Dilemma del cyberspazio: privacy o condivisione?

Alessandro Demma *Dottore in Scienze della Comunicazione, Università di Torino*
Daniele Roffinella *Professore e consulente ICT, Università di Torino*

In un mondo sempre più connesso, la nostra privacy è messa in discussione e la protezione dei dati non è più assicurata, senza specifiche misure. Mentre a livello internazionale si definiscono normative aggiornate, una parte del problema nasce dai comportamenti che noi stessi agiamo quando migriamo parte della nostra vita nel cyberspazio

Privacy, un diritto che ha richiesto tempo per essere riconosciuto

Con il termine *privacy*, nell'uso comune, si fa riferimento al *diritto alla riservatezza* delle informazioni personali e della vita privata. Nel corso del tempo esso ha subito alcune variazioni di significato, dovute all'evoluzione della società e della comunicazione umana.
Per gli antichi greci era motivo di disprezzo il fatto di non poter o voler partecipare alla vita pubblica (come avveniva, ad es., per gli schiavi o gli stranieri); tuttavia era anche riconosciuta la necessità di una vita privata, legata ai propri bisogni esclusivi[1]. Nel Medioevo il termine *privato* divenne sinonimo di *familiare*; la vita privata si basava sulla fiducia reciproca che univa i membri del gruppo, dando luogo a una vita familiare intensa, dove non vi era spazio per l'individuo isolato. È qui che inizia a prendere forma la necessità di garantire perimetri di intimità in tutti i campi (religioso, sociale, di pensiero), un concetto di riservatezza che si avvicina molto a quello odierno.
Le origini moderne del termine, tradizionalmente, si fanno risalire a due statunitensi, Samuel Warren e Louis Brandeis, con il loro saggio *The Right to Privacy. The Implicit Made Explicit*[2]. Era il 1890 e i due giovani avvocati stavano lavorando a una causa contro le indiscrezioni sulla vita matrimoniale della moglie dello stesso Warren da parte di un giornale, la *Evening Gazette* di Boston. Warren non accettava che i giornali si occupassero troppo della vita mondana di sua moglie. I due valutarono quali informazioni riguardanti la vita personale di un individuo dovessero essere di pubblico dominio e quali, invece, dovessero essere tutelate e rimanere private, e scrissero un articolo destinato a diventare famoso, nel quale esaminarono approfonditamente tutti gli aspetti del rapporto tra *diritto a informare e rispetto della riservatezza*.
La nascita e lo sviluppo in Europa del diritto giuridico di protezione dei dati personali è legato alla CEDU (Convenzione Europea dei Diritti dell'Uomo) e alla costituzione dell'Unione Europea. La CEDU, ratificata da tutti gli stati membri dell'UE, ha avuto un ruolo fondamentale perché, prima ancora che fossero istituite le comunità europee, ha inserito fra i diritti fondamentali dell'uomo l'*Articolo 8* (*Diritto al rispetto della vita privata e familiare*)[3], nel quale di

1 Vedi *Storia della Privacy*, a cura di M. Iaselli e S. Gorla, Roma, Lex et Ars, 2015. Estratto Ebook disponibile nel sito *Sicurezza e Giustizia*, https://www.sicurezzaegiustizia.com/storia-della-privacy/

2 S. Warren e L. Brandeis, *Right to Privacy*, "Harvard Law Review", 15 dicembre 1890. https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

3 Vedi sito Mondodiritto.it: *Diritto al rispetto della vita privata e familiare*, www.mondodiritto.it/codici/convenzione-europea-dei-diritti-dell-uomo/art-8-cedu-diritto-al-rispetto-della-vita-privata-e-familiare.html

fatto emerge già il diritto alla riservatezza. Ogni persona ha diritto al rispetto della propria vita privata e di quella della propria famiglia. Tale diritto si impone anche nei confronti dell'autorità pubblica, che può entrare nella vita privata degli individui e delle famiglie solo se è strettamente necessario e nei casi previsti dalla legge. Un altro aspetto importante dell'ordinamento CEDU è la *Convenzione 108* del 1981[4], con la quale il trattamento "automatizzato" (come la profilazione) dei dati dei cittadini viene sottoposto a regole specifiche di garanzia, tra cui il consenso al trattamento da parte dei cittadini e l'obbligo di non trasferire i dati verso ordinamenti che non ne garantiscono la protezione. CEDU è aperta anche all'adesione da parte di Paesi extraeuropei; ad esempio, l'Uruguay ha aderito nel 2013[5].
Il contributo diretto dell'Unione Europea, successivo rispetto a quello della CEDU, risale al 1995, con una serie di provvedimenti comunitari in cui viene ribadita la tutela della riservatezza come protezione dei dati personali.

1. Direttiva 95/46/CE[6]: relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, conosciuta anche come "direttiva madre".
2. Direttiva 97/66/CE[7]: relativa al trattamento dei dati personali ed alla tutela della vita privata nel settore delle telecomunicazioni.
3. Direttiva 2002/58/CE[8]: relativa al trattamento dei dati personali ed alla tutela della vita privata nel settore delle comunicazioni elettroniche.

Si arriva, infine, al 2016, data in cui entra in vigore il *Regolamento Generale sulla Protezione dei Dati* n. 2016/679 (GDPR)[9], che sostituisce la vecchia direttiva 95/46/CE e diventa il documento ufficiale comunitario in ambito di privacy. La sua effettiva attuazione avviene due anni dopo, nel 2018. Esso ha costituito un grande momento di svolta in termini di tutela della privacy, andando a potenziare le normative precedenti e rappresentando un insieme organico e coerente di regole.
Oggi la privacy viene definita anche come *diritto alla protezione dei dati personali*; tuttavia *privacy* e *protezione del dato* non sono esattamente la stessa cosa. Quando parliamo di privacy e riservatezza intendiamo la *tutela della sfera privata*, mentre la protezione del dato riguarda tutte le informazioni su una persona; se io voglio sentirmi libero di girare per casa mia vestito come più mi aggrada, chiedo che sia tutelata la mia privacy, mentre quando acquisto un biglietto per un viaggio, dove sopra c'è scritto il mio nome, l'orario di partenza, la destinazione, ecc., entra in gioco il trattamento di dati personali. Per *dati personali*, infatti, si intendono tutte le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire elementi conoscitivi circa sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc.
L'articolo analizza alcune problematiche della privacy nel mondo di oggi, relazionandola con la formidabile crescita delle nuove tecnologie e con il processo di migrazione di porzioni crescenti della nostra esistenza verso ambienti virtuali (inclusi i più basilari e oggi comuni, come le reti sociali su Internet), evidenziando come, inevitabilmente, diventi cruciale e ineludibile la scelta fra *socialità aumentata* e tutela del privato.

Privacy e Digitale

Oggi una percentuale continuamente crescente delle nostre azioni si svolge utilizzando, direttamente o indirettamente, reti di telecomunicazione e in particolare Internet; conseguentemente, quantità difficilmente stimabili di nostri dati personali vengono immessi in rete, subiscono trattamenti dalle Applicazioni che utilizziamo, finiscono memorizzati in archivi elettronici che possono trovarsi anche in altri Paesi. Non sempre le società che vengono in possesso di tali dati li utilizzano con modalità del tutto trasparenti. Molto frequentemente siamo noi stessi che cediamo nostri dati; in alcuni casi siamo quasi "costretti" a farlo perché richiesto da enti pubblici o per finalità di interesse generale (un esempio che aveva suscitato dibattiti

4 Vedi sito del Garante della Privacy: *Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data*, www.garanteprivacy.it/documents/10160/10704/Convention+no.+108.pdf/a1f4f72f-7060-4e35-b371-2a31d158f1ec?version=1.2

5 Vedi sito del Consiglio d'Europa: *Protezione dei dati personali: l'Uruguay è il primo Stato non europeo ad aderire alla Convenzione 108*, www.coe.int/it/web/portal/-/personal-data-protection-uruguay-becomes-first-non-european-state-to-accede-to-convention-108-

