La sicurezza nell'era della digitalizzazione: rischi, difese e prospettive future

di *Marino D'Amore*[*]

L'articolo esamina i rischi associati alla sicurezza dei dati: gli attacchi informatici, le violazioni della privacy, il ransomware e il phishing. Inoltre, si analizzano strategie come la crittografia, i firewall, i sistemi di rilevamento delle intrusioni, le sfide etiche legate all'utilizzo dei dati personali e il bilanciamento tra la sicurezza pubblica e l'intelligenza artificiale, evidenziando l'importanza di un approccio multidisciplinare.

Parole chiave: sicurezza; rischio; digitale; intelligenza artificiale; tecnologia; privacy.

Security in the age of digitalisation: risks, defences and future prospects

The article examines the risks associated with data security: cyber attacks, privacy breaches, ransomware and phishing. Furthermore, strategies such as encryption, firewalls, intrusion detection systems, ethical challenges related to the use of personal data and balancing public safety and artificial intelligence are analysed, highlighting the importance of a multidisciplinary approach.

Keywords: security; risk; digital; artificial intelligence; technology; privacy.

1. Digitalizzazione e mutamento sociotecnico

La digitalizzazione, intesa come processo, sociale e tecnologico, che trasforma sistematicamente e dematerializza attività sociali, culturali, economiche e politiche, ha profondamente ridisegnato le relazioni tra individui, organizzazioni e istituzioni (Castells, 2009). Essa ha modificato il tessuto comunicativo, sociale e produttivo della società stessa, introducendo però nuove criticità e forme di vulnerabilità. In tale contesto la sicurezza digitale non deve interpretata esclusivamente come una mera questione tecnica, bensì come un fenomeno multifattoriale che intreccia diverse traiettorie semantiche caratterizzata da competenze informatiche, governance normativa, etica dei dati e struttura sociale (Maras, 2015).

DOI: 10.5281/zenodo.17558936

[*] Università Niccolò Cusano. marinodamore@gmail.com.

Floridi (2014), sostiene che, attualmente, l'esistenza antropica abita e si dipana nella cosiddetta "infosfera", un ambiente ontologico in cui l'interazione tra esseri umani e agenti digitali diventa prodromo, parte integrante ed elemento costitutivo della realtà sociale in quanto tale. In un ecosistema *always networked* ogni azione digitale può rappresentare una potenziale esposizione al rischio e, quindi, necessita di un ripensamento critico dei concetti classici di sicurezza, privacy e responsabilità.

Nella società del rischio (Beck, 1992) i pericoli derivanti dalla digitalizzazione, come la perdita di dati sensibili, la manipolazione algoritmica e le aggressioni informatiche, non derivano da eventi imprevedibili, ma dalla stessa essenza intrinseca della modernità e dalla razionalità tecnico-scientifica che la sostiene. Il rischio, pertanto, diventa una categoria sociale prodotta, comunicata e negoziata collettivamente, mentre i media, le élite tecnoscientifiche e le istituzioni contribuiscono alla definizione socioculturale di cosa sia considerato una minaccia, calibrando continuamente la percezione pubblica e influenzando la domanda di sicurezza (Douglas, Wildavsky, 1983). Da questo punto di vista, la *cybersecurity* oltre a rappresentare una risposta squisitamente tecnica, si palesa anche come un prodotto della cultura della sorveglianza e della governance neoliberale, in cui la responsabilità della protezione viene sempre più delegata all'individuo (Zuboff, 2019). La narrazione dominante del "cittadino digitale consapevole" oscura spesso le asimmetrie di potere tra attori coinvolti nei complessi processi di digitalizzazione posti in essere. Le implicazioni etiche della digitalizzazione richiedono un ampliamento della prospettiva normativa oltre la mera compliance giuridica. Il Regolamento Generale sulla Protezione dei Dati (GDPR), promulgato dall'Unione Europea nel 2016 ed entrato in vigore nel 2018, ha rappresentato un passo fondamentale verso il diritto alla protezione dei dati, un diritto centrato sull'individuo (Voigt, von dem Bussche, 2017). Tuttavia, numerose ricerche mostrano i limiti strutturali della regolamentazione giuridica nella tutela della privacy, soprattutto quando questa si confronta con logiche, estrattive e predittive, dei dati (Mittelstadt *et al.*, 2016).

