ALESSANDRO ALONGI, FABIO POMPEI

Algoritmi, sicurezza ed etica dell'innovazione

La persona al centro della transizione digitale

prefazione di Massimiliano Capitanio
introduzione di Fabio Massimo Castaldo

SAGGI

tab edizioni

© 2023 Gruppo editoriale Tab s.r.l.
viale Manzoni 24/c
00185 Roma
www.tabedizioni.it

Prima edizione settembre 2023
ISBN versione cartacea 978-88-9295-757-2
ISBN versione digitale 978-88-9295-758-9

È vietata la riproduzione, anche parziale,
con qualsiasi mezzo effettuata, compresa la
fotocopia, senza l'autorizzazione dell'editore.
Tutti i diritti sono riservati.

Crediamo in una transizione digitale antropocentrica. Si tratta di chi vogliamo essere, in quanto europei. Per coglierne l'essenza formuleremo una serie di principi digitali. Tra questi, l'accesso a Internet per tutti; uno spazio online sicuro; il diritto di acquisire competenze digitali; algoritmi rispettosi delle persone; la protezione dei minori online. Questi principi essenziali integreranno i diritti già previsti dal quadro giuridico dell'UE a tutela degli europei online, tra cui la protezione dei dati personali o la libertà di espressione.

Ursula von der Leyen, *Guidare il decennio digitale*,
Sines, 1° giugno 2021

Indice

Prefazione

In principio erano i diritti

L'Italia non è (ancora) un paese digitale. Basti pensare che, prima dell'approvazione del decreto Covid del settembre 2020, i certificati di nascita e di morte, in tutti i Comuni italiani, dovevano essere stampati, per legge, con stampanti ad aghi su fogli A3+. La sola mancata digitalizzazione della pubblica amministrazione fa perdere all'Italia qualcosa come 25 miliardi di euro ogni anno[1]. Del resto, a oggi, la patente non è digitale, non lo è la carta di identità, ma nemmeno la tessera elettorale. Non parliamo, poi, del passaporto e dell'odissea per ottenerlo.

Eppure, la trasformazione digitale ha parzialmente rivoluzionato numerosi settori cruciali della nostra società, quali i trasporti, l'energia, la sanità, l'istruzione e la finanza, ma anche il settore dei media e dell'informazione. Durante la pandemia, senza digitalizzazione, non sarebbero stati possibili lavoro agile e didattica a distanza.

Scuola e lavoro sono diritti costituzionali, e la digitalizzazione rende questi diritti più accessibili. È sufficiente questo, e molto altro, per sostenere incondizionatamente i processi di dematerializzazione e semplificazione che sono alla base del passaggio dall'analogico al digitale?

La dipendenza dalle tecnologie può essere un rischio come giustamente ci interrogano gli autori di questo volume?

Fa bene questo libro a mettere "la persona al centro della transizione digitale". Di fronte al predominio della tecnica e della tecnologia, è quanto mai urgente affiancare delle riflessioni sui risvolti etici di questa epoca digitale.

Il paragone è presto fatto. L'avvento dell'automobile è stato rivoluzionario, nessuno vorrebbe tornare all'epoca dei carri trainati dai cavalli. Eppure, gui-

1. Fonte: Confindustria digitale, https://confindustriadigitale.it/.

dare un'auto richiede un corso di formazione e una patente, ma soprattutto la consapevolezza legata ai rischi per sé e per gli altri.

I navigatori del web o i giustamente amanti della tecnologia hanno questa consapevolezza? Ce l'hanno le imprese che gravitano attorno a questo business?

Lo sviluppo tecnologico non può chiudere gli occhi davanti ai costanti furti di dati, di brevetti, di fronte alle truffe, ai più disparati reati digitali, al dilagare della disinformazione, all'evoluzione della criminalità organizzata, alle nuove dipendenze patologiche.

Fanno bene gli autori a evidenziare che la sicurezza trattata in questo libro non riguarda solo la vulnerabilità delle infrastrutture di comunicazione, ma anche delle dinamiche sociali che ne sono veicolate, talvolta con effetti distorsivi e dannosi per la società. Negli ultimi anni, ad esempio, si è osservato un aumento preoccupante della violenza verbale, di dinamiche discriminatorie all'interno degli ambienti digitali e di incremento della polarizzazione delle posizioni. Nei casi più gravi si può addirittura parlare di veri e propri discorsi d'odio.