6 Vedi sito della Commissione Europea: *Direttiva 95/46/CE*, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=LEGISSUM%3Al14012

7 Vedi sito della Commissione Europea: *Direttiva 97/66/CE*, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A31997L0066

8 Vedi sito della Commissione Europea: *Direttiva 2002/58/CE*, https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A32002L0058

9 Vedi sito della Commissione Europea: *Regolamento n.2016/679*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434

era stata la cessione di dati medici in occasione della campagna per il contenimento del COVID-19), ma spesso consegniamo senza difficoltà nostri dati a chiunque ci "regali" una App, un gioco, una iscrizione a un canale social, una partecipazione a un qualche tipo di concorso a premi, ecc.
Con l'espressione *Digital Privacy* si fa riferimento, letteralmente, alla riservatezza all'interno del mondo digitale. Potrebbe quasi sembrare un ossimoro, visto che la maggior parte della nostra vita in rete riguarda la *condivisione*: tutto ciò che accade all'interno del digitale è condiviso, in una qualche misura. Condividere è così semplice che spesso non ci si rende nemmeno conto di quanto comunichiamo di noi stessi, e più condividiamo, più la nostra privacy si riduce.
Un tempo molte informazioni riguardanti la sfera personale venivano condivise soltanto con la propria cerchia ristretta di familiari o amici; oggi invece quantità crescenti di informazioni personali non soltanto diventano disponibili per un insieme di persone estremamente più ampio, ma sono anche destinate a rimanere nella rete per sempre, dal momento che diventa praticamente impossibile cancellare definitivamente qualcosa che sia stato immesso online[10].
Un altro punto importante è la distinzione tra *Cybersecurity* e *Digital Privacy*. Per *Cybersecurity* si intende la capacità di difendere i nostri dati da attacchi esterni (ad es., da eventuali hacker), mentre quando si parla di *Digital Privacy* ci si riferisce alla capacità di ognuno di decidere consapevolmente cosa rendere pubblico e cosa mantenere privato nel mondo digitale. Qualsiasi servizio online che utilizziamo tipicamente usa i nostri dati per varie finalità, tra le quali ad esempio il marketing, secondo i termini di accordi che sottoscriviamo "volontariamente e liberamente" al momento dell'iscrizione quando, forse troppo velocemente, mettiamo un segno di "spunta" su una qualche casellina in lunghi moduli illeggibili che ci compaiono velocemente sullo schermo. Siamo ormai abituati a servizi che offrono un'alta personalizzazione: quando usiamo un motore di ricerca come *Google*, ad esempio, quest'ultimo è in grado di "ricordare" le nostre ricerche precedenti, così come accade quando facciamo un acquisto su un sito di *e-commerce* come *Amazon* o scriviamo la recensione di un ristorante su un sito di condivisione specializzato come *TripAdvisor*. Più usiamo questi servizi, più la loro capacità di offrirci soluzioni e prodotti adatti a noi aumenta; questo è effettivamente un aspetto positivo, purtroppo ciò è possibile solo grazie al fatto che i nostri dati vengono raccolti, memorizzati, analizzati (e non raramente anche "rivenduti") dalle società che ci offrono i servizi, spesso con il nostro inconsapevole consenso. Chi davanti a una nuova App o a un nuovo servizio online di interesse per noi si è fermato a leggere tutte le condizioni, i vincoli, le liberatorie, anche soltanto nelle parti principali? Solitamente ci si limita ad accettare e dare il consenso al trattamento senza leggere nulla. Se ci fermassimo ad esaminare le varie clausole, forse saremmo meno pronti a "vendere" (o regalare) i nostri dati; ma, d'altra parte, forse il nostro interesse verso la applicazione in oggetto potrebbe essere tale da indurci ad accettare in ogni caso i termini del contratto.
Per quanto riguarda la tutela della privacy in termini generali (cioè non specificamente nel mondo digitale) esistono enti appositamente costituiti per contrastare abusi e pratiche scorrette. A livello nazionale, con la *legge n.675* (la cosiddetta *legge sulla privacy*) del 31 dicembre 1996 venne istituita la figura fondamentale del *Garante per la Protezione dei Dati Personali* (GPDP)[11]. È un'autorità amministrativa indipendente che assicura la tutela dei diritti e delle libertà fondamentali e il rispetto della dignità nel trattamento dei dati personali. È un organo collegiale composto da quattro membri eletti dal Parlamento, i quali rimangono in carica per un mandato di sette anni non rinnovabile.
A livello europeo l'autorità fondamentale per quanto riguarda la tutela dei dati personali è la *Commissione Europea*, della quale fanno parte i singoli organismi nazionali, tra i quali il citato GPDP. Come già richiamato, il contributo normativo iniziale dell'Unione Europea risale al 1995, con una serie di provvedimenti comunitari (3 diverse direttive). La svolta, però, si ha solamente nel 2016 con l'attuazione del citato GDPR. Esso definisce quali sono i soggetti in gioco nel trattamento dei dati personali ma soprattutto quali sono i *diritti fondamentali* degli interessati. Esso stabilisce, inoltre, che ogni trattamento di dati personali deve avvenire secondo definiti principi di liceità; soprattutto deve essere sempre presente il *consenso* dell'interessato (tranne in alcuni casi limite, in cui prevale, ad es., il diritto all'informazione pubblica).
Il GDPR ha rappresentato un passaggio fondamentale per la tutela della privacy; grazie ad esso è aumentata la stessa consapevolezza degli individui sul tema, come indirettamente dimostrato dall'incremento del numero delle segnalazioni di

10 Vedi sito Garante della Privacy: *Diritto all'oblio*, www.garanteprivacy.it/i-miei-diritti/diritti/oblio

11 Vedi sito GPDP: www.garanteprivacy.it

violazioni di dati personali, che, ad esempio, nei primi tre anni di attuazione del suddetto regolamento sono state oltre 25mila[12].

Tuttavia, il GDPR non tutela specificamente tutte quelle forme di comunicazione che avvengono nel *Cyberspazio*, come ad esempio il marketing, l'E-commerce, i call center, la pubblicità online; questo è un compito affidato al regolamento per la tutela della cosiddetta *e-Privacy*[13], che non è ancora in vigore. Il 10 gennaio 2017 è stata formulata una proposta di regolamento che sta ancora seguendo l'iter nelle sedi istituzionali UE. Dopo anni di sostanziali "nulla di fatto" ci fu una prima svolta l'11 febbraio 2021 con l'approvazione definitiva di un testo aggiornato da parte del Consiglio UE. Il Regolamento *e-Privacy* potrebbe, nella migliore delle ipotesi, entrare in vigore nel corrente anno 2023, con la previsione di un periodo di ulteriori due anni prima di una sua piena applicazione. Il futuro Regolamento *e-Privacy* potrà innalzare il livello di protezione, integrandosi con il GDPR e fornendo finalmente tutele specifiche per tutti i tipi di comunicazioni elettroniche.
La complessità e intrinseca lunghezza dei processi approvativi a livello comunitario europeo non impediscono che i lavori proseguano, su aspetti generali come su problematiche specifiche; ad esempio molto recentemente (maggio 2023) c'è stato il via libera dalle commissioni Giustizia e Mercato Interno dell'Eurocamera all'AiAct[14], che fissa per la prima volta le regole UE per l'Intelligenza Artificiale, toccando anche tematiche di privacy. L'Eurocamera ha votato per il divieto di utilizzo di tecnologie a Intelligenza Artificiale per il riconoscimento facciale nei luoghi pubblici in tutti i Paesi europei. Sempre nel maggio 2023 è entrato in vigore il *Digital Markets Act* (DMA)[15], il Regolamento dell'Unione Europea per il contrasto alle potenziali pratiche scorrette dei cosiddetti *Gatekeepers* (le grandi piattaforme online che detengono una posizione dominante all'interno del mercato digitale); la nuova normativa è molto ampia e contiene anche tutele per i dati personali degli utenti delle piattaforme. A fine 2022 era entrato in vigore il *Digital Services Act* (DSA)[16], legge sui servizi digitali che rappresenta, con il DMA, un insieme organico di norme, definito avendo fra i suoi obiettivi principali la creazione in Europa di uno spazio digitale più sicuro, in cui siano protetti i diritti fondamentali di tutti gli utenti dei servizi digitali. I lavori su tutta l'area tematica sono in corso.