La governance e la profilazione algoritmica impongono nuove sfide, sia in termini di responsabilità sia di trasparenza dei processi decisionali. le tecnologie non sono neutre, ma si caratterizzino per valori e finalità politiche, richiedendo analisi, critiche e interdisciplinari, capaci di indagare le implicazioni sociopolitiche che determinano. In tale contesto la dimensione socioeconomica è spesso trascurata, ma riveste un'importanza centrale, infatti, le disuguaglianze non si limitano all'accesso alla tecnologia (*first-level digital divide*), ma comprendono anche la capacità di utilizzarla in modo efficace (*second-level*) e il conseguimento di eventuali i benefici (*third-level*). Le categorie sociali svantaggiate, come anziani, migranti, individui con bassa scolarizzazione, risultano più esposti

ai rischi analizzati, a causa della scarsa alfabetizzazione digitale e della limitata possibilità di adottare misure preventive efficaci (van Dijk, 2012). In questo scenario, la sicurezza digitale si configura come un bene stratificato, che riflette le gerarchie sociali esistenti e contribuisce alla loro reiterazione nel tempo, ma, al tempo stesso, deve considerare le dimensioni strutturali e socioculturali che caratterizzano l'accesso, l'utilizzo e la protezione nelle nuove tecnologie.

2. Il concetto sociologico di minaccia digitale

Nel contesto contemporaneo le minacce alla sicurezza digitale non si riducono a problematiche meramente tecniche, ma si caratterizzano come fenomeni complessi che riflettono, producono e amplificano, come spiegato, traiettorie di potere, disuguaglianza e dinamiche controllo. Esse rientrano in quella che Ulrich Beck ha definito *modernizzazione riflessiva*, ovvero una fase storica in cui i rischi sono generati dai successi della razionalità tecnico-scientifica stessa (Beck, 1992). La cybersicurezza, pertanto, si pone metà tra innovazione tecnologica e vulnerabilità strutturale, evidenziando il paradosso insito nella società dell'informazione come innovativa e minacciosa al tempo stesso. I pericoli digitali rappresentano una criticità in continua evoluzione e si concretizzano in modalità di attacco che risultano particolarmente dannose per il loro impatto diffusivo: il *ransomware,* ad esempio*,* si manifesta come una fattispecie particolarmente aggressiva di estorsione digitale. Tale pratica, attraverso l'acquisizione dei dati, e la conseguente richiesta di pagamenti come riscatto, nei casi più gravi, inficia il funzionamento di infrastrutture e servizi essenziali, estendendosi, secondo una logica induttiva, dai singoli utenti alle grandi aziende pubbliche, diventando, di fatto, una minaccia transnazionale. Un altro attacco particolarmente diffuso è il *phishing*, un fenomeno che si basa sulla manipolazione emozionale e delle dinamiche decisionali dell'utente per indurlo a rivelare informazioni sensibili. L'aspetto critico di tale minaccia risiede nel fatto che essa non si basa su un deficit di tipo tecnologico, ma su istanze psicologico-culturali che rendono essenziale e inderogabile l'adozione di strategie educativo-preventive (Livingstone, Helsper 2007).

La violazione sistematica della privacy costituisce un rischio di ampia e imprevedibile portata, infatti l'accumulazione massiva di dati personali, attraverso piattaforme digitali e dispositivi mobili ha trasformato la privacy da diritto individuale a macrofenomeno strutturale legato alla redistribuzione del potere informativo. In questo complesso panorama, il controllo dei dati espone gli individui a furti d'identità o discriminazioni algoritmiche e, al contempo, altera profondamente il rapporto biunivoco tra cittadini e istituzioni. La violazione della privacy

si configura anche come un fattore di progressiva erosione della fiducia sociale, infatti l'instabilità della sicurezza digitale mina il capitale fiduciario tra governati e governanti, aggravando le disuguaglianze e favorendo l'adozione di pratiche difensive da parte degli utenti (Solove, 2008).

Le minacce digitali non sono distribuite in modo uniforme, ma riflettono forti asimmetrie tra il nord e il sud globale, tra aziende multinazionali e microimprese, tra esperti IT e cittadini comuni. I paesi con minore capacità tecnologica e tutela giuridica sono spesso terreno fertile per attività criminali informatiche, mentre le grandi multinazionali globali dispongono di mezzi adeguati per proteggersi e, soprattutto, per sfruttare i dati raccolti finalizzati ad azioni quali guerre informative, spionaggio industriale e controllo politico (Greenberg 2019).