Quando si arriva a invocare l'inserimento dell'identità digitale in Costituzione lo si fa anche perché oggi, quotidianamente, si violano i principi fondamentali di tutela della persona, del rispetto della dignità umana e del principio di non discriminazione. Per contrastare questa situazione, l'autorità per le garanzie nelle comunicazioni ha adottato regolamenti e delibere che promuovono il rispetto della persona, in linea con quanto gli autori denunciano nelle pagine che seguono. Si pensi, a titolo esemplificativo, al "Regolamento recante disposizioni in materia di rispetto della dignità umana e del principio di non discriminazione di contrasto all'hate speech" del maggio 2019, a cui si è recentemente affiancato il "Regolamento in materia di tutela dei diritti fondamentali della persona ai sensi dell'articolo 30 del Decreto Legislativo 8 novembre 2023, n. 208 (Testo unico dei servizi di media audiovisivi)" del febbraio 2023. Quest'ultimo è un presidio necessario per prevenire questo genere di reati commessi attraverso i servizi media e che permette all'autorità di un imporre sanzioni fino a 600.000 euro, in caso di inosservanza dei divieti.

Anche la legge, avvedendosi finalmente del problema, ha dotato l'autorità di nuovi poteri di intervento nei confronti dei fornitori di piattaforme online, al fine di contrastare le espressioni di odio nel mondo digitale. In particolare, il Capo II del Titolo V del già citato TUSMA, rafforza le tutele nei confronti dei minori per proteggerli da quei contenuti che possono nuocere al loro sviluppo

fisico, mentale o morale. In generale, viene contenuta l'istigazione alla violenza sulle piattaforme di condivisione video.

Insieme alle importanti innovazioni apportate all'intero settore del diritto d'autore, grazie al recepimento della direttiva "Copyright" con le modifiche alla legge 22 aprile 1941 n. 633, queste sono soltanto alcune delle recenti competenze acquisite da Agcom nel contesto di un ecosistema digitale, che cambia e pervade sempre di più la nostra quotidianità. Si tratta di argomenti che ravvivano la necessità di rendere sicuro, tutelante e vivibile il web. La sfera della sicurezza, dunque, non è soltanto l'adozione di misure finalizzate alla protezione delle informazioni personali online, attraverso l'utilizzo di password robuste, sistemi crittografici e protezione antivirus (che rimangono comunque fondamentali), c'è molto di più.

Gli autori, nel loro testo, affrontano con chiarezza cosa voglia dire vivere in un ambiente digitale "a misura d'uomo", adottando una serie di approcci e politiche per porre realmente al centro le persone e i loro diritti nel contesto digitale.

Nonostante l'esigenza di regolamentare in modo nuovo il mondo del web sia diventata sempre più evidente, trovare un sistema di diritti e doveri per lo spazio virtuale rimane un compito complesso. L'idea che Internet dovesse rimanere un territorio privo di regole si è dimostrata fallace, anche a causa dei tentativi di autoregolamentazione che hanno avuto scarso successo. Nonostante la veemenza dei toni con cui nel 1996 venne pubblicata la *Dichiarazione di indipendenza del cyberspazio* è evidente, infatti, che non si è realizzata una "civiltà della mente" improntata agli ideali di libertà e autodeterminazione né uno «spazio sociale globale [...] indipendente». È ormai chiara, sia a livello conscio che inconsapevole, la necessità di pensare a un sistema che tuteli adeguatamente i diritti fondamentali nel più grande spazio di confronto che a oggi l'umanità abbia mai conosciuto.