Il cyberspazio: un luogo confortevole o insidioso?

Il termine cyberspazio[17] deriva dalla fusione di cibernetica (parola coniata nel 1948 da Norbert Wiener per indicare i fenomeni biologici o artificiali di autoregolazione) e spazio; esso apparve nel 1982, nella sua forma inglese *cyberspace*, in un racconto di fantascienza dal titolo *Burning Chrome* ("La notte che bruciammo Chrome"), pubblicato da William Gibson sulla rivista *Omni*, e due anni dopo nel suo romanzo *Neuromancer*. L'opera ebbe un discreto successo e contribuì in modo importante alla diffusione del termine, utilizzato nel romanzo per indicare uno spazio digitale e navigabile (dal greco *kyber*: timone).
Il cyberspazio è un luogo praticamente infinito e sempre immediatamente accessibile. In città come in campagna, a casa, sui luoghi di lavoro, di svago, essere costantemente *online* genera relazioni multiple, immateriali, istantanee, che avvengono in simultanea: passeggiando per la strada posso chiacchierare con un amico e tenere il vivavoce attivo per far partecipare alla conversazione un'altra persona lontana, mentre pubblico un *selfie* su Facebook, e magari scorro alcuni *tweet* e metto dei *like* a qualche post; intanto il mio *fitness ring* prende nota con cura del mio consumo di calorie, del percorso che sto facendo, forse anche delle mie pulsazioni, e trasmette tutti i dati a qualche server nel *Cloud*, per poi preparare dei rapporti dettagliati che saranno utili a me e al mio *personal trainer*.
Si tratta di uno spazio immateriale di informazioni, che è stato reso possibile dallo sviluppo costante delle reti [1], e che ha ulteriormente ridotto i "6 gradi di separazione" fra gli individui ipotizzati dal-

12 A. Cataleta, *GDPR, un bilancio dei primi tre anni*, sito Agenda Digitale, giugno 2021, www.agendadigitale.eu/sicurezza/privacy/gdpr-un-bilancio-dei-primi-tre-anni-di-applicazione-effetti-traguardi-e-prossimi-step

13 Vedi sito EU: *Proposta di regolamento ePrivacy*, https://digital-strategy.ec.europa.eu/it/policies/eprivacy-regulation

14 Vedi sito ANSA: *No al riconoscimento facciale nei luoghi pubblici*, maggio 2023, Primo via libera del Parlamento alle regole per l'Intelligenza Artificiale - Europarlamento - ANSA.it

15 Vedi sito della Commissione EU: *Digital Market Act*, https://digital-markets-act.ec.europa.eu/index_en

16 Vedi sito della Commissione EU: *Digital Service Act*, https://digital-strategy.ec.europa.eu/it/policies/digital-services-act-package

17 Vedi sito Treccani: *Ciberspazio*, www.treccani.it/vocabolario/ciberspazio

lo scrittore ungherese Frigyes Karinthy [2]; è il risultato della combinazione da un lato di un processo graduale di *moltiplicazione*, ovvero dell'aumento quantitativo dei legami e delle relazioni, dall'altro di un salto, una svolta *qualitativa nelle interazioni* degli individui fra di loro e con il contesto, il quale nel frattempo si è dematerializzato.
Alla loro nascita le reti sociali essenzialmente replicavano le preesistenti reti che le persone avevano costruito nella loro vita reale, ed erano pertanto socialmente e geograficamente limitate. Ben presto avere migliaia di amici nel mondo online diventò un indice di popolarità e influenza; dal momento che quell'indice era pubblico, ben visibile, le persone furono motivate ad estendere le proprie reti oltre i vincoli materiali, cognitivi e culturali presenti nel mondo fisico. Altri incentivi entrarono in gioco, come quello economico; per favorire l'estensione delle reti le piattaforme indussero gli utenti a trovare gruppi di "amici" completamente nuovi, perché in questo modo veniva incrementato il tempo di permanenza online e la conseguente possibilità di ottenere profitti grazie alla visualizzazione di un maggior numero di annunci pubblicitari, selezionati sulle base delle caratteristiche del gruppo oltre che dell'individuo. Sistemi di raccomandazione personalizzati favorirono il collegamento tra persone che non si conoscevano ma che avevamo almeno un amico (oppure almeno degli interessi) in comune: fenomeno definito come la *chiusura dei triangoli* [3].
Tutto questo, e la indubbia semplicità di utilizzo e "utilità" di molteplici App, per lo più gratuite, ha fatto in modo che il cyberspazio sia sempre più popolato; report pubblici[18] indicano che oggi 5,44 miliardi di persone usano telefoni cellulari, pari al 68% della popolazione mondiale, e ci sono 5,16 miliardi utenti di Internet che tutti i giorni trascorrono in media oltre 6 ore e mezza sulla rete. Poco meno del 60% della popolazione mondiale sono utenti dei social media, e vivono nel cyberspazio principalmente per rimanere in contatto con amici e familiari (53,7%), rimanere aggiornati su notizie e attualità (50,9%), e guardare video (49,7%). Analisi dell'uso della App TikTok su piattaforma Android mostrano che i post contrassegnati con #FYP ("Per te", la pagina personale di TikTok) sono stati visualizzati per un totale di 35 trilioni di volte lo scorso anno; anche se ognuna di queste views fosse durata solo un secondo, vorrebbe dire un milione di anni, e solo per quel particolare sottoinsieme di video.
La espansione del cyberspazio va ben oltre ciò che facciamo al PC, tablet o smartphone: accanto alle persone, cresce vertiginosamente il numero delle "cose" che vengono a popolarlo. L'*Internet of Things* (IoT) comprende tipologie estremamente variegate di dispositivi connessi che generano e condividono dati fra loro, come elettrodomestici (TV *smart*, termostati, impianti di illuminazione e di sicurezza), assistenti intelligenti (Google Home, Amazon Echo, Apple Homepod), sistemi di videosorveglianza, automobili sempre più *smart*, dispositivi medicali, tecnologie indossabili (Fitbit, scarpe intelligenti, Apple Watch, cappelli smart), ma anche ciotole per il cibo degli animali, materassini per yoga, saliere, tostapane, specchi, bottiglie dell'acqua, fasciatoi per cambiare i bambini, ecc., oltre a tutto il mondo dell'industria, della *smart agricolture*, dell'automazione. Si stima che l'IoT generi molte decine di zettabyte[19], dati che, uniti a quelli derivati dall'uso delle App, del web e dei *social networks*, arriva a quintilioni[20] di byte di dati ogni giorno (cifra che si scrive con 18 zeri). Ci stiamo muovendo verso la *Quettabyte Era*[21], e quando anche solo porzioni minime di questa enorme quantità di informazioni vengono raccolte, memorizzate ed elaborate, diventa possibile costruire rappresentazioni estremamente dettagliate dei comportamenti delle persone, con impatti distruttivi sulla privacy; le piattaforme probabilmente conoscono di noi molto più di quanto ne sappiamo noi stessi.
Questa esplosione di dati comporta rischi crescenti per la *sicurezza* in senso stretto, ma non è solo questo che turba le nostre esistenze nel mondo digitale.
Si può affermare che i rischi per la sicurezza sono ormai ben noti; il cyberspazio è teatro di continue lotte, e vere e proprie guerre, fra chi attua attacchi telematici di svariate tipologie e chi cerca di sventarli. Come ricordato anche dal *Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale*[22], secondo una stima di Microsoft i tentativi di cyber