3. Difese e strategie di protezione: sicurezza informatica come ecosistema socio-tecnologico

La cybersicurezza rappresenta una pratica sociale emergente che coinvolge attori, tecnologie, norme e valori come elementi coinvolti in un continuo adattamento a un ambiente digitale in costante trasformazione (Bauman, 2011). Essa rappresenta una complessa commistione di elementi umani e tecnologici, basata sull'interdipendenza tra software, hardware, competenze antropiche e contesto normativo. La crittografia, ad esempio, è uno degli strumenti necessari per l'implementazione di sistemi di sicurezza digitale; essa si basa su articolate logiche matematiche atte a garantire la riservatezza e l'integrità dei dati durante la trasmissione (Diffie, Hellman, 2022). La sua efficacia dipende dalla complessità strutturale che ne definisce la cifra identitaria e dal rapporto fiduciario instaurato con le istituzioni che ne gestiscono l'uso. Tale strumento ha assunto un significato simbolico, che lo definisce come un mezzo di autodeterminazione digitale, ma anche come una tecnologia finalizzata al controllo diffuso, il cui utilizzo viene spesso regolato, o ostacolato, dalle classi dirigenti per motivi di sicurezza nazionale (Greenberg, 2019), ponendo in essere interrogativi cruciali sul rapporto, dicotomico e bidirezionale, tra libertà individuale e controllo statale. I firewall e i sistemi di rilevamento delle intrusioni (IDS) sono i dispositivi fondamentali per la protezione delle reti informatiche: i primi regolano il traffico di rete, mentre i secondi controllano le attività al suo interno, nella ricerca di anomalie e comportamenti sospetti. Entrambi si inseriscono nella logica della sicurezza perimetrale, messa in crisi dalla diffusione di architetture decentralizzate, dal cloud computing e dalla mobilità dei devices, elementi che palesano l'obsolescenza del concetto limitante e anacronistico del "muro digitale" in favore di

modelli più fluidi (Bauman, 2011), come la sicurezza zero-trust[1], che non presuppongono una fiducia ciecamente fideistica nei confronti dei nodi della rete (Shostack, 2014).

Un vulnus significativo nei sistemi di sicurezza è rappresentato dall'errore umano: la disattenzione o la mancanza di formazione si pongono spesso all'origine delle violazioni informatiche più gravi. La sicurezza deve essere certamente garantita dai devices tecnologici, ma necessita inoltre da un bisogno, culturale e organizzativo, che catalizzi l'apprendimento continuo, la responsabilizzazione degli utenti e la comunicazione trasparente. L'educazione alla sicurezza digitale, intesa come forma di *digital literacy*, è quindi una componente essenziale della protezione, che include le conoscenze tecnico-teoriche e le competenze critiche per riconoscere le violazioni, interpretare i rischi e prendere decisioni efficaci (Livingstone, Helsper, 2007).

4. Il ruolo delle normative: il GDPR e la protezione dei dati personali

La circolazione commercializzata dei dati costituisce il fondamento dell'economia digitale, perciò, la protezione della privacy si configura come uno dei postulati, prodromici e irrinunciabili, per la tutela della sicurezza digitale. Il regolamento generale sulla protezione dei dati (GDPR), in vigore nell'Unione Europea dal 2018, è il primo strumento normativo a definire la tutela dei dati personali come un diritto fondamentale, con conseguenze, endogene e esogene, vincolanti e extraterritoriali, per gli stati, le aziende e i cittadini europei (Voigt, von dem Bussche, 2017). Infatti, il GDPR indica direttive e obblighi da rispettare (il *data breach notification* o principio di minimizzazione dei dati[2]), ma, soprattutto, catalizza un evidente cambio di rotta, basato sulla responsabilizzazione degli attori coinvolti, che utilizzano i dati stessi. Tuttavia, tale impianto normativo non è sufficiente a garantire un'effettiva protezione della privacy digitale, infatti, diverse ricerche evidenziano come la rocciosa asimmetria di potere tra utenti e piattaforme digitali renda spesso irrealizzabili le intenzioni regolatrici

[1] La sicurezza Zero Trust è un modello che adotta un approccio di "mai fidarsi, sempre verificare" per la protezione delle risorse, indipendentemente dal fatto che si trovino all'interno o all'esterno del perimetro di rete dell'organizzazione. Invece di presumere che tutto ciò che si trova all'interno della rete sia sicuro, Zero Trust richiede che ogni utente, dispositivo e applicazione venga autenticato e autorizzato prima di concedere l'accesso alle risorse.