In questo solco sembrano molto promettenti i progressi compiuti recentemente dall'Europarlamento, con l'architettura di una serie di norme finalizzate a regolamentare l'intelligenza artificiale, con precisi obblighi per i fornitori e gli operatori dei sistemi di IA basati sul livello di pericolosità che tale tecnologia può comportare. È in questo senso che si muove l'Artificial Intelligence Act, il progetto di normativa sull'intelligenza artificiale proposto dalla Commissione europea nell'aprile del 2021. Appena le nuove regole entreranno in vigore, saranno vietati i sistemi di IA che rappresentano un livello di rischio

inaccettabile per la sicurezza delle persone. Un esempio di tali sistemi è quello utilizzato per attribuire il cosiddetto "punteggio sociale", che classifica le persone in base al loro comportamento sociale o alle loro caratteristiche personali. Saranno inoltre banditi i sistemi di IA che potrebbero essere utilizzati in modo intrusivo e discriminatorio, quali ad esempio quelli di identificazione biometrica remota "in tempo reale" in luoghi pubblici accessibili al pubblico, oppure quelli utilizzati "a posteriori" senza previa autorizzazione giudiziaria, a meno che non sia strettamente necessario per investigare un reato grave specifico. Verranno inoltre introdotti obblighi per i provider di sistemi di IA generativa e di modelli base dell'IA, tra cui quello alla trasparenza, che prevederà tra le altre cose la messa in chiaro, nell'output finale, che questo è stato generato con l'IA. Tutti temi peraltro approfonditi in questo libro.

Queste nuove norme rappresentano un importante passo avanti nella regolamentazione dell'IA e, in generale, dei nuovi aspetti tecnologici che incidono maggiormente nella nostra quotidianità, con il duplice obiettivo da un lato di proteggere i diritti e la sicurezza delle persone e, dall'altro, di prevenire l'abuso e l'utilizzo scorretto dell'innovazione.

Tuttavia, il carattere transfrontaliero della rete complica la definizione di queste regole, fattore che costringe a una continua ricerca del giusto equilibrio tra l'adozione di regole chiare e la promozione dell'innovazione e della libertà online.

Sono convinto che la sicurezza dell'ambiente digitale nonché un'adeguata educazione all'utilizzo consapevole delle risorse che la rete ci mette a disposizione, debba diventare una priorità nel dibattito pubblico e nelle politiche istituzionali, e questo libro offre una prospettiva approfondita e informata in quella direzione.

Quando mi feci promotore della legge 92/2019 che ha reintrodotto l'educazione civica obbligatoria e curricolare nelle scuole avevamo l'ambizione di aiutare i nostri giovani a crescere come cittadini e non solo come meri consumatori. È qui la differenza sostanziale per rispondere a "cosa possiamo fare con le tecnologie" piuttosto che "cosa possono farci le tecnologie".

Massimiliano Capitanio
commissario Agcom

Introduzione

Il 21 giugno 2021 doveva essere un giorno come un altro nel municipio di Liegi, in Belgio. Tuttavia, le cose presero una svolta inaspettata quando l'intera rete informatica smise di funzionare, gettando l'amministrazione comunale nel caos. I cittadini, già in fila da ore per ottenere documenti essenziali come certificati di nascita, cambi di residenza o nuove carte d'identità, si ritrovarono improvvisamente privati di tali servizi. Tale disastro informatico era stato causato da un criminale.

Gli aggressori hacker avevano approfittato delle vulnerabilità del sistema informatico del Municipio belga per portare avanti il loro piano criminoso. Chiesero un riscatto per sbloccare la rete e ripristinare il funzionamento normale dell'amministrazione. Il Municipio si trovò quindi nella difficile situazione di dover prendere una decisione: pagare il riscatto o resistere all'attacco.

Le conseguenze dell'attacco furono gravi e durature. Le operazioni degli uffici furono bloccate per oltre due settimane, e più di 1800 computer dovettero essere disconnessi e reinstallati completamente[1].

Situazioni come quella descritta richiamano l'attenzione sulla necessità di una maggiore consapevolezza e preparazione per affrontare le minacce informatiche. I settori che svolgono funzioni critiche per la società dovrebbero essere particolarmente vigili nella protezione dei propri sistemi informatici e dei dati sensibili dei cittadini.

In particolare, settori critici come i trasporti, l'energia, la sanità e la finanza,

1. Si stima che, nel 2021, le perdite dovute al crimine informatico abbiano superato i 5,2 trilioni di euro, equivalente all'intero PIL di Francia, Italia e Spagna.

che dipendono sempre di più dalle tecnologie digitali per la gestione delle loro attività principali, sono sempre più esposti a rischi crescenti.