18 Vedi sito WeAreSocial: *Report DIGITAL 2023*, https://wearesocial.com/it/blog/2023/01/digital-2023-i-dati-globali

19 Analisi IDC, citata in articolo su sito Network Digital: A. Casali, *Industrial IoT*, novembre 2020, www.industry4business.it/industria-4-0/industrial-iot-cose-e-quali-sono-i-vantaggi-per-la-smart-factory

20 Vedi sito BigData4Innovation: *Big Data: ogni giorno prodotti 3 quintilioni di Byte*, febbraio 2019, www.bigdata4innovation.it/big-data/big-data-ogni-giorno-prodotti-3-quintilioni-di-byte

21 T. Fruet, *La Quettabyte era*, marzo 2023, www.italiagrafica.com/la-quettabyte-era

22 Vedi sito della Autorità Nazionale per la Cybersicurezza: www.acn.gov.it

attacchi al secondo nel mondo sono 1.300, cioè 110 milioni al giorno, 3 milioni dei quali in Italia[23]. È una guerra senza esclusione di colpi, che coinvolge aziende, singoli individui, gli Stati, e che si è intensificata anche a causa della crescita delle tensioni geopolitiche internazionali, mentre si fatica a trovare intese fra Paesi anche solo sul piano del diritto normativo[24]; per conoscere i dati principali del fenomeno (che esula dallo scopo di questo articolo) si può ad esempio fare riferimento al *Global Cybersecurity Outlook 2023*[25] pubblicato in occasione del *World Economic Forum* tenutosi a Davos a gennaio.

Anche senza considerare questa vera e propria guerra, e rimanendo nella legalità, il cyberspazio nasconde altre insidie, tanto più pericolose quanto più cresce la compenetrazione fra i due mondi, quello fisico e quello digitale. Oggi, con lo smartphone diventato quasi una protesi del nostro corpo, abbiamo a che fare con un unico ambiente, il cosiddetto *phygital*[26] (o in italiano *figitale*) in cui non è facile distinguere il "fisico" dal "digitale". Il mondo del marketing e delle vendite da qualche tempo ha chiaramente identificato questa nuova dimensione mista, per sfruttarla secondo i propri obiettivi[27]. Si sta modificando il nostro modo di lavorare, di studiare, di socializzare, di trascorrere il tempo libero, con una crescita continua delle "cose che facciamo" con ausilio di applicazioni, reti e dispositivi ICT. La vita diventa ibrida, fra fisico e digitale, e la pandemia mondiale COVID-19 ha accelerato questo processo, che determina purtroppo anche vere e proprie patologie come *Hikikomori*, termine giapponese che significa "stare in disparte", e indica chi decide di ritirarsi dalla vita sociale per lunghi periodi, alle volte anni. Rinchiusi nella propria abitazione, anche in Italia decine di migliaia di persone, soprattutto adolescenti, vivono solo nel cyberspazio, evitando qualunque tipo di contatto fisico diretto con il mondo fisico esterno[28].

Ma potenzialmente ancora più preoccupanti, anche se forse meno evidenti, sono gli effetti della espansione del cyberspazio sui comportamenti collettivi nel medio e lungo termine. Ci si vuole qui riferire non ai ben noti (e in molti casi spesso vantaggiosi) cambiamenti nelle modalità con cui, da un numero crescente di persone, vengono svolte con l'aiuto di App, terminali, piattaforme ICT, molteplici attività quotidiane nel lavoro, nella formazione, nel tempo libero; il tema è invece *l'influenza sulle persone considerate nella loro collettività*, su fenomeni sociali, in alcuni casi anche violenti, associati alla rapidissima diffusione su larga scala, facilitata dalle reti, di elementi di condizionamento soft o hard, come polarizzazione, manipolazione, disinformazione e teorie del complotto. Si tratta di un tema di grande complessità, ed una sua trattazione esula dallo scopo di questo articolo; tuttavia c'è lo spazio per citare *The Social Dilemma*[29], un documentario di Netflix uscito a fine 2020, incentrato sul lato oscuro dei social media. Esso esplora come le piattaforme social utilizzino, per autoalimentarsi, da un lato la dipendenza psicologica degli utenti e dall'altro la violazione sistematica della privacy. Il fatto che il cyberspazio crei dipendenza non sorprende; senza arrivare ai livelli patologici della FOMO (*Fear Of Missing Out*)[30]: l'ansia e il panico generati dal non poter avere notifiche e aggiornamenti quando si è offline), tutti noi abituati a utilizzare quotidianamente App e *social networks* sappiamo che non è semplice "dimenticare" per mezza giornata il cellulare, smettere di aggiornare la pagina della home, staccarsi dalle *storie* di amici e personaggi che ci interessano. Ciò che invece rende inquietante la visione del

23 Vedi sito ANSA: *Cybersicurezza: Baldoni, in Italia 3 mln di attacchi al giorno*, gennaio 2023, www.ansa.it/sito/notizie/topnews/2023/01/24/cybersicurezza-baldoni-in-italia-3-mln-di-attacchi-al-giorno_ec662dab-aaa6-4998-bb06-6acdba9e4371.html

24 Vedi sito di Agenda Digitale: G. Iuvinale, *Offensive e spionaggio nel cyberspazio: quali norme applicare*, marzo 2023, www.agendadigitale.eu/sicurezza/offensive-e-spionaggio-nel-cyberspazio-quali-norme-si-applicano

25 Vedi sito del World Economic Forum: *Global Security Outlook Report 2023*, www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

26 Vedi sito EconomyUp: L. Maci, *Phygital: cos'è, come funziona e come sfruttarlo per migliorare la customer experience*, 18 settembre 2020, www.economyup.it/innovazione/phygital-cose-come-funziona-e-come-sfruttarlo-per-migliorare-la-customer-experience

27 Vedi sito del Sole24Ore: *L'esperienza di acquisto è sempre più phygital*, novembre 2021, www.ilsole24ore.com/art/l-esperienza-acquisto-e-sempre-piu-phygital-ecco-perche-incontro-i-canali-tradizionali-e-digitale-puo-essere-vantaggio-i-consumatori-AE9GY5x

28 Vedi sito di *La Repubblica: Allarme hikikomori in Italia*, marzo 2023, www.repubblica.it/cronaca/2023/03/02/news/hikikomori_adolescenti_italia_54_mila_casi_ricerca-390255495/

29 Vedi sito di CineFilos: C. Guida, *The Social Dilemma, recensione del documentario Netflix*, settembre 2020, www.cinefilos.it/tutto-film/recensioni/the-social-dilemma-netflix-463195

30 Vedi sito di *Wired*: M. Musso, *Come si manifesta la Fomo*, ottobre 2022, www.wired.it/article/fomo-sindrome-cos-e-spiegazione-sintomi

documentario Netflix è che questa dipendenza non è semplicemente un effetto collaterale, bensì un obiettivo specifico perseguito dalle aziende della Silicon Valley, almeno secondo quanto dichiarano i "pentiti dei social network" intervistati nel documentario. Le notifiche *push*, l'aggiornamento della pagina con lo scorrimento del dito dall'alto verso il basso, le pagine sponsorizzate personalizzate, utilizzano i dati non solo per prevedere ma anche e soprattutto per influenzare le nostre azioni, per alterare i nostri bisogni trasformandoci in "merce" messa a disposizione degli inserzionisti: "Se non stai pagando per il prodotto, allora il prodotto sei tu".

Non si tratta soltanto delle tecniche (peraltro forse discutibili) del *Programmatic Advertising* [4]. Nel *Programmatic*, lo spazio pubblicitario disponibile nella pagina che ci compare sullo schermo del PC o dello smartphone viene aggiudicato mediante aste istantanee automatiche a uno degli inserzionisti che, in quel momento, vogliono trasmetterci una informazione pubblicitaria, specificamente correlata al profilo che è stato costruito su di noi. Secondo il documentario Netflix (volutamente provocatorio) si va oltre, generando stimoli specifici di vario tipo indirizzati a ciascun abitante del cyberspazio, finalizzati a modellare i suoi stessi orientamenti e comportamenti. Le tecniche utilizzate sono molteplici, e le più insidiose sono quelle meno facilmente riconoscibili.