[2] La notifica di data breach, nel contesto della CSA (Cloud Security Alliance) e secondo il GDPR, è l'obbligo di comunicare alle autorità competenti, e in alcuni casi agli interessati, una violazione della sicurezza dei dati personali che potrebbe comportare rischi per i loro diritti e libertà.

del GDPR in casi concreti (Mittelstadt *et al.*, 2016), tutto ciò dimostra come la tutela suddetta sia diventata, di fatto, un diritto formalmente garantito, ma sostanzialmente neutralizzato da modelli, politici e economici, basati sull'appropriazione e sull'uso, invasivo e sistematico, di informazioni. Essa deve essere considerata come un diritto inviolabile, ma anche come una condizione, fondamentale e strutturale al contempo, di autodeterminazione, soggettiva e collettiva, nelle società digitalizzate, perché permette agli utenti di mantenere un'autonomia, critica e fattuale, dall'intromissione istituzionale e di partecipare alla vita pubblica senza timori, complottisti e distopici, di sorveglianza (Solove, 2008; Zuboff, 2019). Uno degli aspetti più complessi nel dibattito sulla protezione dei dati riguarda l'equilibrio tra privacy individuale e sicurezza pubblica. Le misure adottate per contrastare il terrorismo o la criminalità informatica, come il controllo algoritmico o l'uso di backdoor crittografici, possono minare le garanzie fondamentali dell'ordinamento democratico. Si tratta quindi di un conflitto inevitabile tra due beni pubblici: la sicurezza e la libertà che una governance democratica generalmente intesa deve essere capace di gestire, neutralizzando tali tensioni con trasparenza, legittimità e inclusività, impedendo che questi intenti protettivi diventino il pretesto eziologico e meccanicistico per pericolose derive autoritarie. Il GDPR ha avuto un impatto oltre i confini europei, diventando un riferimento globale nel processo di armonizzazione delle leggi in questo ambito. Paesi come Brasile, India e California si sono ispirati esplicitamente al modello europeo, attuando un processo di convergenza normativa noto come *Brussels Effect* (Bradford, 2020). Tuttavia, l'emergere di altri modelli normativi, come quello cinese basato sul concetto di *cyber-sovereignty*, evidenzia la crescente politicizzazione di tale modello che sfocia nell'oscuramento censorio delle informazioni. La cybersicurezza diventa così un campo di conflitto geopolitico e ideologico, in cui si confrontano visioni differenti dei diritti, della sovranità e del ruolo statuale.

5. Intelligenza Artificiale e sicurezza: potenzialità e rischi

L'intelligenza artificiale realizza l'analisi di grandi quantità di dati in tempo reale, attraverso il *machine*[3] e il *deep learning*[4], consentendo di rilevare potenziali minacce, attuare risposte automatizzate agli attacchi e pianificare strategie difensive dedicate (Ejreaw, Annowari, 2023). Il suo utilizzo pone sul tavolo

[3] Una categoria di intelligenza artificiale che permette alle macchine di apprendere dai dati e migliorare le proprie prestazioni su specifiche attività senza essere programmate direttamente.
[4] Una branca specifica del machine learning che utilizza reti neurali artificiali complesse per l'elaborazione dei dati, ispirate al funzionamento del cervello umano

della riflessione pubblica questioni etiche, sociali e politiche significative, in quanto sicuramente rappresenta un'opportunità per la sicurezza digitale, ma costituisce anche la sua nemesi, ossia il rischio venga utilizzata per fini illegali, come la creazione di malware e lo sviluppo di attacchi a sistemi informatici. Essa catalizza una profonda ridefinizione delle dinamiche relazionali, e fidelizzanti, tra utenti, istituzioni e tecnologia, poiché la delega del controllo all'IA maginalizza il ruolo antropico, lo relega in una posizione residuale, depauperando il suo ruolo e trasformandolo, di fatto, in un target passivo sottoposto a una potenziale profilazione.

La tecnologia *blockchain* assicura una maggiore affidabilità nelle transazioni digitali, anche grazie alla condivisione di un registro aggiornato dei soggetti coinvolti, in particolare per quanto riguarda la tracciabilità e la trasparenza dei dati (Narayanan *et al.*, 2016), tuttavia, nonostante in ambiti come la finanza e la gestione delle identità digitali, essa sia considerata un'infrastruttura efficace per ridurre i rischi di manipolazione e di hackeraggio, in contesti più ampi e meno monitorabili, può subire imprevedibili e pericolose evoluzioni criminali.