La sicurezza digitale non riguarda solo le istituzioni, ma anche i singoli cittadini. La scarsa cultura o una cattiva progettazione del sistema algoritmico possono causare errori significativi in grado di bloccare i servizi essenziali o compromettere i diritti fondamentali delle persone. È quindi responsabilità di tutti contribuire a creare un ambiente digitale sicuro e resiliente.

Se è vero, dunque, che la digitalizzazione porta con sé enormi opportunità e offre soluzioni a molte delle moderne sfide, allo stesso tempo espone la società a nuove e diverse minacce. Non è un caso, forse, come gli attacchi e la criminalità informatica stanno aumentando in tutto il globo, in termini sia di quantità che di sofisticazione. Una tendenza destinata a crescere in futuro, visto che si prevede che 22,3 miliardi di dispositivi in tutto il mondo saranno collegati all'Internet delle cose entro il 2024[2].

Ma la sicurezza non riguarda soltanto le infrastrutture di comunicazione. La crescente disponibilità di nuove tecnologie e dati digitali a volte può condurre a inconvenienti tutt'altro che piacevoli e di vasta portata per i cittadini. Tali rischi, negli ultimi anni, sono aumentati in modo significativo, e riguardano tutti gli ambiti della persona: violazioni della vita privata e dei dati personali, diffusione di contenuti illeciti e nocivi in grado di minare la reputazione o la salute stessa, disinformazione, criminalità, sfruttamento e abuso di esseri umani (bambini, adolescenti o adulti), sorveglianza di massa.

Nel prossimo futuro l'intelligenza artificiale[3], la realtà virtuale, l'Internet

2. Cfr. Consiglio europeo, *Cibersicurezza: la risposta dell'UE alle minacce informatiche*, disponibile su https://www.consilium.europa.eu.

3. L'intelligenza artificiale (IA), consiste in una famiglia di tecnologie in grado di generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono. Secondo la definizione impiegata in studi del Parlamento europeo l'intelligenza artificiale (IA) è l'abilità di una macchina di mostrare capacità umane quali il ragionamento, l'apprendimento, la pianificazione e la creatività; tali caratteristiche consentono all'IA la comprensione del proprio ambiente, l'elaborazione di ciò che viene percepito e l'individuazione di soluzioni per un obiettivo specifico. In particolare, il sistema è in grado di ricevere i dati (già preparati o raccolti tramite sensori), di processarli e di indicare la risposta richiesta. Nella società e nell'economia attuali si conoscono numerose categorie di intelligenza artificiale realizzate mediante varie forme: si tratta, tra l'altro, di software come assistenti virtuali, strumenti di analisi di immagini, motori di ricerca, sistemi di riconoscimento facciale e vocale; l'IA interviene, altresì, sotto forma di sistemi incorporati in altri oggetti quali ad esempio robot, veicoli autonomi, droni, e in generale strumenti nel cosiddetto ambito dell'internet delle cose (IoT – Internet of Things).

delle cose[4], le criptovalute[5] e altri cambiamenti tecnologici, avranno un impatto sempre più pervasivo sulle società: insieme all'innovazione dovranno affrontare nuove sfide a livello giuridico, sociale ed etico.

Le istituzioni hanno il dovere di fornire le giuste risposte normative a questi delicati aspetti. Uno dei più delicati e ampiamente discussi dalle istituzioni europee (e non solo), riguarda l'utilizzo dei sistemi di intelligenza artificiale (nel proseguo di questo libro, anche "IA") nella gestione delle decisioni. Si tratta di una questione che mette a nudo un nervo scoperto dell'innovazione tecnologica. Tra le criticità dedotte dalla Commissione europea, infatti, rientra l'impossibilità di stabilire il motivo per cui un sistema di IA è giunto a un risultato specifico (la c.d. "opacità del processo"), determinando una serie di difficoltà nel valutare e dimostrare l'eventualità che qualcuno sia stato ingiustamente svantaggiato dagli algoritmi, ad esempio nel contesto di una decisione di assunzione o di promozione oppure di una domanda di prestazioni pubbliche[6]. Si immagini, ad esempio, che una richiesta di prestito venga rifiutata dalla banca perché un computer ha analizzato tutte le spese effettuate negli ultimi mesi e ha detto "no", oppure che lo stesso computer scarti un curriculum e non lo ritenga idoneo per effettuare un colloquio di lavoro, prima ancora che il selezionatore abbia incontrato e conosciuto "davvero" la persona interessata. Per questo, delegare completamente taluni processi alla tecnologia, specialmente nel campo delle risorse umane nel mondo del lavoro, può rivelarsi pericoloso e discriminatorio[7].