Ad esempio il *Nudging* si basa sul condizionare una scelta attraverso delle "piccole spinte" (dall'inglese *nudge*, pungolo, termine reso famoso da Richard Thaler, Premio Nobel per l'economia 2017, e Cass Sunstein nel loro libro *Nudge - La spinta gentile* [5]). Proveniente dalla psicologia comportamentale[31], l'approccio si fonda sull'assunto che una persona, attraverso degli stimoli positivi o che deviano l'attenzione, possa mettere in atto delle azioni ben precise; nel cyberspazio, esso evolve diventando *hypernudging*[32] costruito in particolare sul metodo della cosiddetta "selezione di default". Nella teoria dei *nudge*, le *opzioni di default* sono delle scelte predefinite che funzionano come raccomandazioni accettate passivamente, soprattutto a causa del cosiddetto *default bias*, che porta le persone a preferire lo status quo anche quando non vi sono costi per effettuare una scelta diversa. Grazie all'uso dei *big data* e dell'intelligenza artificiale, l'*hypernudging* utilizzerebbe sistemi di default di tipo altamente profilato che appartengono a tre categorie principali: default *persistenti*: le scelte passate funzionano da predittore delle scelte future; default *predefiniti* ad alta correlazione: utilizzano e incrociano dati riferiti sia all'utente che a terzi ad esso collegati; default di *adattamento*: le impostazioni vengono aggiornate in modo dinamico in base alle decisioni in tempo reale fatte dall'individuo. La leva chiave utilizzata è una accurata pre-selezione, effettuata dagli algoritmi, delle informazioni che ci vengono messe a disposizione di volta in volta: la *strategia di oscuramento* di alcuni dati da parte dei social, opera come un nudge costruito per orientare le nostre scelte; la riproposizione, in forme sempre leggermente differenti e anche in contesti differenti, di *nudge* coerenti fra loro, aumenta sia la loro efficacia, sia la nostra difficoltà a prenderne consapevolezza.

Una tecnica diffusa e piuttosto insidiosa sono i cosiddetti *dark patterns*[33], elementi formali dell'interfaccia di interazione uomo-macchina realizzati su piattaforme social network o siti web, concepiti per "confondere" l'utente, e indurlo a compiere azioni non desiderate, oppure in grado di "scoraggiarlo" dal prendere determinate decisioni potenzialmente dannose per la privacy del singolo, ma favorevoli all'interesse della piattaforma o del gestore del servizio.

Le tecniche sono molto numerose[34]; ad esempio gli *stratagemmi nel contenuto* riguardano la formulazione delle frasi e il contesto delle componenti informative mentre gli *stratagemmi sull'interfaccia* sono correlati alle modalità di visualizzazione del contenuto, alla navigazione o all'interazione con i "bottoni cliccabili" presenti in una pagina. Come esempio minimale, solo per chiarire il principio, basti pensare a come normalmente sono fatte le pagine pubblicitarie *pop-up* che ci vengono presentate per effettuare la nostra scelta circa

31 Da ricordare che nell'ambito della psicologia comportamentale non tutti sono d'accordo sulla pratica del *nudging*; si veda ad es. [6]

32 K. Yeung, *Hypernudge: Big Data as a Mode of Regulation by Design*, "Information, Communication & Society", luglio 2016, https://ssrn.com/abstract=2807574

33 Vedi sito Garante delle Privacy: *Modelli di progettazione ingannevoli (Dark Pattern)*, 2023, www.garanteprivacy.it/temi/internet-e-nuove-tecnologie/dark-pattern

34 Vedi sito Agenda Digitale, A. Lo Giudice, *Dark pattern, così le aziende ingannano gli utenti*, marzo 2022, www.agendadigitale.eu/sicurezza/privacy/dark-pattern-cosi-le-aziende-ingannano-gli-utenti-le-nuove-linee-guida-edpb

35 Vedi sito dell'Indiscreto: G. Didino, *Nella gabbia di Skinner: social media, pessimismo e falso Sé*, ottobre 2020, www.indiscreto.org/social-dilemma

l'accettazione o meno dei *cookies*; l'opzione a noi più favorevole (il rifiuto) è spesso non immediatamente visibile nella pagina, e può contenere elementi grafici o testuali che tendono a scoraggiarne la scelta, mentre quelle sfavorevoli sono sempre ben evidenziate (Figura 1).
Nel cyberspazio gli individui vengono messi in condizioni operative semplici e accattivanti, ma che possono ridurre e anche azzerare la consapevolezza riguardo a "come" si formano le scelte che continuamente essi prendono mentre stanno nel mondo virtuale. Non è solo un tema di manipolazione in senso stretto: l'individuo non arriva quasi mai a percepire la possibilità di un condizionamento e, quando ci riuscisse, metodi e processi utilizzati dalle piattaforme rimarrebbero comunque a lui inaccessibili e quindi difficilmente elaborabili cognitivamente. Si attua quindi una doppia limitazione della autonomia decisionale: da un lato, perché i cyber-abitanti si illudono di perseguire fini propri, dall'altro perché vengono indirizzati verso fini a loro ignoti, decisi da altri.
Secondo alcuni, migrare nel cyberspazio è come entrare volontariamente in una *gabbia di Skinner*[35]: una volta dentro, ci mettiamo alla mercé di complessi, instancabili, onnipresenti meccanismi di condizionamento, finalizzati nei casi migliori a obiettivi di marketing. Nei casi peggiori gli utilizzi strumentali delle piattaforme del cyberspazio, resi possibili dalla volontaria rinuncia alla privacy, possono avere effetti devastanti nello spazio della vita reale. Ad esempio i meccanismi di scelta dei rappresentanti degli elettori dei paesi democratici sono messi a rischio dalla facilità con cui si può manipolare l'opinione pubblica grazie alla comunicazione online micro-targettizzata, costruita sui big data, e le tecniche messe a punto per rendere virali i messaggi, fino ad arrivare alla possibilità di veicolare velocemente, a costi ridicoli, *hate speech* di propaganda e *fake news* che possono distorcere la percezione della realtà e, quindi, orientare il consenso. Anche escludendo il dolo, le norme della *par condicio* utilizzate in periodi elettorali sono del tutto inefficaci nel mondo dei social, nel quale avviene una percentuale sempre più importante degli scambi informativi, ma che rimane sostanzialmente fuori dalla normativa.
Non solo le informazioni che ci vengono mostrate possono essere il risultato di un filtraggio preventivo personalizzato, ma la stessa "costruzione" delle reti sociali fatta dalle persone può venire orientata. Una delle attrattive irresistibili del cyberspazio è la grande facilità con cui, vivendolo, diventa possibile creare, estendere e utilizzare le nostre reti di conoscenze e relazioni. Come noto, sono le stesse piattaforme che continuamente ci propongono altre persone con cui stabilire un link, grazie alle analisi che fanno sui nostri profili, elaborando i dati relativi ai nostri comportamenti, alle nostre preferenze, alla nostra storia personale; e sono ancora le piattaforme che, instancabilmente, scelgono quali "novità" segnalarci, fra tutte quelle che riguardano le persone che sono entrate nelle nostre reti sociali. Le nostre reazioni alle loro proposte (i nostri like, cuoricini, il tempo che dedichiamo a leggere una notizia o guardare un post che ci viene proposto, ecc.) istruiscono gli algoritmi rendendoli sempre più bravi nel fare le loro selezioni. Tuttavia, questa "creazione guidata" delle comunità virtuali di cui andiamo a far parte può facilmente determinare la costruzione di vere e pro-

