il-manifesto/

IV

Le fake news nella società democratica



Le *fake news*, come nota bene **Antonello Soro**, Garante per la privacy[7] italiano, sembrano unite a doppio filo all'architettura stessa dei social network, dove paiono aver trovato un terreno ideale per fiorire e moltiplicarsi.
Il concetto di *fake news* è semplice da comprendere: "*fake*" vuol dire "falso", "finto", quindi una "*fake news*" è una notizia, un post, un'immagine, un'informazione, un dato che è **palesemente falso**, ma che qualcuno, in rete, sui social network o in chat, fa comunque circolare.
Purtroppo, se in molte persone contribuiscono a far circolare queste notizie false, esse **diventano "virali"**, ossia si diffondono su molti profili, chat e siti, causando ancora più danni. Questo avviene molto spesso, come nota Soro, sulle piattaforme dei social network.

Estratto da A. Soro, *Persone in rete*, Fazi Editore, Roma 2018, p. 31

"I social assurgerebbero[8] così a luoghi in cui costruire una verità finalmente indipendente, perché liberata dalla soggezione al potere, e in cui custodire l'autenticità contro l'ipocrisia del mainstream[9]. Nasce qui, essenzialmente, il tema delle fake news, alimentato dal meccanismo su cui si fonda la condivisione virale in Rete, che fa dipendere l'attendibilità della notizia non dalla sua verificabilità, ma dalla quantità di condivisioni ottenute. È la logica dell'audience: le notizie, di qualsiasi origine, finiscono con il plasmare post-verità[10] e conferire autorevolezza alla loro fonte in funzione della quantità di lettori. Il che ha implicazioni importanti non soltanto rispetto al tema del pluralismo e della libertà di informazione

> ed espressione, ma anche rispetto alla formazione della volontà del corpo elettorale, laddove le false notizie concernono appunto questioni oggetto di voto popolare. La manipolazione del consenso, resa possibile dal condizionamento delle opinioni di cittadini profilati in base al loro comportamento in Rete, costituisce, infatti, un pericolo per la tenuta delle democrazie, che rischiano di regredire verso regimi plutocratici[11], fondati sul potere informativo.”

Le *fake news* in ambito politico, in particolare, si caratterizzerebbero per **quattro aspetti** che le rendono particolarmente insidiose.

1. Si fondano su una condivisione virale

La notizia falsa inizia immediatamente a circolare grazie ai contatti, alle condivisioni, alle reti di siti o profili appartenenti alla stessa “galassia” che, puntualmente, ne danno grande visibilità. Oggi tutti i partiti politici hanno una rete di profili, più o meno visibili e più o meno dichiarati, che sono in grado, in pochi secondi, di inondare i social network di notizie false. La viralità si appoggia sulla capacità di amplificazione e sulla persistenza dell’informazione, e fornisce lo strumento migliore per l’inizio delle operazioni di disinformazione.

2. Confidano sulla non verificabilità immediata

La ricerca di comunicazione immediata, poco complessa, elementare e superficiale di gran parte degli utenti sui social network fa sì che la maggior parte delle notizie false sfugga a un processo di verifica delle fonti, soprattutto se comporta la ricerca di fonti (investimento di tempo), l’uscita dall’ambiente dove ci si trova (spostarsi dalla pagina aperta di Facebook a un sito web) o se la notizia appare verosimile perché ben falsificata. A ciò si aggiunga il fatto che, se la notizia falsa arriva a una persona di cui già si conosce l’orientamento su quel tema, la verifica molto probabilmente non avviene per auto-convincimento del soggetto stesso.

3. Confidano sulla complicità di tante condivisioni che danno autorevolezza

Le notizie false, man mano che sono condivise, acquistano autorevolezza nel contesto dei social network. Grazie anche a persone che condividono con la classica frase “non so se è vera, ma la condivido”, o senza pensare, o perché in linea con il loro modo di pensare. L’autorevolezza non viene dalla verifica delle fonti ma dal numero di visualizzazioni, condivisioni e like. Lo *share*[12] è la moneta nel mercato dei social network: una valuta che assume sempre più valore tanto più attira condivisioni.

4. Sono sempre più mirate al soggetto

Le *fake news* sono sempre più mirate e ritagliate sul soggetto e sulle sue preferenze, saltando così il delicato aspetto della verifica – il target[13] non controlla la bontà della notizia perché “sente” quell’affermazione come sua – e domandando

al soggetto di far circolare nel suo ambiente (dove presumibilmente ci sono molti soggetti che la pensano allo stesso modo) quelle comunicazioni.
Remo Bodei descrive molto chiaramente questo passaggio nella direzione di un quadro di post-verità, di politica di annunci e, in definitiva, di *fictio* (finzione).

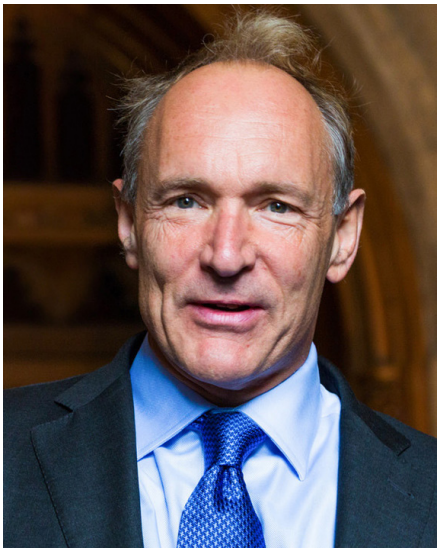
Estratto da R. Bodei, *Vivere online*, in "Il Mulino", 2/17, numero 490, p. 208-209