Da ultimo, è doveroso ricordare il tema dei rischi per l'ordinato svolgimento del dibattito pubblico determinati dall'uso dell'intelligenza artificiale e delle chiavi algoritmiche nel contesto dell'informazione; è il caso, per esempio, della

4. L'"Internet delle cose" è un'espressione impiegata per indicare quell'insieme di oggetti di uso quotidiano come telefoni, automobili, elettrodomestici, vestiti, etc, che sono collegati ad internet con una connessione senza fili tramite chip intelligenti e sono in grado di rilevare e comunicare dati.

5. Il termine "criptovaluta" è composto da due parole: "cripto" e "valuta". Si tratta di una forma di valuta "nascosta" in quanto è visibile e utilizzabile solo attraverso la conoscenza di un determinato codice informatico, noto come "chiavi di accesso" pubblica e privata, espressa in un linguaggio ancora più tecnico. La criptovaluta non esiste fisicamente, motivo per cui viene definita "virtuale". È generata e scambiata esclusivamente attraverso le comunicazioni telematiche. Non è quindi possibile trovare criptovalute in formato cartaceo o metallico in circolazione.

6. Cfr. Camera dei deputati, Dossier di documentazione n. 57 del 12 novembre 2021.

7. Basare le proprie decisioni basandosi su dati contenenti distorsioni storiche, ad esempio, hanno finito per favorire assunzioni o promozioni maschili rispetto a quelle femminili.

capacità dell'IA di creare bolle in rete in cui i contenuti sono presentati in base alle preferenze o le interazioni che l'utente esprime durante la sua navigazione sul web, con l'effetto di impedire la tutela di un ambiente aperto a un dibattito pluralistico, inclusivo e accessibile[8].

Come più volte desiderato (e ribadito con forza) dalla stessa Unione europea, quando interagiscono con l'ambiente digitale, persone e imprese non dovrebbero subire pregiudizi e godere di minori diritti, né essere meno protette rispetto a quando operano nel mondo reale. La trasformazione digitale non giustifica eccezioni o deroghe ai diritti e alle libertà di cui godono i cittadini[9]. Ma, purtroppo, non sempre detto ciò corrisponde alla verità. Anzi.

Gli algoritmi dell'IA, ad esempio, possono essere utilizzati per creare immagini, video e audio falsi (ma estremamente realistici), noti come deepfake, in grado di truffare, pregiudicare la reputazione e mettere in dubbio la fiducia in ciò che vediamo attraverso lo schermo, con il rischio che, in definitiva, si crei un processo di polarizzazione del dibattito pubblico e di manipolazione dei processi decisionali come, ad esempio, le elezioni[10].

Insomma, c'è da stare molto attenti prima di acclamare l'innovazione come panacea di ogni problema. Se è vero che la recente pandemia di Covid-19 ha messo in luce i vantaggi offerti dalle tecnologie digitali, la stessa emergenza sanitaria ha reso visibile la necessità di garantire parità di accesso alle tecnologie (tanto per i dispositivi quanto per la rete), nonché alle capacità e al bisogno di ottenere le giuste competenze digitali, compresa la relativa necessaria alfabetizzazione. In quest'ottica, e per affrontare i rischi e i danni di una società sempre più digitalizzata, è necessario riporre al centro del dibattito la questione della "sicurezza" dell'ambiente digitale in tutte le sue forme, tenuto conto che, ormai, la nostra vita è sempre più legata al mondo dei dati, risorsa sempre più strategica in termini anche di evoluzione[11].