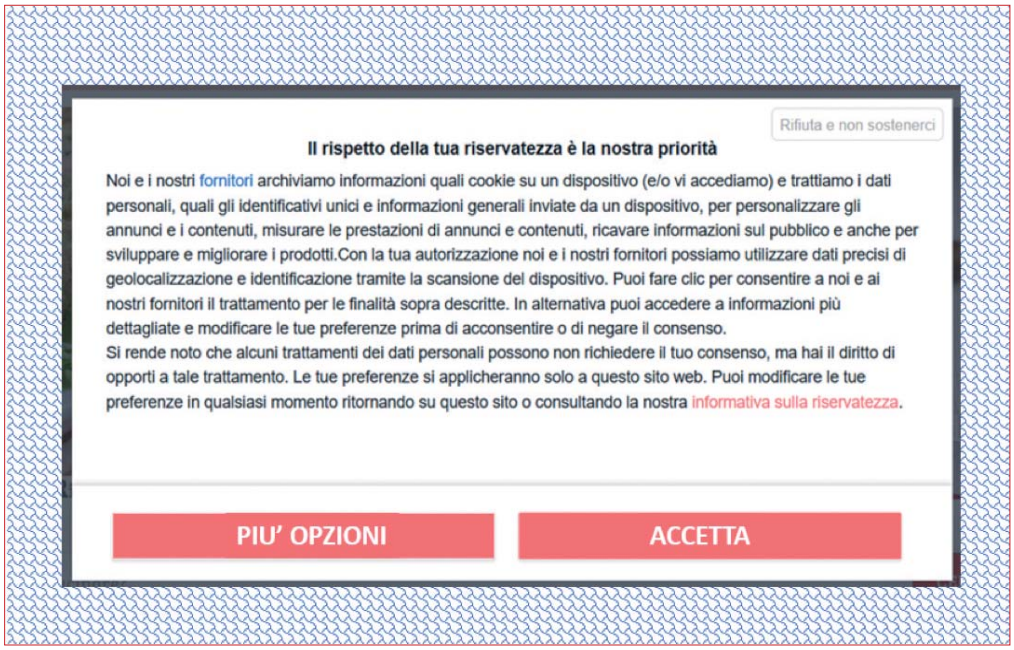

Figura 1
Esempio elementare di "stratagemma sull'interfaccia" - la opzione di maggior tutela (collocata in alto a destra) è realizzata in modo da non attirare la nostra attenzione; inoltre il testo utilizzato per tale scelta ("...non sostenerci") evoca un comportamento riprovevole

prie *echo chambers*[36]. Le reti sociali, che costruiamo con l'aiuto non disinteressato delle piattaforme stesse, diventano spesso luoghi caratterizzati da forti omogeneità (di orientamenti, preferenze, interessi); questo rende più piacevole e confortevole passare il nostro tempo in tali luoghi, ma presenta forti rischi di "segregazione ideologica", che determinano una ulteriore riduzione della nostra libertà effettiva e dell'accesso ad informazioni e visioni pluralistiche. I risultati di studi sul tema[37] hanno evidenziato che l'omofilia generalmente aumenta la diffusione di disinformazione (non solo su specifici fatti, ma soprattutto sugli orientamenti, sui modi con cui ci si approccia ai fatti stessi), ed accentua i fenomeni di polarizzazione degli atteggiamenti e delle opinioni delle persone; le notizie di parte, vere o false, si diffondono maggiormente nelle cosiddette *ideologically segregated networks*. Le nostre reti sociali possono trasformarsi in gigantesche camere d'eco, in cui "gli altri" sembrano pensarla proprio come noi, rafforzando ma irrigidendo la nostra visione del mondo e dei suoi problemi, e non ci sfiora il sospetto che questo in realtà avviene solo perché la nostra rete è stata costruita proprio "su misura" per il nostro profilo, per rendere più efficaci i meccanismi di *confirmation bias* [7]. Inoltre la uniformità creata non solo dalle *filter bubble* ben note da tempo[38], ma anche da selezioni mirate sui componenti stessi delle reti di persone, condiziona i meccanismi di confronto e scambio, e mina la veridicità sostanziale delle informazioni che circolano nel cyberspazio, aumentando l'esposizione a contenuti pre-orientati.
Si potrebbe essere scettici circa l'effettiva efficacia dei condizionamenti soft e hard a cui si è soggetti nel cyberspazio, ma la problematica è oggetto di innumerevoli analisi che purtroppo mettono in luce i risultati ottenibili con un uso mirato delle piattaforme, ad esempio nel campo del marketing, al punto che a livello di istituzioni comunitarie si cerca di definire un minimo di regolamentazione (come il citato *Digital Market Act*). Un altro noto esempio è il possibile uso strumentale delle piattaforme per condizionare gli orientamenti politici; come dichiarato a dicembre 2022 dal *Presidente del Garante per la protezione dei dati personali*[39], "*Il caso di* Cambridge Analytica[40] *ha evidenziato come, utilizzando lo strumento del microtargeting, si possa modellare il messaggio politico da promuovere, orientando il consenso elettorale verso il risultato voluto. Si eludono così le garanzie previste per il pluralismo informativo e politico, come pure per l'autodeterminazione individuale, con il rischio di una manipolazione del consenso, tale da alterare in radice i più rilevanti processi democratici*".
È interessante evidenziare che la tematica del condizionamento delle comunità di individui (per certi aspetti più preoccupante del condizionamento dei singoli), è anch'essa oggetto di analisi. Fra i tanti, si vogliono qui citare gli studi secondo cui i comportamenti umani sulle piattaforme riproducono diversi aspetti di quello collettivo di alcuni animali, ma attraverso reti intenzionalmente condizionate da sofisticati meccanismi[41]; "*The behavior is determined by the structure of the network, which shapes the behavior of the network, which shapes the structure, and so on*". L'esempio più noto è quello degli stormi di uccelli o branchi di pesci, il cui comportamento gregario è orientato da meccanismi imitativi e di propagazione del movimento tra gli individui all'interno del gruppo, ed è subordinato a un complesso insieme di condizionamenti fisiologici e meccanici. Secondo questo approccio di analisi, anche la relazione sociale (nel mondo fisico come nel cyberspazio) può essere descritta come un *fenomeno emergente*, cioè come un dominio con proprietà proprie non presenti nelle parti costitutive, ma che si generano ed emergono appunto nella relazione. Emergenza, nell'interpretazione più classica, significa il sorgere di nuove proprietà a un livello superiore, quella "danza delle parti interagenti" [8] che produce senso e identità. L'idea pro-

36 Vedi sito Culture Digitali: *Echo chambers: opinione pubblica e disinformazione*, giugno 2021, www.culturedigitali.org/echo-chambers-la-formazione-dellopinione-pubblica-e-della-disinformazione

37 Vedi sito della rivista Nature: J. Stein et al., *Network segregation and the propagation of misinformation*, gennaio 2023, www.nature.com/articles/s41598-022-26913-5#msdynttrid=ME5_fRiT2WPzKja4tqsUlu6fGZPf4MlnVHELsClh-6w

38 Vedi sito di Agenda Digitale: V. Bernardinis, *Vedere ciò che vogliamo vedere: le conseguenze della Filter Bubble*, ottobre 2015, www.agendadigitale.eu/cultura-digitale/vedere-cio-che-vogliamo-vedere-le-conseguenze-della-filter-bubble

39 Vedi sito del garante Privacy: M. Cannata, *Un governo sostenibile della Rete serve per difendere la democrazia - Intervista a Pasquale Stanzione*, dicembre 2022, www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9833041

40 Vedi sito ANSA: *Meta paga 725 milioni per lo scandalo Cambridge Analytica*, dicembre 2022, www.ansa.it/sito/notizie/tecnologia/internet_social/2022/12/23/meta-paga-725-milioni-per-lo-scandalo-cambridge-analytica_874c3879-bb31-4925-8399-35b235d47b64.html

41 Vedi sito Noema: R. Diresta, *How Online Mobs Act Like Flocks Of Birds*, novembre 2022, www.noemamag.com/how-online-mobs-act-like-flocks-of-birds

viene dalla scienza della complessità e affonda le sue radici nel concetto di *autopoiesi* (un sistema autopoietico è un sistema capace di auto-organizzarsi e di riprodurre sé stesso attraverso le sue relazioni dinamiche interne).
Similmente a quanto accade negli stormi di uccelli, nei social le persone subiscono e contemporaneamente esercitano influenze nei confronti degli altri individui a loro connessi, e ne scaturiscono caratteristiche "emergenti" del gruppo, proprie di quella particolare rete connessa; come voterà alle elezioni politiche un gruppo social appassionato di escursioni in montagna? e un gruppo di cacciatori? Quale abbigliamento sarà acquistato da un gruppo di Tiktoker adolescenti che ascoltano musica trap in cui i membri più "influenti" pubblicano video mentre indossano magliette o scarpe di una certa marca?