"La verità è oggi insidiata da quelli che [...] si chiamano «fatti alternativi», perché viviamo – è un'espressione che si sta affermando – nell'epoca della post-verità. Esiste ancora un'opinione pubblica, come sfera di dibattito basato su un serio confronto di idee o di posizioni, come «cane da guardia[14]» del potere? O non è anch'essa diventata una *fictio*, una costruzione capillarmente e scientificamente organizzata di una realtà parallela? E questo non avviene già, a monte, attraverso matrici[15] di idee ed emozioni preconfezionate, e, in seguito, mediante il loro ritocco e aggiornamento continuo, che produce un mutevole «clima di opinione»? E i cittadini non sono orientati anche attraverso una politica di annunci cui non segue alcuna effettiva attuazione, anche perché la politica non è più capace di operare scelte rilevanti e deve continuamente ammansire[16] gli elettori, gestire le frustrazioni e lavorare sul registro dell'immaginario[17] (paura e speranza), visto che i reali decisori sono élite economiche transnazionali, anonime e prive di responsabilità nei confronti dei cittadini?"

V

Uno sguardo al futuro. Le nove regole di Tim Berners-Lee

Tim Berners-Lee, uno dei "padri" del World Wide Web, nel novembre 2019 nel corso di una conferenza a Berlino, ha presentato il suo "contratto" (https://contractfortheweb.org), annunciato già nel 2018 a Lisbona in occasione del Web Summit: **nove regole** che dovrebbero **aiutare gli utenti della rete a veder rispettati i loro diritti** e a far sì che la vita online si svolga sempre in un **ambiente democratico e libero**.
Le prime tre regole coinvolgono i **Governi**. Gli Stati dovranno assicurare il rispetto della protezione dei dati, della privacy e dell'intimità degli utenti. Si tratta di un problema molto grave, perché in molti Stati tali diritti non sono rispettati e la privacy non è considerata un diritto fondamentale.
Altre tre regole riguardano, invece, gli **obblighi delle aziende**. I costi di connessione, di collegamento e accesso a Internet dovranno essere accessibili, per


Tim Berners-Lee

permettere a tutto il mondo di entrare online e sulle piattaforme, e le tecnologie stesse dovranno sempre più aiutare l'umanità a comunicare bene e con efficacia.
Infine, tre regole coinvolgono e riguardano direttamente i **cittadini**: gli utenti devono collaborare a creare un web, delle piattaforme e un ambiente che sia civile e che rispetti la dignità dell'uomo e i più diffusi, e comuni, principi di civiltà, soprattutto all'interno delle community[18] dove molti utenti "vivono", ormai, più di dieci ore al giorno.

Le regole di Tim Berners-Lee in sintesi

- Gli Stati e i Governi dovrebbero proteggere la rete e la società digitale.
- Gli Stati e i Governi dovrebbero proteggere la privacy degli utenti.
- La privacy dovrebbe diventare in tutti gli Stati un diritto fondamentale.
- Le aziende dovrebbero garantire a tutti una connessione economica e accessibile.
- Le aziende dovrebbero introdurre tecnologie che proteggano i diritti degli utenti.
- Gli utenti dovrebbero collaborare nel creare una community civile.
- Nella società digitale e sulle piattaforme ci dovrebbe sempre essere al centro il rispetto della dignità dell'uomo.

note

[1] **Empatia**: capacità di comprendere lo stato d'animo altrui.

[2] Stefano Rodotà, Relazione Autorità Garante, 2004, liberamente disponibile in rete: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1093776

[3] È possibile visualizzare l'intero documento al seguente indirizzo: www.camera.it/application/xmanager/projects/leg17/commissione_internet/TESTO_ITALIANO_DEFINITVO_2015.pdf

[4] ***Trending topic***: tema di tendenza, argomento popolare.ì

[5] ***Sexting***: invio di testi o immagini sessualmente esplicite tramite Internet o telefono cellulare.

[6] ***Phishing***: truffa informatica in cui si invita il soggetto a fornire dati riservati (numero di carta di credito, password di accesso al servizio di home banking ecc.), motivando tale richiesta con ragioni di ordine tecnico.

[7] **Garante per la privacy**: not anche come Garante per la Protezione dei Dati Personali, è un'autorità indipendente che in Italia e in tutti i Paesi dell'Unione europea vigila sul rispetto della protezione dei dati personali anche nella società digitale e sanziona enti pubblici e aziende private che operano in violazione dei dati dei cittadini/utenti.

[8] **assurgerebbero**: si eleverebbero, diventerebbero.

[9] **mainstream**: quando si parla di fake news, si intende l'insieme dei canali di comunicazione "ufficiali", per esempio una televisione di Stato o un grande quotidiano, e si contrappongono a canali di comunicazione "indipendenti" o personali che sono gestiti, invece, da piccole realtà o, addirittura, da singole persone.

[10] **post-verità**: indica quella condizione secondo cui, in una discussione relativa a un fatto o una notizia, la verità viene considerata una questione di secondaria importanza.

[11] **regimi plutocratici**: regime in cui il potere è nelle mani di chi detiene la maggior parte della ricchezza.

[12] **Share**: condivisione.

[13] **Target**: segmento di pubblico a cui è diretta una determinata comunicazione.

[14] **"Cane da guardia"**: che svolge una funzione di sorveglianza.

[15] **Matrici**: forme, stampi per modellare.

[16] **ammansire**: calmare, placare.

[17] **Registro dell'immaginario**: coincide con il pensiero del soggetto, con il mondo interiore e coscienziale.

[18] **Community**: si intende un ambiente (una piattaforma, un blog, una chat, un servizio) dove più utenti si incontrano e dialogano o giocano tra loro. Facebook, per esempio, può essere considerata una community, così come lo è anche un sito di videogiochi online.