La decentralizzazione introduce nuove criticità: in assenza di un'autorità centrale, le responsabilità diventano numerose e, in caso di abuso, difficilmente identificabili. La governance dei protocolli blockchain è poco trasparente, tecnocratica e suscettibile a subordinarsi a dinamiche di potere informale, come dimostrato nei casi di *hard fork*[5] o attacchi alle DAO[6] (*Decentralized Autonomous Organizations*). Inoltre, il suddetto registro può confliggere con il diritto all'oblio sancito dal GDPR, rendendo difficoltoso l'inserimento della blockchain nei quadri normativi esistenti.

Le tecnologie analizzate stanno trasformando il cyberspazio in un nuovo, possibile scenario del conflitto geopolitico: stati, terroristi e gruppi di cyber-mercenari utilizzano l'IA e la crittografia avanzata per scopi esecrabili, come la disinformazione strategica e complottista, l'influenza elettorale e la paralisi di infrastrutture statuali (Greenberg, 2019). Insomma, il confine tra difesa e attacco in cybersicurezza diventa labile, si mitiga, poiché, come spiegato, gli strumenti sviluppati per la protezione possono essere facilmente riconvertiti, secondo una logica speculare, per scopi ostili. La militarizzazione del cyberspazio pone, al

[5] Una hard fork è una modifica radicale a una blockchain che crea una nuova versione incompatibile con la precedente. Ciò richiede a tutti i nodi di aggiornare il software per continuare a partecipare alla rete, in caso contrario, si crea una divisione permanente nella blockchain, spesso portando alla nascita di una nuova criptovaluta

[6] La DAO è un'organizzazione autonoma decentralizzata, governata da una comunità che utilizza regole codificate in contratti intelligenti su una blockchain, invece di strutture gerarchiche tradizionali. Le DAO mirano a essere trasparenti e autonome, con un processo decisionale spesso facilitato da sistemi di voto basati su token.

contempo, interrogativi etici e giuridici inediti, perché non esiste ancora una normazione condivisa che disciplini l'uso delle tecnologie digitali. Inoltre, la continua diffusione di attacchi informatici, spesso impossibili da attribuire con certezza, compromette la trasparenza nella governance globale della sicurezza e delle singole nazioni.

Le nuove tecnologie richiedono forme di governo e controllo fluide, duttili, capaci di porsi tra innovazione, diritti fondamentali e coesione sociale, armonizzando il connubio di tali elementi. Occorre considerare però che la velocità dell'innovazione supera spesso la capacità normativa delle istituzioni, creando zone grigie in cui si verificano abusi e discriminazioni (Bauman, 2000), Diventa, quindi, essenziale promuovere un approccio interdisciplinare alla sicurezza digitale, che coinvolga più figure professionalizzate come informatici, sociologi, giuristi, filosofi, poiché solo una visione sinottica in questo ambito può produrre soluzioni resilienti e legittime, evitando che l'innovazione si trasformi in una nuova forma di esclusione o controllo permanente, non regolamentato e quindi potenzialmente discriminatorio.

Conclusioni

L'implementazione della sicurezza informatica non abita esclusivamente il campo del determinismo tecnologico, ma deve essere considerata, secondo un'ottica multifocale, come una costruzione socioculturale. Essa attualizza una doppia sfida: quella epistemica, che riguarda ciò che sappiamo dei rischi potenziali che recare, e quella politica, che attiene alla distribuzione delle risorse, dei poteri e dei diritti (Beck, 1992; Douglas, Wildavsky, 1983). In questo senso la quantità degli attori coinvolti (aziende, governi, hacker, utenti) e la natura transnazionale del cyberspazio impongono un approccio globale, dialogico e interdisciplinare.

La digitalizzazione non ha solo modificato le criticità esistenti, ma ne ha introdotti di nuove, spesso non prevedibili, lasciando emergere la fluidità intrinseca dell'intima essenza delle società moderne (Bauman, 2000). Tecnologie autonome e decentralizzate, come IA, blockchain e ambienti cyber-fisici, amplifica le zone d'ombra, rendendo la sicurezza un processo costantemente adattivo e mai concluso.

Nonostante i significativi progressi nella crittografia, nei sistemi di detection e nella sicurezza perimetrale, le difese si rivelano sempre provvisorie. I sistemi automatizzati possono fallire nel prevenire minacce non convenzionali o mutanti, e l'affidamento eccessivo all'IA può generare una falsa percezione di controllo.