La risposta è dentro di noi, ma è sbagliata: il *privacy paradox*

Il cyberspazio è dunque un luogo che presenta rischi per la nostra privacy. Come richiamato nel capitolo iniziale, le tutele normative vengono gradualmente rafforzate, per proteggerci da attacchi e violazioni malevoli o anche criminali, ma esistono contromisure efficaci per il *paradosso della privacy*? Questo fenomeno, su cui esiste una ampia letteratura[42], si riferisce alla discrepanza tra le preoccupazioni dichiarate dalle persone sulla privacy da un lato, e i loro comportamenti effettivi dall'altro, comportamenti che spesso comportano la divulgazione di informazioni personali.
Secondo la *Teoria del Calcolo della Privacy* [9-10] gli individui decidono di divulgare loro informazioni personali quando i potenziali benefici (servizi personalizzati, sconti, accesso ad informazioni, aumento della propria visibilità, ecc.) superano le perdite di quote di privacy. Tuttavia, le ricerche in Economia Comportamentale hanno evidenziato come il processo decisionale umano, soprattutto nelle microdecisioni (tipiche della vita online) non è affatto razionale, ma è influenzato da molteplici fattori, come l'incompletezza delle informazioni che possiamo utilizzare per effettuare le scelte: non si conosce realmente l'entità e la tipologia dei dati raccolti dalle piattaforme quando le si utilizza, e non si è consapevoli dei rischi e delle conseguenze della loro divulgazione, nonché di cosa verrà fatto con essi.
Inoltre il cybernauta corre continuamente rischi dovuti alla propria capacità cognitiva limitata e ai *bias* cognitivi (ben documentati da una vasta letteratura comportamentale), come il *bias dell'ottimismo*, *l'overconfidence* e lo *sconto iperbolico*. Il primo esprime la tendenza degli individui ad essere irrealisticamente ottimisti nel valutare la probabilità di eventi futuri, il che può portarli a sottovalutare la probabilità di subire un danno di privacy. L'*overconfidence* si riferisce alla tendenza a riporre eccessiva fiducia nelle proprie scelte e capacità previsionali, ad esempio nella stima dei possibili rischi per la propria privacy. Infine, lo sconto iperbolico indica la preferenza delle persone per scelte che comportino vantaggi immediati rispetto a quelli futuri, anche quando i primi implicano una maggiore perdita di privacy (il termine "sconto" si riferisce al "tasso di sconto" utilizzato implicitamente nella valutazione di accadimenti, con un tasso relativamente elevato su orizzonti temporali brevi e relativamente basso su quelli lunghi, il che induce a optare per la gratificazione immediata, ignorando il rischio a lungo termine).
La lista sarebbe lunga: il *confirmation bias* ci spinge a dare più importanza alle informazioni che sostengono la nostra tesi o il nostro pregiudizio, l'*ostrich bias* (effetto struzzo) è quello che ci fa non considerare dati o posizioni che contrastano con le nostre convinzioni, il *bandwagon bias* ci spinge a sviluppare una convinzione in relazione al numero di altre persone che la condividono, ecc.
Il crescente numero di violazioni della privacy e di furti di identità, e alcune campagne di sensibilizzazione, hanno ha reso le persone più consapevoli della necessità di proteggere la propria privacy; ciononostante continuano a crescere le condivisioni di informazioni personali online. Ciò può essere dovuto a molte ragioni, tra cui il desiderio di sentirsi connessi con gli altri, la pressione sociale per partecipare ai social media, la mancanza di reale conoscenza sulle implicazioni della condivisione di dati personali, la fiducia che le aziende proteggeranno i dati dell'utente, e come accennato, una sovrastima dei vantaggi ed una sottostima dei rischi.
In un famoso esperimento di alcuni anni fa [11] ai partecipanti veniva chiesto di effettuare un determinato acquisto da uno a scelta fra due negozi concorrenti, il primo dei quali richiedeva una maggiore divulgazione di dati sensibili (reddito e data completa di nascita) rispetto al secondo (colore preferito e solo l'anno di nascita); quasi tutti i partecipanti scelsero il primo negozio, quando esso praticava un prezzo era più basso (un euro in meno), mentre quando il prezzo era identico, i soggetti acquistavano da entrambi i negozi in egual misura.
Da un certo punto di vista la privacy può essere considerata un "lusso". Molti servizi online, come

42 Vedi sito OpenLibrary: L. Robertson, *The Privacy Paradox: Present and Future*, https://ecampusontario.pressbooks.pub/digitalprivacyleadershipandpolicy/chapter/the-privacy-paradox-present-and-future/

quelli dei social media, dei motori di ricerca, delle App "funzionali" (come i navigatori), sono gratuiti per l'utente finale, ma si basano sulla raccolta di dati personali utilizzati per profilature, pubblicità, ecc. Se l'utente scegliesse di non condividere i propri dati, potrebbe dover pagare un prezzo per l'utilizzo di questi servizi; ma quanti sarebbero disposti a pagare, ad esempio, 200 euro l'anno per usare Facebook?[43]

Davvero vorremmo più privacy?

Il cyberspazio, come sopra argomentato, è un luogo con molte insidie, ma ci passiamo volentieri molto tempo, perché forse sottovalutiamo i rischi, e soprattutto perché è frequentato da persone interessanti e dai nostri amici, è economico, comodo e anche piacevole, e ci troviamo dentro cose utili, anche cose che non sapevamo ci servissero; ci sono applicazioni per tutto: fare acquisti di qualunque tipo, ricevere cibo a domicilio, cucinarlo, allietarci con diverse forme di intrattenimento, gestire la casa, fare nuovi incontri, ecc.
D'altra parte nella *società dell'ostentazione* desideriamo veramente la privacy? Il cyberspazio è per sua natura un luogo di condivisione che esercita attrazione crescente, e funziona così efficacemente proprio grazie alla partecipazione eccitata della massa di persone e all'impegno speso quotidianamente nel farsi contemplare e nel regalare informazioni. Quanto meno, questo è il pensiero (piuttosto noto, anche se non da tutti condiviso) del sociologo Zygmunt Bauman che parlò di "*società confessionale*[44] che promuove la pubblica esposizione di sé al rango di prova eminente e più accessibile, oltre che verosimilmente più efficace, di esistenza sociale". Umberto Eco, in una celebre *Bustina di Minerva* nel 2014, scrisse: "*è paradossale che qualcuno debba lottare per la difesa della privatezza in una società di esibizionisti*" e, in un'altra occasione, "*chi difende la privacy difende qualcosa che la gente in realtà non vuole più; la gente ormai vuole andare in tv a dire che è cornuta, usa in modo spasmodico il telefonino, che è la negazione della privacy; va su Internet, si fa assalire dalle offerte pubblicitarie, paga ed è contenta*".
Nell'opinione di chi scrive, è forse impossibile condurre oggi un'analisi "completa" della tematica, utile per prevedere, anche solo a grandi linee, quale potrà essere il risultato del complesso processo di trasformazione in corso; il cyberspazio non sparirà, anzi continuerà a crescere, ma quale sarà la condizione di equilibrio stabile fra riservatezza e condivisione? Le riflessioni personali di ciascuno potrebbero giovarsi dell'esame di scenari immaginati da scrittori e registi di "fantascienza". Un esempio fra tutti è il celebre romanzo *The Circle* [12] di Dave Eggers, che tratta il tema della privacy nella società tecnologica contemporanea. La storia è costruita intorno alle scelte della protagonista Mae Holland, una giovane donna che inizia a lavorare presso *il Cerchio*, un'azienda tecnologica dominante che mira a creare un mondo in cui tutti i dati delle persone siano accessibili a tutti, con l'obiettivo dichiarato di creare una società perfettamente trasparente. Il libro mette bene in luce il paradosso della privacy, ovvero la contraddizione tra il desiderio di privacy e il bisogno di condividere informazioni per partecipare alla vita comune e contribuire attivamente alla costruzione di una società che si presenta migliore e desiderabile. L'idea centrale è che la *condivisione totale* di informazioni sia la chiave per una società aperta, egualitaria, democratica, in cui addirittura diventano impossibili non solo i reati, ma