Ne è un esempio la storia del professor Tsiknakis, coordinatore del progetto di ricerca ProCAncer-I. Il suo gruppo, composto da 20 partner provenienti da

8. Cfr. Camera dei deputati, Dossier di documentazione, *cit.*

9. Cfr. Comunicazione della Commissione europea COM(2022) 27 final relativa alla definizione di una dichiarazione europea sui diritti e i principi digitali.

10. Cfr. Camera dei deputati, Dossier di documentazione, *cit.*

11. Nel 2018 il volume di dati prodotti annualmente è stato stimato in 33 zettabyte. Entro il 2025, saranno 175 zettabyte. Se si volessero copiare tutte queste informazioni su dei DVD e creare una torre, essa arriverebbe fino alla luna e ritorno per ben 33 volte.

tutta l'UE, dagli Stati Uniti e dalla Turchia, sta lavorando ad una piattaforma basata sull'intelligenza artificiale che si propone di identificare il cancro alla prostata prima e con maggiore precisione. Confrontando le immagini dei tessuti tumorali e i risultati dei test di oltre 17.000 pazienti, l'algoritmo cerca i casi che presentano la più alta probabilità di malattia. Il progetto avanzerebbe molto più velocemente se i ricercatori avessero un accesso migliore e più facile ai dati medici storici, che rimane difficile. Per fortuna tutto questo sta per cambiare[12].

Sicurezza delle infrastrutture, dunque, e sicurezza delle persone, specialmente le più fragili e vulnerabili, come i minori.

L'uso delle tecnologie digitali da parte dei più piccoli è radicalmente cambiato negli ultimi anni. I dispositivi moderni consentono agli utenti minorenni di interagire, creare contatti, giocare e condividere contenuti con altri utenti, spesso senza la supervisione dei genitori. Secondo i risultati dell'indagine "EU Kids Online" del 2020[13] la maggioranza dei minori dichiara di usare il proprio smartphone "ogni giorno" o "quasi sempre"; in molti Paesi il tempo trascorso online dai minori è quasi raddoppiato rispetto al 2010. I minori iniziano a usare dispositivi digitali a un'età sempre più precoce, con conseguenze del tutto benefiche, come approfondito nei vari capitoli di questo splendido volume.

Nella sicurezza tecnologica che impatta sulla vita di adulti e bambini non è da sottovalutare, infatti, l'aspetto riguardante gli effetti dei nuovi strumenti digitali sulla salute. Un livello di utilizzo tanto elevato di Internet (e device connessi) può condurre a uno stile di vita più sedentario con possibili ripercussioni sul benessere della persona. Ma questo, alla luce delle considerazioni sviluppate dall'autore sembra il minimo. Molti psicologi hanno espresso preoccupazione per il rischio che gli utenti – specie se piccoli – sviluppino disturbi dell'attenzione e difficoltà a disconnettersi.

Se, da una parte, si cerca di promuovere un equilibrio sano tra vita online e vita offline, l'astinenza digitale non rappresenta però oggi un'opzione realistica, in quanto l'accesso a informazioni, all'istruzione, ai contatti sociali e all'intrattenimento avviene sempre più spesso online[14]. La tecnologia fa parte

12. Nel maggio 2022, come meglio dettagliato *infra*, l'Unione europea ha adottato la legge sulla governance dei dati. Questa nuova legislazione dell'UE faciliterà l'accesso ai dati nel rispetto della privacy personale.

13. Cfr. EU Kids online 2020.

14. Cfr. Comunicazione della Commissione europea COM(2022) 212 final.

ormai della nostra vita e, come in una nuova e rinnovata scala dei bisogni di Maslow, non è azzardato affermare che essa è divenuta fondamentale per vivere la nostra quotidianità con le sue opportunità e i suoi rischi. Ma c'è di più. le innovazioni stanno infatti creando anche veri e propri nuovi mondi, modificando profondamente il nostro modo di pensare e agire.

Una nuova realtà fisica, metafisica e virtuale ci avvolge, ci cambia, trasforma percezioni, linguaggio e modi di vedere la realtà. Sta a noi rimanere con i piedi ben saldi sulla terra, nonostante il fatto che le nostre teste saranno sempre più immerse nel cloud.

Fabio Massimo Castaldo
europarlamentare