È quindi necessario pensare a una governance integrata della sicurezza, che includa:

- norme giuridiche e regolatorie efficaci;
- pratiche educative e partecipative;
- meccanismi democratici di sorveglianza delle tecnologie;
- infrastrutture sociotecniche resilienti.

Essa mitigare le disuguaglianze digitali e mirare all'inclusività, poiché la sicurezza non è accessibile in tutti i contesti sociali e geografici nello stesso modo (van Dijk, 2012). Quest'ultima dovrà rappresentare la qualità emergente e irrinunciabile di un ecosistema sociotecnico, non come il risultato di un'unica tecnologia o politica, ma di un'interazione dinamica e continua tra innovazione, cultura e pratiche sociali (Maras, 2015).

Per affrontare le sfide emergenti, è imprescindibile un approccio interdisciplinare che unisca:

- le competenze ingegneristiche e informatiche;
- la riflessione etica e giuridica;
- le analisi sociologiche e antropologiche;
- la partecipazione civica e il pluralismo epistemico.

Shoshana Zuboff (2019) sostiene che solo una cultura della resistenza potrà contrastare il capitalismo della sorveglianza e ristabilire il primato dei diritti umani sulle nuove tecnologie. Secondo la studiosa l'innovazione dovrà essere coadiuvata da un'etica della responsabilità, che superi il modello individualista e neoliberale della sicurezza intesa come privilegio privato e rafforzi i diritti digitali, come postulati irrinunciabili per la cittadinanza democratica nell'infosfera (Floridi, 2014).

Il villaggio globale impone che la sicurezza digitale non sia considerata un mero obiettivo tecnico, ma un bene collettivo da difendere con impegno costante, in un'ottica di solidarietà, trasparenza e giustizia sociale (McLuhan, Powers, 1996).

Riferimenti bibliografici

Bauman Z. (2000). *Liquid modernity*. New York: John Wiley and Sons.
Beck U. (1992). *Risk society: towards a new modernity*. London: Sage Publications.

Binns R. (2017). Fairness in machine learning: lessons from political philosophy. In *Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency (FAT*)* (pp. 149-159). New York: ACM.

Bradford A. (2020). *The Brussels effect: how the European Union rules the world*. Oxford: Oxford University Press.

Castells M. (2009). *Communication power*. Oxford: Oxford University Press.

Diffie W., Hellman M.E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6): 644-654.

Douglas M., Wildavsky A. (1983). *Risk and culture: an essay on the selection of technological and environmental dangers*. Berkeley: University of California Press.

Ejreaw A.M.A., Annowari N.B. (2023). Artificial intelligence for cybersecurity: opportunities and challenges. *International Journal of Business Society*, 28(1): 1-15.

Floridi L. (2014). *The fourth revolution: how the infosphere is reshaping human reality*. Oxford: Oxford University Press.

Greenberg A. (2019). *Sandworm: a new era of cyberwar and the hunt for the Kremlin's most dangerous hackers*. New York: Doubleday.

Livingstone S., Helsper E.J. (2007). Gradations in digital inclusion: children, young people and the digital divide. *New Media & Society*, 9(4): 671-696.

Maras M.H. (2016). *Cybercriminology*. Oxford: Oxford University Press.

McLuhan M., Powers B.R. (1996). *Il villaggio globale. XXI secolo: trasformazioni nella vita e nei media*. Milano: Sugarco.

Mittelstadt B.D., Allo P., Taddeo M., Wachter S., Floridi L. (2016). The ethics of algorithms: mapping the debate. *Big Data & Society*, 3(2): 1-21.

Narayanan A., Bonneau J., Felten E., Miller A. (2016). *Bitcoin and cryptocurrency technologies*. Princeton: Princeton University Press.

Shostack A. (2014). *Threat modeling: designing for security* (2ª ed.). Hoboken: Wiley.

Solove D.J. (2008). *Understanding privacy*. Cambridge (MA): Harvard University Press.

Van Dijk J.A.G.M. (2012). *The network society: social aspects of new media*. London: Sage Publications.

Voigt P., von dem Bussche A. (2017). *The EU General Data Protection Regulation (GDPR): a practical guide*. Cham: Springer.

Zuboff S. (2019). *The age of surveillance capitalism. The fight for a human future at the new frontier of power*. New York: PublicAffairs.