Figura 2
Nel romanzo The Circle *si cerca di realizzare una società basata sulla condivisione e sulla trasparenza, a discapito della privacy*

43 Stima relativa al 2016, vedi sito del Sole24Ore: *Il paradosso della privacy, e quanto siamo disposti a pagare per averla*, www.ilsole24ore.com/art/il-paradosso-privacy-e-quanto-siamo-disposti-pagare-averla-AEKG872D

44 Zygmunt Bauman, *Sicuri che il trionfo della privacy sia reale?* vedi estratto sul sito TG24, https://tg24.sky.it/mondo/2014/03/21/zygmunt_bauman_david_lyon_sesto_potere_laterza_libri

45 Vedi sito Wordpress: *Sesto Potere: La Sorveglianza Post-Panottica di Bauman*, settembre 2015, https://theteknologist.wordpress.com/2015/09/19/la-sorveglianza-post-panottica-di-bauman

46 Vedi sito *La Repubblica: Il "padrino" dell'Intelligenza artificiale lascia Google*, www.repubblica.it/esteri/2023/05/02/news/geoffrey_hinton_lascia_google_intelligenza_artificiale-398421958

anche i comportamenti riprovevoli ("*chi compirebbe una cattiva azione se fosse certo di essere osservato e riconosciuto*?"). Torna nuovamente in mente Bauman, che stigmatizza il *synopticon*[45]: la sorveglianza dei molti sui molti, la sorveglianza senza sorveglianti per cui "*non c'è più bisogno di costruire mura ed erigere torri di guardia per tenerci dentro i prigionieri*", perché "*ci si attende che siano loro stessi a erigere le mura*".

Il romanzo di Eggers porta questa idea all'estremo, descrivendo un mondo in cui la privacy è completamente abolita e in cui ogni azione viene monitorata e giudicata dalla comunità online; emergono così anche le conseguenze negative dell'eliminazione della privacy, mostrando come la sorveglianza costante possa portare a una perdita di libertà e autonomia, e come la condivisione eccessiva delle informazioni personali possa essere utilizzata, da pochissimi privilegiati, per manipolare e controllare le masse di persone. Se però cercassimo in questa opera un suggerimento circa quale possa essere il giusto "punto di equilibrio" fra la tutela della privacy e l'accesso ai vantaggi di una società trasparente, rimarremmo con tutti i nostri dubbi. Infatti la ambiguità circa "cosa sia meglio" è rispecchiata nelle posizioni rappresentate dai diversi protagonisti.

Non solo: è interessante notare come la conclusione del romanzo e la conclusione dell'omonimo film (figura 2) da esso tratto siano opposte. In entrambi i casi la protagonista Mae viene messe in guardia da ciò che il Cerchio sta per diventare: una specie di monopolio totalitarista. Nel film lei mostra di comprendere il pericolo ed espone anche i due grandi capi dell'azienda alla completa trasparenza, di fatto smascherando le loro vere intenzioni totalitarie e condannandoli a bere la stessa medicina che essi avevano preparato per le masse. Nel libro invece Mae finisce per abbracciare totalmente le finalità del Cerchio, ed aiuta i due capi a concludere il loro progetto di monopolio dittatoriale tecnologico; estremizzando ulteriormente la visione totalitaria, nelle ultime pagine Mae fantastica su come "*sarebbe bello se anche i pensieri, non solo le effettive azioni, potessero essere condivisi e resi totalmente trasparenti*": lei è convinta sia ciò di cui il mondo ha effettivamente bisogno.

Una conclusione che non si può (ancora) scrivere

Lo scenario tratteggiato da Dave Eggers è, naturalmente, una invenzione; tuttavia val la pena di tenerne conto, nelle riflessioni sui futuri possibili. Oltre a ciò che intenzionalmente condividiamo sui *social networks*, e alle informazioni che ci vengono carpite con poca nostra consapevolezza tutte le volte che scorriamo post e pagine web, usiamo una App, tagghiamo qualcosa o mettiamo un *like*, scegliamo un programma sulla nostra Smart TV, esistono altre minacce per la privacy: in casa come in auto e al lavoro, gli assistenti virtuali come Alexa, Siri, Cortana, mentre ci aiutano in modo sempre più efficace, finiscono per conoscere porzioni crescenti della nostra vita che crediamo "privata". Nel frattempo la *Intelligenza Artificiale Generativa* (come *ChatGPT*) sta iniziando a farci intravedere, non senza dibattiti, polemiche[46] e qualche preoccupazione, le incredibili potenzialità di sistemi che hanno accesso a una quantità incalcolabile di informazioni, e le sanno utilizzare maledettamente bene. Ci sarà un momento in cui decideremo di fermare il processo di espansione del cyberspazio, rinunciando a grandi comodità, per difendere qualcosa di "solamente nostro"? Difficile prevederlo; l'unico auspicio che gli autori del presente articolo si sentono di fare è il seguente: che un numero sempre maggiore di persone acquisisca rapidamente una consapevolezza sempre più ampia e aggiornata sulle dinamiche straordinarie dell'universo digitale.

Gli autori ringraziano l'ing. Angelo Luvison per il costante incoraggiamento e i preziosi suggerimenti che hanno reso possibile la preparazione dell'articolo.

BIBLIOGRAFIA

[1] S.Drago, D.Roffinella: Reti sociali, small world, privacy, *AEIT*, novembre/dicembre 2021.

[2] F. Karinthy: *Viaggio intorno al mio cranio*, BUR Biblioteca Univ. Rizzoli, 2010.

[3] S. Aral: *Hype machine. Come i social media sconvolgono le elezioni, l'economia e la salute*, LaFeltrinelli, 2021.

[4] E. Lanfranco, D. Roffinella: Programmatic Advertising e intelligenza artificiale, *AEIT*, gennaio-febbraio 2020.

[5] R. Thaler, C. Sunstein: *Nudge, la spinta gentile. La nuova strategia per migliorare le nostre decisioni su denaro, salute, felicità*, LaFeltrinelli, 2014.

[6] M. Galletti, S. Vida: *Libertà vigilata. Una critica del paternalismo libertario*, IF Press, 2018.

[7] S. Modgil et al.: *A Confirmation Bias View on Social Media Induced Polarisation During Covid-19*, Springer Link, novembre 2021.

[8] G. Bateson: *Verso un'ecologia della mente*, Adelphi, 1977.

[9] S. Kokolakis: Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon, *Elseviere*, 2015.

[10] M.J. Culnan, P.K. Armstrong: *Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation*, Organization science, 1999.

[11] A. Beresford et al.: Unwillingness to pay for privacy: A field experiment, *Elseviere*, 2012.

[12] D. Eggers: *Il Cerchio*, Mondadori, novembre 2014.